The Heritage Foundation

SPECIAL REPORT
No. 247 | SEPTEMBER 2, 2021

North Korean Cyberattacks: A Dangerous and Evolving Threat

Bruce Klingner

The Heritage Foundation

North Korean Cyberattacks: A Dangerous and Evolving Threat

Bruce Klingner

SPECIAL REPORT

No. 247 | SEPTEMBER 2, 2021

ASIAN STUDIES CENTER

About the Author

Bruce Klingner is Senior Research Fellow for Northeast Asia in the Asian Studies Center, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

This paper, in its entirety, can be found at **http://report.heritage.org/sr247**

The Heritage Foundation | 214 Massachusetts Avenue, NE | Washington, DC 20002 | (202) 546-4400 | heritage.org

North Korean Cyberattacks: A Dangerous and Evolving Threat

Bruce Klingner

North Korea has conducted cyber guerrilla warfare to steal classified military secrets, absconded with billions of dollars in money and cybercurrency, held computer systems hostage, and inflicted extensive damage on computer networks. Defending against Pyongyang's cyberattacks requires the same constant vigilance and rapidly evolving methods and techniques that law enforcement agencies had to use in response to its evasion of sanctions. The United States has taken only limited actions against North Korean hackers and foreign countries that allow them to operate and launder money from cybercrimes. Without a firm response from the U.S., the North Korean regime will continue to undermine the effectiveness of international sanctions and could inflict even greater damage during a crisis or military conflict.

North Korean missiles and nuclear weapons have garnered fear, international condemnation, and tough sanctions. Pyongyang's cyber activities, however, have elicited less reaction and punishment despite having been used repeatedly in attacks against governments, financial institutions, and industries.

The attitude of experts toward North Korea's cyber capabilities was initially dismissive, just as their reaction to the regime's nuclear and missile programs had been.[1] Many, pointing to the famous nighttime satellite imagery of northeast Asia with a dark North Korea surrounded by the blazing lights of its neighbors, did not believe that the technologically backward regime was capable of sophisticated cyberattacks.

Nevertheless, although the regime fails to provide technological comforts for its populace, Pyongyang developed an advanced cyber warfare prowess that is surpassed by few nations. From initial rudimentary distributed

denial-of-service (DDoS) attacks against South Korea, the regime improved its cyber programs to create a robust and global array of disruptive military, financial, and espionage capabilities.

As its cyber proficiencies evolved, Pyongyang implemented ever more sophisticated techniques and prioritized financial targets to evade international sanctions and augment the regime's coffers for its nuclear and missile programs. Although it appears to have de-emphasized cyber operations against military and infrastructure targets in recent years, the regime previously alluded to attacking allied info-centric warfare strategies and civilian networks during a crisis.

The scope of North Korea's demonstrated cyber capabilities and the severity of other recent cyberattacks, such as the Russian-sponsored SolarWinds hack, Chinese exploitation of Microsoft Exchange vulnerabilities, and DarkSide malware shutting down of the Colonial Pipeline, demonstrate the continued critical vulnerability of the government, financial, infrastructure, and corporate sectors. 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.

Cyber: A Key Component of North Korean Strategy

Pyongyang has developed a comprehensive and sophisticated arsenal of cyberattack tools and methods. In 2017, senior U.S. intelligence officials assessed that North Korea was one of the top four cyber threats capable of launching "disruptive or destructive cyberattacks" against the United States.[2] The Director of Central Intelligence warned in January 2019 that North Korea "poses a significant cyber threat to financial institutions, remains a cyber-espionage threat, and retains the ability to conduct disruptive cyber attacks."[3]

North Korea's cyber weapons and tactics are consistent with the regime's asymmetric military strategy. As North Korea's conventional military forces deteriorated in comparison with those of the United States and South Korea, Pyongyang developed new weapons to counter the growing gap in capabilities, including nuclear weapons, missiles, and long-range artillery.

After studying U.S. military operations in Iraq, North Korean leader Kim Jong-il concluded that allied high-tech warfare was vulnerable to cyberattacks and that "in the 21st century, war will be [fought as] information

warfare."[4] Kim opined that "cyber attacks are like atomic bombs" and that "[w]ar is won and lost by who has greater access to the adversary's military technical information in peacetime."[5]

North Korean strategists see cyberspace as an integral part of its military strategy, designating it "the fifth major battlefield" along with ground, air, sea, and space.[6] By 2009, Kim declared that North Korea was "fully ready for any form of high-tech war."[7] The South Korean Ministry of Defense warned that North Korea was able to disrupt Global Position System (GPS) networks and was developing the means to jam high-tech missiles and precision-guided bombs.[8]

Kim Jong-il initiated North Korea's foray into cyber warfare, but it was during Kim Jong-un's reign that Pyongyang accelerated and expanded its cyberattacks on a broader spectrum of targets. Since 2010, North Korea is believed to have jammed the GPS systems of planes over Incheon Airport; stopped the release of a major motion picture in the United States; hacked into South Korean banks, newspapers, and nuclear power plants; and defrauded banks and cybercurrency exchanges to gain billions of dollars.

"With intensive information and communication technology, and the brave Reconnaissance General Bureau (RGB) with its [cyber] warriors," Kim declared in 2013, "we can penetrate any sanctions for the construction of a strong and prosperous nation."[9] It is noteworthy that even then, Kim highlighted the financial sanctions–evading aspect of cyber operations.

Kim Jong-un declared that cyber warfare is a "magic weapon"[10] and an "all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles."[11] In the run-up to a crisis or as an alternative to kinetic strikes, the regime could conduct cyberattacks on government and civilian computer networks that control communications, finances, and infrastructure such as power plants and electrical grids.

