The Heritage Foundation

BACKGROUNDER
No. 3790 | SEPTEMBER 20, 2023
ASIAN STUDIES CENTER

North Korea's Cybercrimes Pay for Weapons Programs and Undermine Sanctions

Bruce Klingner

KEY TAKEAWAYS

North Korea's cyberattack capabilities pose a grave threat to international peace and security, as well as to the stability of the global financial system.

Pyongyang conducts cybercrimes to fund its nuclear and missile programs and to undermine the effectiveness of international sanctions.

The United States must work with the private sector and foreign governments to augment cyber defenses and respond more forcefully to North Korean cyberattacks.

North Korea's nuclear weapons and missiles pose a direct military threat to the United States and its allies. Pyongyang has long threatened to use its nuclear weapons in pre-emptive attacks and vowed never to abandon its "trusted shield" and "treasured sword"[1] in negotiations.

Similarly, Pyongyang's cyberattack capabilities pose a multi-faceted threat to international security since the regime has successfully penetrated and inflicted damage on military, government, media, and infrastructure computer networks. North Korea could inflict devastating damage during a crisis by simultaneously targeting the military, financial, and infrastructure sectors of one or several countries. Kim Jong-un declared that cyber warfare is a "magic weapon"[2] and an "all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability."[3]

North Korea is in the top tier of global cyber threats and is unique amongst cyber-capable nations in prioritizing cybercrimes to circumvent international sanctions and finance its nuclear and missile programs. Pyongyang modified its strategy as other countries' financial cyber defenses improved, shifting from cyberattacks on traditional financial institutions to cryptocurrency providers, then to decentralized finance (DeFi) platforms, which are more vulnerable to hacking. Regime tactics continue to evolve in response to enhanced protections and new technologies.

Despite growing awareness and actions against North Korean financial cybercrimes, the regime continues to score major thefts against an array of victims. Pyongyang's sophisticated cybercrimes pose a threat to the international financial system, undermine United Nations and U.S. sanctions, and enable the regime to augment its nuclear threat against the United States and its allies.

The United States must take the lead in working with foreign governments and the private sector to augment cyber defenses and respond more forcefully to North Korean cyberattacks. Washington should increase enforcement of existing laws and implement necessary additional legislation and regulatory measures.

North Korea's Cyber Capabilities Pose Grave Threat to U.S. and Allies

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.[4]

In February 2023, the Director of National Intelligence assessed that North Korea's cyber program posed 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."[5] 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.[6] North Korean hackers were estimated to account for more than 50 percent of the total global losses arising from cryptocurrency hacks.[7]

North Korea has developed a comprehensive program to train thousands of cyberwarriors. While most toil covertly, North Korean university students have demonstrated that they are among the best in the world. North Korean contestants from the Kim Chaek University of Technology and Kim Il-sung University swept the top four prizes in a May 2023 online computer program coding contest of 1,700 contestants hosted by U.S. IT company

HackerEarth. In 2020, North Korean students won the CodeChef online coding contests for six months running in a competition of 30,000 university students from around the world.[8]

New Tools for an Old Strategy. The North Korean regime has a long history of using criminal activities to acquire money. Earlier criminal enterprises 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 more efficient, cost-effective, and lucrative ways 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[9] 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 North Korea's successful theft of $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 increased cyber protections, Pyongyang shifted to targeting cryptocurrency exchanges, which proved to be far more lucrative. By 2020, North Korean "attacks against virtual currency exchange houses [had] produced more illicit proceeds than attacks against financial institutions."[10] North Korea has now switched almost 100 percent of its operations to cryptocurrency-related hacks.[11]

North Korea is unique amongst nations with cyberattack capabilities because it devotes so much of its efforts to generating illicit crypto revenue and evading sanctions. Other nations focus their offensive operations on espionage, sabotage, and disinformation campaigns. Pyongyang continues operations in all those categories but, according to the Harvard Kennedy School's 2020 Cyber Power Index, "North Korea was the only country observed pursuing wealth generation via illegal cyber means."[12]

Assessing the North Korean Cybercrimes Threat

As with any criminal activity, it is difficult to assess conclusively 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. Pyongyang may have been unable to convert all its stolen cryptocurrency into traditional currency. Cyber security firm Chainalysis identified $170 million in yet-to-be-laundered funds linked to 49 separate hacks by North Korea from 2017 to 2021.[13]