Cybercrime: New Methods for Old Strategy

North Korea's cyber operations are consistent not only with its asymmetric military strategy, but also with the regime's 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. There have been very few United Nations (U.N.) or U.S. sanctions imposed or legal actions taken against North Korean cyber groups. Cybercrime is especially beneficial to the regime as it faces the cumulative effects of international sanctions and the impact of self-imposed COVID restrictions on legal and illicit foreign trade, as well as natural disasters in the agricultural heartland and decades of devastating socialist economic policies.

Cybercrime Eclipsing Traditional Crimes. As the international community cracked down on North Korea's various criminal endeavors, the beleaguered regime shifted toward new ways to gain money. Cyber operations are now a greater component of North Korean criminal activities than earlier, more traditional "bricks and mortar" endeavors such as counterfeiting and smuggling. North Korea's hackers "have become the world's leading bank robbers," in the words of John Demers, head of the National Security Division of the U.S. Department of Justice. "Simply put, the regime has become a criminal syndicate with a flag, which harnesses its state resources to steal hundreds of millions of dollars."[12]

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 August 2019, the U.N. Panel of Experts estimated that North Korea had cumulatively gained $2 billion from cybercrime.[13] For comparison, in 2019, North Korea legally imported $2.7 billion in assorted civilian merchandise, mostly from China,[14] and its annual gross domestic product (GDP) was $29 billion.[15]

A South Korean organization has estimated that North Korean cybercrimes generate an annual revenue of $860 million,[16] but others assess that Pyongyang may gain $1 billion a year—a third of the value of the nation's exports—from cyber heists.[17] During 2017–2018, North Korea was estimated

to account for 65 percent of all global cybercrime.[18] One regime hacking unit, the Lazarus Group, is assessed to have gained more than $1.75 billion worth of cryptocurrency.[19]

In September 2018, a grand jury issued an indictment of North Korean cyber operative Park Jin-hyok for attempted cyber heists and extortions in Asia, Africa, North America, and South America totaling $1.3 billion during 2015–2018.[20] In 2020, the U.S. Department of Justice declared that North Korean hacking of virtual currency exchanges and related money laundering "poses a grave threat to the security and integrity of the global financial system."[21]

North Korean Cyber Agencies

Pyongyang has an expansive array of government organizations and affiliated hacker groups conducting malicious cyber operations.[22] Organizations appear to have specified missions, although there also appear to be overlap or changes in mission over time. The shadowy nature of covert cyber groups, as well as fragmentary and conflicting information, makes a definitive understanding difficult.

The predominant government organizations for cyber operations are the Reconnaissance General Bureau and the General Staff Department. Both are subordinate to the State Affairs Commission,[23] which is chaired by Kim Jong-un, and have numerous subordinate units. Other government units include the State Security Department and the Defense Commission.

In additional to government agencies, numerous affiliated North Korean hacker groups are conducting attacks against government, financial, infrastructure, and other sectors. These groups include:

- Andariel;
- BeagleBoyz;
- Bluenoroff;
- The Chollima groups;
- Dark Hotel;
- Group 123;

- The Kimsuky group;
- Lazarus (also known as APT38);[24]
- Reaper (also known as APT37 and Thallium); and
- Starcraft.

The U.S. government refers to the North Korean government's malicious cyber activity collectively as Hidden Dragon.

North Korea's Illicit Cyber Operations

Cyber operations provide new methods and tools that Pyongyang can use to fulfill its long-standing objectives of espionage, disruptive and destructive operations, extortion and terrorism, illicit money-making activities, and evasion of sanctions. North Korean hackers have penetrated computer networks to:

- Collect intelligence on and steal secrets from defense, military technology, intelligence, financial, nuclear, and pharmaceutical targets;
- Disrupt, damage, and destroy computer systems through DDoS attacks;
- Deploy ransomware to encrypt data or files to hold computer systems hostage until extortion payments or other demands were met, sometimes in conjunction with violent physical attacks, as well as running cyber protection rackets whereby North Korean cyber groups will refrain from attacking entities in return for payment;
- Retaliate against opponents of the regime or those who demean North Korean leaders; and
- Illegally acquire and launder stolen money to evade sanctions and raise funds for the cash-strapped regime by cyberattacking banks, financial institutions, cryptocurrency exchanges, and the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network.[25]

Tactics, Techniques, and Procedures

North Korean hackers are adept at developing sophisticated cyber coding to gain access even to well-protected government, military, and financial computer networks. They are also astute at exploiting human vulnerabilities through social engineering methods to trick victims into uploading malware that compromises network security.

Hackers seek access in much the same way that intelligence agencies recruit human assets. Like intelligence agencies, they ascertain the information and organizations that would achieve government-directed objectives, conduct reconnaissance to identify individuals that could provide access to that information, assess vulnerabilities and the means by which to exploit them, and determine which methods they can use to exfiltrate the data.

North Korea often delivers malware through spear-phishing emails targeted at people who can provide either direct or tertiary access to a target network. While many of these attempts are variants on "please click on the (infected) attachment," the means employed to allay the target's suspicions have become increasingly clever. The hackers use "spoofing" tactics to disguise an email, social media account, or website so that it appears to be from a recognized reliable source so that the target will unwittingly upload malware. The approaches are often individually customized and highly profiled, using personal information either about the target or about individuals or organizations that the target would trust.

In Operations Dream Job, In(ter)ception, North Star, and WannaJob, North Korea targeted Australian, Indian, Israeli, Russian, South Korean, and U.S., defense and aerospace experts to gain classified or proprietary information by using fake job offers from defense contractors as lures to install data-gathering implants on the victims' systems. The cyber groups impersonated job recruiters by creating fictitious WhatsApp, Facebook, and LinkedIn profiles of legitimate companies and even conducted extensive dialogue through email and phone calls.

Similar techniques were used against employees of banks, companies, and other organizations to gain access to computer networks.[26] North Korean groups will mimic colleagues, friends, journalists, or Korea-related organizations to gain access to a victim's computer and then use acquired information or contact lists to conduct follow-on approaches.[27] The groups have even commissioned experts to write papers that were then used as bait when targeting other experts.[28]

Hackers and intelligence agencies also welcome targets that offer themselves as sources. A "walk-in" intelligence source walks into an embassy or

otherwise contacts a government source to volunteer his or her services without having been previously targeted. Hackers conduct "watering hole" attacks by either infecting or creating websites that potential sources are likely to visit.

The hackers can create infected documents or links and wait for someone to arrive and unknowingly take the bait. In 2017, North Korean hackers infected the website of the Polish Financial Supervision Authority with malware that was programmed to download to computers that visited the site only if they were from 104 preselected financial institutions and telecommunications companies.[29]

Once a source has provided access, the available information, including information on possible access to other potential targets, is investigated and vetted for its usefulness. North Korean hackers may spend nine to 18 months conducting reconnaissance, elevating user privileges, and disabling security procedures before attempting to execute a cybertheft. North Korean hackers are seen as unique in their willingness to destroy large amounts of data to cover their tracks or distract targets while a theft is in process.[30]

North Korea's Evolving Cyber Operations

Pyongyang's cyberattacks developed through several phases.[31] Initially, the regime focused on cyber espionage to steal information and cyberattacks to disrupt or destabilize networks related to national defense, nuclear power plants, infrastructure, telecommunications, media, and corporations. Early cyber operations were a form of "reconnaissance by fire" to test preliminary capabilities against opponents' defenses and may have served as proof of concept for far more extensive and crippling operations to be used in a time of military conflict or major crisis.

As North Korea improved the scope, scale, and sophistication of its cyber operations, it progressed through phases of cyberterrorism, revenge attacks, and extortion; cyber bank robbery; cryptocurrency exchanges and decentralized finance (DeFi) platforms; and (after the onset of COVID) pharmaceutical companies. The initiation of a new phase did not curtail cyberattacks prevalent in previous phases, although their scope and prioritization might have changed. For example, cyberespionage operations continued after Pyongyang initiated cybercriminal activities to generate revenue.

In 2015, North Korea began cyber robbery operations 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. After the international community took notice of these attacks, the regime shifted to targeting cryptocurrency exchanges. 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" with stronger cyber protections.[32]

Potential North Korean Cyber Actions During a Crisis

North Korea has proven to be adept at deeply penetrating even highly secure computer networks of governments, militaries, banks and international financial transaction systems, and critical infrastructure targets. More worrisome, however, is the possibility that Pyongyang could inflict even greater damage during a crisis or hostilities on the Korean Peninsula. These attacks indicate that Pyongyang has the potential to engage in cyber warfare with disproportionately massive impact—in other words, to create a cyber 9/11.

North Korea could paralyze critical infrastructure systems such as communications, dams, electrical grids, hospitals, nuclear power plants, supply chains, and traffic-control systems. North Korean hackers have targeted railroad companies and airlines, including an automated operating system that controls trains' speed. Hackers have already jammed airline GPS signals and might seek to gain control of airplane controls.[33]

In 2013, South Korea's National Intelligence Service (NIS) revealed that Pyongyang had developed a Trojan program to take over computer networks and power supply systems, chemical materials facilities, oil storage terminals, water treatment stations, and subway networks throughout South Korea. The NIS indicated that the regime had recorded the geographic coordinates of South Korean chemical materials facilities, oil storage terminals, water treatment stations, and power plants and that it had collected information on power substations, subway networks and elevated roadways in major cities, tunnels, bridges, and railroad stations.[34]

In 2017, North Korea attempted to use spear-phishing emails to gain entry into U.S. electric companies as an early-stage reconnaissance operation. Computer security firm FireEye reported that the hackers failed to gain access at that time to computer systems or industrial control systems that regulate the supply of power.[35] Nevertheless, the U.S. government has warned that North Korea's illicit cyber activities "threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity and stability of the international financial

system," in addition to which "[t]he DPRK has the capability to conduct disruptive or destructive cyber activities affecting U.S. critical infrastructure."[36]

Pyongyang could engage in economic warfare to steal massive amounts of money or undermine the stability of the international financial system or worldwide markets. The regime could conduct ransomware attacks on banks to gain money or to disable or destroy computer networks as well as flood the SWIFT system with fraudulent transactions. In 2019, more than 11,000 SWIFT member institutions worldwide sent approximately 33.6 million transactions per day through the network.[37]

What the United States Should Do

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.

Washington needs to make addressing this threat a national priority by establishing a comprehensive whole-of-government strategy, to be coordinated with other governments as well as the private sector. The U.S. should fully enforce existing laws and assess whether additional legislative and executive actions are needed, including enhanced regulations of cybercurrency exchanges and DeFis. Washington should determine a range of punitive steps, both cyber and kinetic, for responding to attacks deemed detrimental to national security.

Specifically, Washington should:

- **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. These reports should be submitted to appropriate committees in Congress.