Even with fully executed cybercrimes, North Korean hackers are unlikely to have converted crypto to cash at full value, instead having to accept a lower percentage because brokers will take a cut of the profits. Governments and cybersecurity firms have been able to claw back some stolen cryptocurrency from North Korea by gaining access to the North Korean cyber accounts before the hackers cashed out the cryptocurrency. For example, North Korea hackers stole $275 million from the KuCoin currency exchange in 2020, and KuCoin's CEO stated that the exchange recovered $204 million of the stolen funds.[14]

North Korean cybercrimes likely also suffered from the global downturn in cryptocurrency markets. The $170 million that Pyongyang stole from 2017 to 2021 but had not cashed out would have decreased in value to $65 million by 2022.[15] The $625 million stolen in 2022 from the Ronin Network would have devalued to about $250 million.[16]

Despite these uncertainties, North Korea's cybercrimes have proven a boon for the regime—and if nothing else the expansion of this activity suggests that it is working. In October 2022, Secretary of Homeland Security Alejandro Mayorkas stated that "in the last two years alone, North Korea has largely funded its weapons of mass destruction programs through cyber heists of cryptocurrencies and hard currencies."[17] In May 2023, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger estimated that approximately half of North Korea's missile program has been funded through cyberattacks and cryptocurrency theft.[18]

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.[19] In 2020, 2021, and 2022, North Korea is estimated to have stolen at least $316 million,[20] $400 million,[21] and $1.7 billion[22] worth of cryptocurrency, respectively.

Major North Korean crypto heists include:

- 2018: $532 million stolen from Japanese firm Coincheck.[23]
- 2018: Nearly $250 million worth of digital currency stolen from an undisclosed digital currency exchange.[24]

- 2020: $275 million stolen from South Korean KuCoin currency exchange. (The company's CEO declared that the exchange has recovered $204 million of the stolen funds.)[25]

- 2022: $620 million stolen by penetrating the Ronin Network, which supports Axie Infinity, a crypto token–based online video game that enables its 2.5 million participants to accumulate cryptocurrency.[26] This was the largest crypto heist in the world to date.

- 2022: $100 million in cryptocurrency stolen from Harmony's Horizon Bridge blockchain bridge service that allows users to transfer cryptocurrency across different blockchains.[27]

- 2023: An estimated $100 million in cybercurrency stolen from Atomic Wallet, a cryptocurrency wallet provider;[28] $60 million stolen from Alphapo, a crypto payment provider;[29] and $37 million stolen from CoinsPaid, a crypto payment platform.[30]

For context: North Korea's total gross domestic product in 2019 was $29 billion.[31] In 2022, Pyongyang's total legitimate international trade was $1.59 billion, *less* than its gains that year from cybercrimes.[32]

The North Korean cyber threat is increasing and evolving. The South Korean National Intelligence Service assessed that 1.37 million daily cyberattacks took place in South Korea during the first half of 2023, more than double the previous six months. North Korea was assessed as responsible for 70 percent of those attacks, followed by China with 4 percent, and Russia with 2 percent.[33] The Mandiant cybersecurity firm tracked more than 10 million non-fungible token–related phishing scams successfully delivered to cryptocurrency users since 2022 and determined that most of those were linked to North Korea.[34]

North Korea has started attacking the global cryptocurrency supply chain. Whereas Pyongyang had previously targeted crypto companies one at a time, it now seeks to compromise software or service providers to gain access or digital currencies from users downstream.[35]

The South Korean National Police Agency declared that North Korea targeted as many as 10 million users across 61 organizations that had downloaded a banking security application. The North Korean hackers altered software by Initec, a major financial security provider, then created a "watering hole attack" by infecting websites that users downloading that software would likely visit. Doing so triggered malware to be loaded onto their computers.[36]

North Korea also penetrated JumpCloud, an American IT management company, to gain access to its cryptocurrency company clients.

North Korean hackers have targeted investment banking and venture capital firms in the U.S, Japan, and Vietnam to gain access to the firms' computers and customer information.[37] Pyongyang has also impersonated venture capital firms in Japan, the U.S., and other countries to then target start-up companies with phishing e-mails or watering hole attacks.[38]

North Korea's Other Cyber Cash Cow: Overseas IT Workers

U.N. Security Council Resolution 2397 (adopted in December 2017) required U.N. 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 Belarus, China, Malaysia, the Philippines, Russia, and Singapore.[39] The North Koreans use false foreign identities to fraudulently gain employment as freelance computer engineers with technology and virtual currency companies located in Asia, Europe, and North America.

Some North Korean IT workers can each earn more than $300,000 per year with 90 percent of the wages going to the regime.[40] Overall, the program generates hundreds of millions of dollars annually for the regime to fund its nuclear and missile programs.[41]

Most of the North Korean IT workers are likely engaged in non-hacking 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 that enable them to launder illicitly obtained funds back to North Korea.[42]

Some North Korean workers, however, have engaged in malicious cyber activities by utilizing their access through foreign companies where they are employed. The South Korean government identified that a significant percentage of the North Korean IT workers are subordinate to entities that have been designated for sanctions under U.N. Security Council resolutions, such as the Munitions Industry Department and Ministry of National Defense.[43]

U.S. and South Korean Responses 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 measures to combat North Korea's cyberattack strategies.[44]

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

What Washington Should Do

In order to crack down on North Korean cybercrime, Washington should:

Enhance Engagement with International Partners. The U.S. should expand coordination 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 Senior Cyber Group committed to greater sharing of information and technology with regional partners to strengthen preventive measures against malicious cyberattacks and improve response capabilities.[45]

Sanction Any Entities Assisting North Korean Cybercrimes. Washington should make sure 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. The Departments of the Treasury and Justice should target banks, financial institutions, and front companies that are used to launder money stolen by North Korea. Successive U.S. Administrations have inexplicably refrained from imposing sanctions on Chinese banks for laundering North Korean illicit funds.

The United States should apply secondary sanctions on any entity supporting North Korean cybercrimes and malicious cyber activity, including providing technology, equipment, training, and safe haven to North Korean hackers. Washington could thus pressure China and other nations to dismantle North Korean hacking networks on their soil.

Similarly, Internet service providers and telecommunications companies should be required to exercise due diligence against cybercrime. Those that do not should also lose their protections against civil liability.

Target North Korean Overseas IT Workers. U.N. 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.[46]

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.

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. This exception should not waive foreign sovereign immunity for state-directed espionage against the U.S. government, but only with respect to state-sponsored cyberattacks intended to cause commercial harm, property damage, personal injury, an invasion of privacy against a private person, or any change in the conduct of a private person.

Similarly, Congress should enact a limited waiver of nonliability provisions, such as section 230 of the Communications Decency Act, allowing 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 allowed to sue state-sponsored hackers to obtain civil judgments against hackers and their state sponsors for cyberattacks on U.S. critical infrastructure.[47] 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.

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. The U.S. should work with other nations to provide similar enforcement overseas.

Congress could grant an appropriate federal 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. The legislation would be similar to existing laws prohibiting material support to terrorists, such as 18 U.S. Code §§ A, B, and C.[48]

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 licit international financial network. Pyongyang's cybercrimes provide a means for North Korean cyber hackers to circumvent sanctions and undermine international measures 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.

Bruce Klingner is Senior Research Fellow in the Asian Studies Center at The Heritage Foundation.

Appendix

Compendium of Recent U.S. and South Korean Law Enforcement Actions Against North Korean Cyber Threats

This appendix provides an update to a 2021 *Special Report* by the author.[49]

U.S. Actions

February 2021. The U.S. indicted three North Korean hackers for participating in a

> wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of money and cryptocurrency from financial institutions and companies, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform.[50]

Washington also charged a Canadian–American citizen with engaging in several money-laundering operations for North Korea.[51]

April 2022. A U.S. court sentenced Virgil Griffith, an American cryptocurrency expert, to 63 months in prison for making an unauthorized trip to North Korea to teach North Koreans how to use cryptocurrency and blockchain technology to launder money and evade U.S. sanctions.[52]

May 2022. The U.S. issued its first sanctions against a virtual currency mixer. Washington cited the firm Blender for providing support to North Korean malicious cyber activities and money laundering of stolen virtual currency. Blender had more than $20.5 million of the $620 million stolen from the Ronin Network by North Korea hackers.[53]

July 2022. The FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of the Treasury released a joint cybersecurity advisory to highlight North Korean hackers infecting U.S. hospital computer systems with ransomware to freeze company files until a payment was made.[54]