  The U.S. should also continue to issue threat advisories that provide detailed technical details of North Korean cyber organizations, recent cyberattacks, ways to evade cyber defenses, and money laundering in order to alert government and private-sector entities to take appropriate actions to improve cyber defenses. Widespread public dissemination of threat information and private contacts with other governments as well as banks, financial institutions, and companies

enable the sharing of more detailed information while still protecting classified sources and methods.

- **Create a comprehensive national strategy to combat cyber threats.** Addressing North Korea's cyber threat should be a national priority that requires a comprehensive whole-of-government response that uses all of the instruments of national power. Given the expansive nature of Pyongyang's cyber operations, the effort should be directed by the White House and should include, at a minimum, the Departments of Treasury, Justice, Defense, Commerce, and Homeland Security as well as the Intelligence Community.

  It is encouraging that the 2021 National Defense Authorization Act created the position of National Cyber Director to serve as principal adviser to the President on cyber policy. Chris Inglis, a 28-year veteran of the National Security Agency, was confirmed in June 2021 to lead coordination of U.S. cybersecurity policy and strategy implementation; oversee efforts to increase cybersecurity and deter malicious cyber activity; coordinate the federal response to cyberattacks; engage with the private sector; engage in diplomatic efforts to develop norms of and international consensus on responsible state cyber behavior; and support "the integration of defensive cyber plans and capabilities with offensive cyber plans."[38] Also encouraging was President Biden's announcement that he would "make cybersecurity a top priority at every level of government...further strengthen partnerships with the private sector, and expand our investment in the infrastructure and people we need to defend against malicious cyberattacks."[39]

  However, questions remain with respect to how the National Cyber Director will interact with other senior officials and organizations with direct or indirect cyber responsibilities. Who will have the clout to direct a coherent, comprehensive policy across vast bureaucratic organizations with overlapping responsibilities and conflicting priorities? Without real authority over departments and agencies, the new cyber director could face some of the same problems that plagued the Director of National Intelligence, whose position was created after the 9/11 attack. If bureaucratic turf battles and inertia are to be overcome, the President will have to make clear who has real authority on cyber policy, particularly as it interacts with national security, economic, and law enforcement policies.

- **Coordinate with the private sector.** Extensive sharing of cyber-threat information among and between the public and private sectors is critical for improving defenses against North Korean and other hackers. Collaboration and coordination enable a more comprehensive assessment of weaknesses in government, industry, business, financial, and infrastructure computer networks as well as proposals for innovative technical or methodological fixes. In conjunction with industry, businesses, and financial institutions, Washington should therefore develop, coordinate, and promulgate cyber rules, regulations, security protocols, and best practices to improve cybersecurity and the resilience of networks.

  The Cybersecurity Information Sharing Act[40] authorized the Department of Homeland Security to "encourage robust sharing of useful cybersecurity information among all types of entities—private, Federal, state, local, territorial, and tribal."[41] The new Office of the National Cyber Director will join existing government bodies in engaging with the private sector, and this will increase the potential for competition, confusion, and industry frustration.[42] Care should be taken to delineate responsibilities among government agencies.

  Despite all actions that governments, industries, and banks implement, the weak link will still be the individual employee who inadvertently allows malware to penetrate the system. No matter how strong the castle's defenses are, one person carelessly allowing the drawbridge to drop down undermines all defenses. With that in mind, organizations should explore technical measures that preclude or reduce the downloading of malware. Preventing North Korean cyber intrusions will require both improved technical defenses and effective measures to thwart the regime's sophisticated social engineering techniques that induce individuals to upload malware unknowingly into computer systems.

- **Engage international partners.** U.S. defenses are only as strong as the weakest link overseas. The U.S. should continue and 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. There should also be engagement with foreign financial institutions and businesses to disseminate information on North Korean cyber hacking and money-laundering tactics, techniques, and procedures.

The United States should take the lead in multiple fora to establish and ensure compliance with international cybersecurity standards. Such efforts could take place in existing diplomatic entities, such as the United Nations or G20 forum, led by the White House or State Department, as well as with financial and law enforcement organizations.

1. The U.N. Panel of Experts recommended that financial institutions, including banks and cryptocurrency exchanges, enhance cyber defenses by sharing threat information and best practices through organizations such as the Financial Services Information Sharing and Analysis Center.[43] The Treasury Department's Office of Foreign Assets Control (OFAC) could take the lead on encouraging and facilitating information sharing among law enforcement and financial institutions. The initiative could be modeled on the Treasury Department's Financial Crimes Enforcement Network FinCEN Exchange program to enhance the sharing of information on priority illicit finance threats with financial institutions.[44]

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

3. Given the United States' extensive intelligence collection capabilities and law enforcement expertise, Washington should dispatch teams overseas to engage with foreign government, law enforcement, financial institutions, and private-sector entities to provide targeted information on North Korean cyber programs. The U.S. did this extensively to counter North Korean evasion of sanctions. Those efforts successfully alerted entities that were unaware of North Korean activities and triggered compliance prior to the issuing of formal U.S. punitive measures.