August 2022. The Department of the Treasury sanctioned virtual currency mixer Tornado Cash for laundering more than $7 billion worth of virtual currency since its creation in 2019. The company laundered $455 million stolen by the North Korean Lazarus Group, $96 million from the June 2022 Harmony Bridge Heist, and at least $7.8 million from the August 2, 2022, Nomad Heist.[55]

September 2022. The Department of Justice and the FBI announced the recovery of more than half a million dollars in ransom payments from disrupting North Korean ransomware operations targeting U.S. medical facilities.[56]

September 2022. The FBI and cryptosecurity companies were able to seize more than $30 million worth of cryptocurrency stolen from the Ronin Network by North Korea–linked hackers.[57]

March 2023. U.S. and European authorities sanctioned cryptocurrency platform ChipMixer for laundering more than $3 billion of criminal proceeds, including $700 million stolen by North Korean hackers from the Ronin Network and Harmony technology company.[58]

April 2023. The U.S. charged a North Korean Foreign Trade Bank representative for cryptocurrency money-laundering conspiracies on behalf of North Korea. The representative used stolen funds from virtual currency exchange hacks to make payments in U.S. dollars to buy goods for North Korea. He also conspired with North Korean IT workers to generate and launder revenue from illegal employment at blockchain development companies in the United States.[59]

April 2023. The U.S. Department of the Treasury's Office of Foreign Assets Control sanctioned three individuals operating in China for facilitating North Korean cryptocurrency money laundering used to fund weapons of mass destruction and missile programs.[60]

May 2023. The Treasury Department sanctioned four entities and one individual linked to North Korean hacking and IT scams. The U.S. designated Pyongyang University of Automation for providing training for Reconnaissance General Bureau (RGB) intelligence assets, along with two other RGB-controlled operation centers (the Technical Reconnaissance Bureau and the 110th Research Center) conducting offensive cyber operations. The Treasury Department also sanctioned Chinyong Information Technology Cooperation Company and Kim Sang Man for assisting North Korean IT workers in falsifying identities to work overseas in defiance of a U.N. resolution.[61]

South Korean Actions

February 2023. South Korea sanctioned seven North Korean entities and four individuals that raised funds for the regime's nuclear and missile programs. These were Seoul's first independent sanctions targeting North Korean cyber activities. The entities were the Chosun Expo Joint Venture, Lazarus Group, Bluenoroff, Andariel, the RGB's Technology

Reconnaissance Team, the Unit 110 hacking group, and the Pyongyang University of Automation.[62]

June 2023. South Korea sanctioned North Korean hacking group Kimsuky, the first government to do so. As of June 2023, the South Korean government had sanctioned 43 individuals and 45 organizations linked to North Korea's illicit cyber activities.[63]

Coordinated U.S.–South Korean Actions

May 2022 Summit in South Korea. Presidents Yoon and Biden committed to "significantly" expanding bilateral cooperation to confront North Korean cyber threats and to reinforce alliance deterrence against the North's destabilizing activities.

August 2022. The U.S. and South Korea agreed to upgrade cyber cooperation and regularize combined cyber exercises. South Korea's Cyber Operations Command and the U.S. Cyber Command signed a memorandum of understanding on "cooperation and development in cyberspace operations."[64]

October 2022. South Korea participated in the U.S.-led Cyber Flag multinational cyber exercise for the first time and agreed to regularly participate.

April 2023 Summit in Washington. Presidents Yoon and Biden established a bilateral Strategic Cybersecurity Cooperation Framework to "expand cooperation on deterring cyber adversaries, increase the cybersecurity of critical infrastructure, combat cybercrime, and secure cryptocurrency and blockchain applications." The two leaders committed to expanding information sharing to combat North Korean cyber threats and block its cyber-enabled revenue generation.[65]

April 2023. The U.S. and South Korea simultaneously sanctioned Sim Hyon-sop, a North Korean banking official, for financing the regime's nuclear and missile programs through illegal cyber activities. Sim also laundered millions of dollars, including cryptocurrency, earned by North Korean IT workers illegally working overseas using false identities.[66]

May 2023. South Korea and the U.S. jointly announced sanctions on seven North Koreans and three organizations responsible for overseeing North Korean IT workers illegally earning and laundering money overseas.[67]

June 2023. The U.S. and South Korea created the first joint cybersecurity guidance to link South Korea's Allied Korea Joint Command and Control System and the U.S. Combined Enterprise Regional Information Exchange System–Korea. The guidance will establish cybersecurity standards and procedures.[68]

Endnotes

1. Daniel Russel, "The North Korean Crisis Just Around the Corner," *The Japan Times*, October 19, 2022, https://www.japantimes.co.jp/opinion/2022/10/19/commentary/world-commentary/north-korea-nuclear-ambitions/ (accessed September 12, 2023).
2. "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 (accessed August 7, 2023).
3. Kong Ji-young, Lim Jong-in, and Kim Kyoung-gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," in Tomáš Minárik et al., eds., *11th International Conference on Cyber Conflict: Silent Battle*, Tallinn, Estonia, May 28–31, 2019, p. 143, https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf (accessed September 12, 2023).
4. 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 (accessed August 7, 2023).
5. 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 (accessed August 7, 2023).
6. 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/ (accessed August 7, 2023).
7. 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 (accessed August 7, 2023).
8. "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 (accessed August 7, 2023).
9. North Korea uses a broad coalition of government organizations and affiliated hacking groups to conduct illicit and malicious cyber activities. While organizations have specified missions, there appear to be overlapping responsibilities as well as changing tasks over time. Identifying the specific North Korean group responsible for a cyberattack is complicated by the shadowy nature of covert cyber groups as well as different naming protocols used by U.S. government agencies and private cybersecurity firms. This *Backgrounder* generically refers to "North Korean hackers" rather than identifying specific groups. For a detailed description of North Korean government agencies and subordinate groups conducting cyber operations, see Bruce Klingner, "North Korean Cyberattacks: A Dangerous and Evolving Threat," Heritage Foundation *Special Report* No. 247, September 2, 2021, https://www.heritage.org/sites/default/files/2021-09/SR247.pdf.
10. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, August 28, 2020, p. 43, https://undocs.org/S/2020/840 (accessed August 7, 2023).
11. Shannon Vavra, "Cash-Starved North Korea Eyed in Brazen Bank Hack," *The Daily Beast*, November 22, 2021, https://www.thedailybeast.com/cash-starved-north-korea-eyed-in-brazen-bank-rakyat-indonesia-hack (accessed August 7, 2023).
12. Alex O'Neill, "Cybercriminal Statecraft: North Korean Hackers' Ties to the Global Underground," Harvard Kennedy School Belfer Center for Science and International Affairs, March 2022, https://www.belfercenter.org/sites/default/files/files/publication/Cybercriminal%20Statecraft%20-%20Alex%20O%27Neill.pdf (accessed August 7, 2023).
13. Chainalysis, "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/ (accessed August 7, 2023).
14. 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 (accessed September 14, 2023).
15. 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/ (accessed August 7, 2023).
16. 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 (accessed August 7, 2023).
17. 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 (accessed August 7, 2023).
18. 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 (accessed August 7, 2023).
19. United Nations Security Council, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," August 30, 2019, pp. 4 and 26, http://undocs.org/S/2019/691 (accessed August 7, 2023).
20. United Nations Security Council, "Letter Dated 2 March 2021 from the Panel of Experts Established Pursuant to Resolution 1874 (2009) Addressed to the President of the Security Council," March 4, 2021, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf (accessed August 7, 2023).