- **Fully enforce laws against illicit activities and cyber operations.** Despite the severity of Pyongyang's cyberattacks, the U.S. government has taken action only against a handful of North Korean actors. Unfortunately, this is consistent with actions by successive U.S. Administrations to limit law enforcement efforts against North Korean, Chinese, and other entities that violate U.S. laws and U.N. resolutions. The U.S. government should take action against North

Korean hackers as well as countries that enable them to operate from their soil or that provide technology, equipment, or training.[45] This can be done by:

1. Fully resourcing the sanctions enforcement effort by dedicating sufficient investigative and enforcement effort to it;

2. Fully enforcing FinCEN regulations that are applicable to crypto-currency transactions by U.S. nationals or within the United States;

3. Prohibiting transactions by U.S. nationals or within the U.S. that involve cryptocurrencies the anonymity of which has facilitated illicit transactions on behalf of North Korea;

4. Amending the North Korea Sanctions and Policy Enhancement Act of 2016[46] to ban transactions in proceeds derived from cryptocurrency that constitute the proceeds of illicit activity or were involved in carrying out illicit activity; and

5. Putting greater pressure on host nations to expel or extradite North Korean hackers, including terminating the U.S. Department of Commerce technology export licenses of nations that fail to do so.[47]

Stronger action could constrain North Korea's ability to gain funding for its prohibited nuclear and missile programs. The Departments of Treasury and Justice should target banks, financial institutions, and front companies that are used to launder money stolen by North Korea. In 2017, the U.S. Congress passed to the Trump White House a list of 12 Chinese banks that were believed to be committing money-laundering crimes in the U.S. financial system. To date, the executive branch has taken no action. In the past, the U.S. imposed $8 billion–$9 billion in fines on European banks that laundered money for Iran, but it has yet to impose any fines on Chinese banks that launder money for North Korea.

Justice Department actions against some North Koreans revealed the extent to which they had moved money illicitly through nine different Chinese banks. The Treasury Department should engage with those banks to discern whether they unwittingly facilitated financial crimes, in which case they should be subject to remedial actions, or were

complicit, in which case they should be fined, labelled money-laundering concerns, and denied access to the U.S. financial system.[48] 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.[49]

In January 2021, Congress enacted the National Defense Authorization Act for fiscal 2021,[50] which includes the Anti-Money Laundering Act of 2020. The statute updates U.S. anti-money laundering laws, significantly expands the U.S. government's authority to subpoena documents held by foreign banks overseas, and codifies a $50,000 daily fine for failing to comply with subpoenas. The act also preserves the government's ability to terminate foreign correspondent accounts in the U.S. financial system, which is a financial "death penalty" for foreign banks that do not comply.[51]

- **Augment regulation of cryptocurrency exchanges.** As banks and financial institutions responded to North Korean cyberattacks, Pyongyang shifted toward cryptocurrency exchanges and DeFis both as targets and as means to launder money. 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.

  The U.N. Panel of Experts recommended that member states should implement Financial Action Task Force standards and "that to manage and mitigate the risks emerging from virtual assets," such assets should be subject to enhanced monitoring and compliance standards.[52] The United States could augment its technical warning notices to include increased emphasis on identifying North Korean attacks, specific actors and their virtual coin "wallets," and techniques used against cryptocurrency exchanges.

- **Determine U.S. responses to North Korean cyberattacks.** The potential for greater and even catastrophic North Korean cyberattacks against the United States, its partners, and the international financial system raises questions about the proper levels of retaliatory or even preemptive actions against the regime. "[A] good defense isn't enough,"

President Biden has commented; "we need to disrupt and deter our adversaries from undertaking significant cyberattacks in the first place. We will do that by, among other things, imposing substantial costs on those responsible for such malicious attacks, including in coordination with our allies and partners."[53]

Given North Korea's limited exposure to cyberattacks, a U.S. or international response would also need to consider non-cyber tools of national power. These include "diplomatic action, cooperation reduction, visa restriction, financial sanctions, legal action, and military action. A consistent pattern of imposing meaningful costs for malicious cyber behavior will strengthen our cyber deterrence if applied consistently, and in some cases, publicly."[54] A military response to a non-military cyberattack would be a difficult decision, particularly given the difficulty of conclusively assigning blame for cyber operations. In 2014, however, NATO leaders agreed that a large-scale cyberattack on a member country would be considered an attack on the entire alliance, potentially leading to the invocation of Article 5 and triggering a military response.[55] Similarly, the United States and Japan agreed in 2019 that in certain circumstances, a cyberattack could constitute an armed attack for the purposes of Article V of the U.S.–Japan Security Treaty.[56]

The United States should consider discussing with other U.N. member nations whether future North Korean cyberattacks should merit a U.N. Security Council resolution and accompanying sanctions, such as those imposed in response to the regime's nuclear and missile tests.[57] North Korean cyber groups that commit cybercrimes to evade sanctions and gain funding for the regime's prohibited nuclear and missile programs could be sanctioned under existing resolutions.

Conclusion

North Korea is a direct threat to the security of the United States, its allies, and the international financial system. Pyongyang continues to augment and refine its nuclear, missile, and cyber threats to the United States and its allies. While its kinetic military attacks have been limited in recent years, the regime has freely engaged in an expansive cyber gray-zone war with much lower risk of retaliation than conventional military actions entail. Pyongyang has conducted cyber guerrilla warfare to steal classified military

secrets, has absconded with billions of dollars in money and cybercurrency, has held computer systems hostage, and has inflicted extensive damage on computer networks.

Defending against North Korean cyberattacks requires constant vigilance and rapidly evolving methods and techniques of the sort that law enforcement agencies had to use in response to Pyongyang's improved tactics for evading sanctions. Complacency or a lack of vigor will leave critical government, military, financial, and industry sectors vulnerable to potentially devastating attacks.

Yet the United States has taken only limited actions against North Korean hackers and foreign countries that allow them to operate and launder money from cybercrimes. Without a firm response from the U.S. to North Korea's hack of Sony and subsequent threat of terrorism, such attacks against the U.S. and its interests will only grow more common.