21. Chainalysis, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High."
22. Chainalysis, "2022 Biggest Year Ever for Crypto Hacking with $3.8 Billion 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/ (accessed August 7, 2023).
23. 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 (accessed August 7, 2023).
24. U.S. Department of State, U.S. Department of the Treasury, U.S. Department of Homeland Security, and the Federal Bureau of Investigation, "DPRK Cyber Threat Advisory: Guidance on the North Korean Cyber Threat," April 15, 2020, p. 4, https://ofac.treasury.gov/recent-actions/20200415 (accessed September 12, 2023). (Click "issued an advisory" hyperlink in first paragraph to reach the advisory.)
25. 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 (accessed August 7, 2023).
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 (accessed August 7, 2023).
27. 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 (accessed August 7, 2023).
28. 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 (accessed August 7, 2023).
29. Tom Blackstone, "Alphapo Payment Provider Hack Now Estimated at Over $60M," *Coin Telegraph*, July 25, 2023, https://cointelegraph.com/news/alphapo-payment-provider-hack-estimated-over-60m-on-chain-sleuth (accessed August 7, 2023).
30. Ernestas Naprys, "Crypto Payments Platform CoinsPaid Loses $37M, Points Finger at Lazarus Group," *CyberNews*, July 28, 2023, https://cybernews.com/news/crypto-platform-coinspaid-loses-37m-lazarus-group/ (accessed August 7, 2023).
31. 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 (accessed August 7, 2023).
32. "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 (accessed August 7, 2023).
33. Youn Sang-un and Lee Ho-Jeong, "More North Korean Cyberattacks Likely in Lead Up to General Election," *Korea Joongang Daily*, July 19, 2023, https://koreajoongangdaily.joins.com/2023/07/19/national/northKorea/North-Korea-National-Intelligence-Service-Hacking/20230719195101413.html (accessed August 7, 2023).
34. Tonya Riley, "North Korean Hackers Turn to 'Cloud Mining' for Crypto to Avoid Law Enforcement Scrutiny," *Cyberscoop*, March 28, 2023, https://cyberscoop.com/north-korean-hackers-cloud-mining-cyrptocurrency/ (accessed August 7, 2023).
35. Christopher Bing and Raphael Satter, "North Korean Hackers Breached a US Tech Company to Steal Crypto," Reuters, July 20, 2023, https://www.reuters.com/technology/n-korea-hackers-breached-us-it-company-bid-steal-crypto-sources-2023-07-20/ (accessed September 12, 2023), and Bob Phan, "Security Update Incident Details," JumpCloud, July 12, 2023, https://jumpcloud.com/blog/security-update-incident-details (accessed August 7, 2023).
36. Esther Chung, "North Korean Hacking Group Lazarus Behind Cyber Attack Last Year: Police," *Korea Joongang Daily*, April 18, 2023, https://koreajoongangdaily.joins.com/2023/04/18/national/northKorea/korea-north-korea-hacking/20230418165722642.html (accessed August 7, 2023).
37. Jeff Seldin, "Financial Institutions in US, East Asia Spoofed by Suspected North Korean Hackers," *VOA News*, June 6, 2023, https://www.voanews.com/a/financial-institutions-in-us-east-asia-spoofed-by-suspected-north-korean-hackers/7125085.html#:~:text=A%20report%20published%20Tuesday%20by,hackers%20access%20to%20critical%20systems (accessed August 7, 2023).
38. Derek B. Johnson, "North Korean Hacking Outfit Impersonates Venture Capital Firms," SC Media, December 27, 2022, https://www.scmagazine.com/analysis/identity-and-access/north-korean-hacking-outfit-impersonates-venture-capital-firms (accessed August 7, 2023).
39. 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 (accessed August 7, 2023).
40. News release, "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities," U.S. Department of the Treasury, May 23, 2023, https://home.treasury.gov/news/press-releases/jy1498 (accessed August 7, 2023).
41. South Korean 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 (accessed August 7, 2023).
42. News release, "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities."
43. South Korean Ministry of Science and ICT, "Advisory on the Democratic People's Republic of Korea Information Technology Workers."

44. For a detailed compendium of recent U.S. and South Korean government responses to the North Korean cyber threat, see the appendix to this *Backgrounder*.
45. The American Presidency Project, "Quad Senior Cyber Group Joint Cybersecurity Statement," Joseph R. Biden, February 2, 2023, https://www.presidency.ucsb.edu/documents/quad-senior-cyber-group-joint-cybersecurity-statement (accessed August 7, 2023).
46. 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 (accessed August 7, 2023).
47. 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: H.R. 1607—HACT Act, 117th Congress, https://www.congress.gov/bill/117th-congress/house-bill/1607?s=1&r=5 (accessed August 7, 2023).
48. Cornell Law School Legal Information Institute, "18 U.S. Code § 2339A—Providing Material Support to Terrorists," https://www.law.cornell.edu/uscode/text/18/2339A (accessed September 12, 2023); Cornell Law School Legal Information Institute, "18 U.S. Code § 2339B—Providing Material Support or Resources to Designated Foreign Terrorist Organizations," https://www.law.cornell.edu/uscode/text/18/2339B (accessed September 12, 2023); and Cornell Law School Legal Information Institute, "18 U.S. Code § 2339C—Prohibitions Against the Financing of Terrorism," https://www.law.cornell.edu/uscode/text/18/2339C (accessed August 24, 2023).
49. See Bruce Klingner, "North Korean Cyberattacks: A Dangerous and Evolving Threat," Heritage Foundation *Special Report* No. 247, September 2, 2021, "Appendix 3: U.S. Government Responses to the North Korean Cyber Threat," pp. 35–38, https://www.heritage.org/sites/default/files/2021-09/SR247.pdf.
50. U.S. Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and?utm_source=pocket_mylist (accessed August 7, 2023).
51. Ibid.
52. News release, "U.S. Citizen Who Conspired to Assist North Korea in Evading Sanctions Sentenced to Over Five Years and Fined $100,000," U.S. Department of Justice, April 12, 2022, https://www.justice.gov/opa/pr/us-citizen-who-conspired-assist-north-korea-evading-sanctions-sentenced-over-five-years-and (accessed August 7, 2023).
53. News release, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," U.S. Department of the Treasury, May 6, 2022, https://home.treasury.gov/news/press-releases/jy0768 (accessed August 7, 2023).
54. Cybersecurity and Infrastructure Security Agency, "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector," July 7, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a (accessed August 7, 2023).
55. News release, "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 (accessed August 7, 2023).
56. Ines Kagubare, "North Korea's Increasing Use of Crypto Heists to Fund Nukes Worries US," *The Hill*, August 9, 2022, https://thehill.com/policy/technology/3590126-north-koreas-increasing-use-of-crypto-heists-to-fund-nukes-worries-us/ (accessed August 7, 2023).
57. 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/ (accessed August 7, 2023).
58. Mengqi Sun, "ChipMixer Is Shut Down for Allegedly Laundering $3 Billion in Crypto," *The Wall Street Journal*, March 15, 2023, https://www.wsj.com/articles/chipmixer-is-shut-down-for-allegedly-laundering-3-billion-in-crypto-325a55ee (accessed August 7, 2023).
59. News release, "North Korean Foreign Trade Bank Representative Charged in Crypto Laundering Conspiracies," U.S. Department of Justice, April 24, 2023, https://www.justice.gov/opa/pr/north-korean-foreign-trade-bank-representative-charged-crypto-laundering-conspiracies (accessed August 7, 2023).
60. News release, "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," U.S. Department of the Treasury, April 24, 2023, https://home.treasury.gov/news/press-releases/jy1435 (accessed August 7, 2023).
61. News release, "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities," U.S. Department of the Treasury, May 23, 2023, https://home.treasury.gov/news/press-releases/jy1498 (accessed August 7, 2023).
62. Shreyas Reddy, "South Korea Issues First-Ever Cyber Sanctions Against North Korea," NK News, February 10, 2023, https://www.nknews.org/2023/02/south-korea-issues-first-ever-cyber-sanctions-against-north-korea/#:~:text=The%20South%20Korean%20government%20announced,sanctions%20targeting%20DPRK%20cyber%20activities (accessed August 7, 2023).
63. Esther Chung, "Seoul Sanctions North Korean Hacking Group Kimsuky," *Korea Joongang Daily*, June 2, 2023, https://koreajoongangdaily.joins.com/2023/06/02/national/northKorea/korea-north-korea-hacking/20230602095559808.html (accessed August 7, 2023).
64. Ji Da-gyum, "S. Korea, US Agree to Upgrade Cyber Cooperation, Regularize Cyber Exercises," *The Korea Herald*, August 18, 2023, https://www.koreaherald.com/view.php?ud=20220818000752 (accessed August 7, 2023).

65. The White House, "Leaders' Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea," April 26, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/leaders-joint-statement-in-commemoration-of-the-70th-anniversary-of-the-alliance-between-the-united-states-of-america-and-the-republic-of-korea (accessed August 7, 2023).
66. Chae Yun-hwan, "S. Korea, U.S. Simultaneously Sanction N. Korean Involved in WMD Financing," Yonhap News Agency, April 24, 2023, https://en.yna.co.kr/view/AEN20230424008700325 (accessed August 7, 2023).
67. Choi Si-young, "S. Korea, US Sanction N. Korean IT Workers," *The Korea Herald*, May 23, 2023, https://www.koreaherald.com/view.php?ud=20230523000776 (accessed August 7, 2023).
68. "S. Korea, US Craft 1st Cybersecurity Guidance," *The Korea Herald*, June 2, 2023, https://www.koreaherald.com/view.php?ud=20230602000470#:~:text=of%20National%20Defense)-,South%20Korea%20and%20the%20United%20States%20signed%20an%20arrangement%20Friday,operations%2C%20Seoul's%20defense%20ministry%20said (accessed August 7, 2023).