Appendix 1: North Korean Government Agencies and Subordinate Groups Conducting Cyber Operations

Government Agencies

- **Reconnaissance General Bureau (RGB).** Formed in 2009 during a restructuring of military and intelligence organizations, the RGB is the primary agency responsible for intelligence, clandestine, and terrorist operations. It includes the majority of North Korea's cyber units with an estimated 6,800 "trained cyber-warfare specialists."[58] Subordinate units include:

    1. **Unit 35** (also known as the Central Party Investigative Group), which is responsible for developing malware, identifying opponents' vulnerabilities, and conducting technical education and training.[59]

    2. **Unit 91**, which is responsible for acquiring information and technology on nuclear development and long-range missiles. It has conducted cyberattacks against the South Korean Ministry of Defense and critical national infrastructure targets such as Korea Hydro and Nuclear Power, which operates nuclear and hydroelectric power plants.[60]

    3. **Unit 121** (also known as the Cyber Warfare Guidance Unit), which is North Korea's largest cyber unit and has both intelligence-gathering and attack components.[61] It is responsible for infiltrating computer networks, hacking secret information, and planting viruses to paralyze enemy networks.[62] It is also responsible for attacking infrastructure networks in the transportation, telecommunications, gas, electric and nuclear power, and aviation sectors[63] and may be responsible for Korea Peoples' Army jamming operations[64] and the disabling of South Korean command, control, and communications structures during an armed conflict. Unit 121 oversees Unit 91; Lab 110, which manages Offices 35, 98, and 414; Unit 180; 128 Liaison Office; and 413 Liaison Office.[65]

        a. **Lab 110** conducts cyber intelligence missions and cyberattacks against computer command systems. It is believed to have been responsible for the 2009 DDoS attacks against South Korean

telecommunications targets. The South Korean National Intelligence Service reported that the unit had received orders to "destroy the South Korean communications networks in an instant."[66]

b. **Unit 180** is responsible for hacking international financial institutions to gain foreign currency to support the regime's nuclear and ballistic missile programs.[67] It has shifted its focus to targeting cryptocurrency exchanges.[68]

- **General Staff Department of the Korea Peoples' Army (GSD).** The GSD focuses on the military applications of cyber operations. Its primary cyber goal is to integrate cyber capabilities into North Korea's warfighting strategy. The GSD's cyber responsibilities are divided among its:

  1. **Operations Bureau,** which creates cyber strategy, force planning, and missions.

  2. **Command Automation Bureau,** which conducts cyber warfare operations. Subordinate Units 31, 32, and 56 develop malware development, military software, and command and control software, respectively.

  3. **Enemy Collapse Sabotage Bureau,** which conducts information and psychological warfare.[69]

- **State Security Department Bureau 225.** Bureau 225 produces anti–South Korea propaganda to be disseminated through covert networks in China and Japan as well as hundreds of social media sites. According to South Korea's National Intelligence Service, Pyongyang seeks to manipulate online opinion by posting articles on blogs or sending emails to South Korean journalists.[70] The unit trains agents, conducts infiltration operations in South Korea, and creates underground political organizations in order to incite disorder. It plays a more traditional intelligence and psychological operations role rather than focusing heavily on cyber operations.[71]

- **Defense Commission Psychological Operations Department Unit 204.** Unit 204 engages in cyber-psychological warfare, espionage, and cyberattacks against South Korea and Western targets.[72]

North Korean–Affiliated Hacker Groups

- **Lazarus** is the largest and most prevalent of North Korea's hacker groups. It was created in 2007 and is subordinate to Lab 110 of Bureau 121 of the RGB. It has targeted the aerospace, chemical, electronic, entertainment, financial, government, health care, infrastructure, manufacturing, media, military, publishing, and shipping sectors. It also has targeted North Korean human rights organizations in South Korea and Japan.[73] Lazarus was responsible for many of North Korea's most audacious cyberattacks, including attacks against South Korean banks in 2013, Sony Pictures Entertainment in 2014, and the WannaCry ransomware attack in 2017.

- **Kimsuky** was created in 2012 with a global intelligence-gathering mission. The organization has extensively targeted U.S., South Korean, and Japanese individuals, think tanks, government agencies, and other organizations focused on Korean security issues, nuclear policy, and sanctions. Kimsuky seeks access to computers to gain information through social engineering tactics such as phishing, credential and password harvesting, and watering hole attacks.[74]

- **Reaper (APT38)** targets financial institutions and interbank financial systems to obtain money for the regime. Since 2015, APT38 has been linked to attempts to steal hundreds of millions of dollars from financial institutions, including the Vietnam TP Bank (2015); Bangladesh Bank (2016); Far Eastern International Bank (2017); Bancomext (2018); and Banco de Chile (2018).[75]

- **Andariel** has conducted cyber espionage and cybercrimes against foreign businesses, defense industries, financial institutions, and government agencies since 2015. It has been linked to hacks into ATMs to withdraw cash and steal customer information that it later sells on the black market. Andariel also has developed malware to hack into online poker and gambling sites.[76]

- **Bluenoroff** conducts cyber heists to generate revenue and enable the regime to evade sanctions. The group was first noticed in 2014 as part of Pyongyang's new emphasis on financial targets. Bluenoroff has attempted to steal over $1.1 billion from financial institutions and cryptocurrency exchanges in Bangladesh, India, Mexico, Pakistan,

Philippines, South Korea, Taiwan, Turkey, Chile, and Vietnam.[77] In conjunction with the Lazarus group, Bluenoroff stole $81 million from the Central Bank of Bangladesh's New York Federal Reserve account using stolen SWIFT credentials. An attempt by the two groups to steal an additional $851 million was thwarted by an alert bank officer who noticed a typographical error.

- **Chollima** consists of "four groups, differing in the objectives and methods of attacks:"

  1. **Labyrinth Chollima**, which "focuses on countering intelligence services;"

  2. **Ricochet Chollima**, which steals user data;

  3. **Silent Chollima**, which "acts against the media and government agencies, primarily in South Korea;" and

  4. **Stardust Chollima**, which "specializes in 'commercial attacks.'"[78]

Appendix 2: Compendium of North Korean Cyber Attacks

Phase 1: Espionage and Disruptive/Destructive Attacks

2007

- North Korea's first DDoS attack appears to have been **Operation Flame,** which formed the foundation for subsequent attacks using some of the same identifying encryption keys, malware codes, and techniques.[79]

2008

- Large-scale cyberattacks in South Korea included shutting down 400 computers at the transition office of President Lee Myung-bak.[80]

2009

- **Operation Troy** involved DDOS, espionage, and disk-wiping attacks against South Korean and U.S. government, military, media outlet, and financial websites. Targets included the White House, U.S. Treasury, U.S. Secret Service, and New York Stock Exchange; the South Korean Blue House, Ministry of Defense, and National Assembly; Shinhan Bank and Korea Exchange Bank; and Naver, South Korea's top internet portal. The attacks came from 435 different servers in 61 countries around the world.[81]

2010

- Cyberattacks jammed GPS signals at Seoul's Incheon airport.[82]

2011

- **Operation Ten Days of Rain** targeted 40 South Korean government, media, and financial websites as well as the networks of U.S. Forces Korea and the U.S. Air Force Base in Kunsan. The attack coincided with the annual combined U.S.-South Korea military exercises. The DDoS attacks were highly destructive, requiring a rebuild of operating systems, applications, and user data.[83]

- DDoS attacks on Seoul's Incheon Airport. South Korean police arrested a South Korean game distributor who had met with North Korean RGB agents in China to acquire computer games infected with malware. South Koreans subsequently playing the games unwittingly uploaded the malware onto their computers enabling them to be used as zombie computers in the cyberattack on the airport.[84]

- South Korean police arrested five people for purchasing malware from North Korean hackers to enable illegally gaining points and in-game special items in popular video games that could be converted into real cash. The group was in regular contact with North Korean agents. In less than two years, the group made $6 million, an unknown portion of which was sent to North Korea.[85]

2012

- Large-scale cyberattacks jammed GPS navigation signals for at least 674 commercial air flights and 122 ships, as well as in-car navigation for a week.[86]

- South Korean conservative *JoongAng Ilbo* newspaper was attacked and its photo and article databases destroyed. North Korea had previously denounced the newspaper's articles that were critical of the regime and warned that it would stage military attacks against South Korean media companies.[87] Pyongyang responds forcefully to any perceived insults to its leaders.

2013

- **Operation Dark Seoul** targeted South Korea's three largest TV broadcasters (KBS, MBC, and YTN) and three major banks (Nonghyup, Shinhan, and Jeju).[88] North Korean malware erased critical records of 40,000 computers, disrupted operations for days, and caused $700 million in damage.[89]

- The Kimsuky group sent spear-phishing emails targeting two South Korean think tanks, the Sejong Institute and Korea Institute for Defense Analyses, as well as human rights groups, the Ministry of Unification, and U.N. officials.[90]

2016

- **Operation Desert Wolf** targeted the U.S.–South Korean Combined Forces Command, South Korean Joint Chiefs of Staff, and the Defense Integrated Data Center where all South Korean defense information is stored. The hackers infected 3,200 computers and stole 235 gigabytes of classified information. They gained access to the U.S.–South Korean combined Operations Plan 5015 (OPLAN 5015) military strategy for responding to a North Korean invasion, including the decapitation plan to remove Kim Jong-un during wartime, and OPLAN 3100 for responding to North Korean commando attacks.[91]

- North Korea hacked into the South Korean defense industry, stealing and subsequently deleting 42,000 documents, including designs for the F-15 wing and components of a reconnaissance satellite.[92]

- Jamming operations targeting GPS navigation equipment at Seoul's airports affected 962 planes.[93]

- North Korea hacked dozens of top South Korean government officials' smartphones and stole text messages and voice communications.[94] Pyongyang also gained access to the Defense Minister's personal computer the Defense Ministry's intranet in order to extract military operations intelligence.[95]

- North Korea gained entry into computers of Daewoo Shipbuilding & Marine Engineering Company and stole blueprints for South Korean warships, including information on the planned 3,000-ton submarine as well as its ballistic missile and vertical launch systems.[96]

2017

- North Korean hackers tried to infiltrate U.S. electric companies' networks but did not compromise any of the industrial control systems that regulate the supply of power.[97]

2018

- The Kimsuky group conducted multi-year operations targeting the government; national security; aerospace and defense; experts on

North Korea, nuclear policy, sanctions, and international relations; academia; and the media. These campaigns have included:

1. **Operation Baby Coin** against experts on sanctions;[98]
2. **Operation Baby Shark** against U.S. national security think tanks for information related to Northeast Asia's national security issues;[99]
3. **Operation Kabar Cobra** against the Ministry of Unification press corps;[100]
4. **Operation Kitty Phishing** against the Ministry of Unification press corps;[101]
5. **Operation Red Salt** against retired South Korean diplomatic, government, and military officials;[102]
6. **Operation Stealth Power** against U.S. and South Korean experts on North Korea;[103]
7. **Operation Smoke Screen** against U.S. experts on North Korea;[104] and
8. **Operation Stolen Pencil** against academic institutions.[105]

- **Operation Sharpshooter** targeted 87 organizations in 24 countries in the communications, defense, energy, financial, health care, information technology, and infrastructure (energy, gas, nuclear, telecommunications, and transportation) sectors. The hackers masqueraded as job recruiters to induce targets to download infected documents. The recruiting companies, job listings, and recruiter profiles all appeared to be legitimate.[106]

- **Operation Ghost Secret** was a data-theft campaign to gain intellectual property from companies in critical infrastructure, entertainment, finance, health care, higher education, and telecommunications sectors in 17 countries. The cyber campaign began by targeting a major Turkish government-controlled financial organization, followed by three additional financial institutions, before moving on to global targets.[107]

- North Korea breached computers of the South Korean Ministry of Defense's Defense Acquisition Program Administration and stole arms procurement plans, including plans for the country's next-generation fighter aircraft.[108]

2019

- Several computer security firms reported links between North Korea and the Trickbot Group, an Eastern European cybercrime organization, to deploy malware in the first identified cyber collusion between North Korea and non-state actors.[109]

- North Korean hackers breached the nuclear power plant in Kudankulam, India. The Kimsuky group was seeking proprietary information on thorium-based reactors. India is the leader in commercializing the use of thorium as a safer and more efficient alternative to uranium. The hackers also targeted several Indian nuclear physicists and scholars around the world who had published papers on thorium energy.[110]

- North Korean hackers targeted phishing attacks against the French, South African, and Slovak ministries of foreign affairs, the U.K.'s Royal United Services Institute think tank, and the U.S. Congressional Research Service.[111]

2020

- The Lazarus group targeted defense industry organizations in at least a dozen countries through spear-phishing emails with malware attachments or links. The malware gathered sensitive information and gained access to the organizations' restricted networks, which contained mission-critical assets as well as computers with highly sensitive data with no Internet access.[112]

- North Korean hackers attacked Israel's Ministry of Defense. The government claimed the intrusion was thwarted, but cybersecurity firm ClearSky assessed that the hackers penetrated the ministry's computer system and stole a large amount of classified information in addition to infecting several dozen companies and organizations both in Israel and around the globe. A similar but less effective campaign targeted Israeli experts in 2019.[113]

- North Korean cyber groups impersonated journalists and news outlets to seed false stories with other reporters to spread disinformation. The hackers used real emails gleaned from experts on North Korea to gain access to the computers of other foreign policy experts, North Korean defectors, and people interested in North Korean refugees. The attacks gained access to contact lists for surveillance and follow-on cyberattacks.[114]

- The Kimsuky group engaged in spear-phishing campaigns against 28 U.N. officials, including six members of the U.N. Security Council. The emails contained malicious attachments or a link redirecting the victim to a site to steal usernames and passwords.[115]

2021

- The Lazarus group targeted cybersecurity experts in the U.S., Europe, and China by posing as researchers seeking to collaborate on cyber threat projects. The hackers created false identities on Twitter, Telegram, Keybase, LinkedIn, and Discord; created followers on those accounts; and populated websites with reports and articles to establish credibility.[116]

- The Kimsuky group hacked into the Korea Atomic Energy Research Institute; Korea Aerospace Industries, a defense firm that is building the KF-21 fighter jet; and Daewoo Shipbuilding & Marine Engineering, which is building submarines and ships for the South Korean navy.[117]

Phase Two: Cyberterrorism, Revenge Attacks, and Extortion

2014

- **Operation Blockbuster.** North Korea conducted cyberattacks against and sent threatening messages to employees of Sony Pictures Entertainment to prevent the release of its film *The Interview*, which satirized Kim Jong-un.[118] Pyongyang also threatened "merciless counter-measures" and "9/11-type attacks" against any U.S. theaters showing the film.[119] The cyberattacks and accompanying threats of violent attack met the legal definition of international terrorism contained in the U.S. Code.[120] The regime declared that the film was an "act of

war" and had called on both U.N. Secretary General Ban Ki-moon and President Barack Obama to prevent its release.[121] Sony and theater chains quickly withdrew the film, but the hackers still destroyed more than 3,000 computers and 800 servers; extracted the personal records, salary figures, and emails of 6,000 employees; and stole business records, several unreleased movies, and unfinished scripts that were posted on the Internet.[122] Cancelling the film's release cost Sony an estimated $100 million in lost revenue.[123]

- **Revenge Attacks Against Other "Anti-Kim" Film and TV Projects.**

  1. As a result of the Sony hack and terrorist threats, New Regency announced that it would cancel production of a movie with Steve Carell that was to have been set in North Korea.[124]

  2. North Korea similarly attacked Mammoth Screen, the production company for British Broadcaster Channel Four, which had announced plans for a 10-part television series *Opposite Number* about a British nuclear scientist kidnapped by North Korea. The cyberattack did not cause any damage, but the project was still cancelled.[125]

- **Korea Hydro and Nuclear Power Company.** North Korea conducted a series of cyberattacks against South Korean nuclear facilities that led to the disclosure of blueprints for nuclear reactors and personal information of employees. The hackers demanded money and the shutting down of three reactors, threatening to destroy the nuclear facilities[126] and warning nearby residents that it would "be a Fukushima" nuclear disaster.[127] Korea Hydro and Nuclear Power Company, which controls South Korea's nuclear power plants, reported that its computer systems were breached but that the reactor control systems were not breached.[128]

2017

- **WannaCry** was the largest ransomware attack in history, infecting more than 300,000 computers in more than 150 countries and causing more than $4 billion in damage. The attack crippled the United Kingdom's National Health System, affecting one-third of hospitals

providing intensive care and other emergency services and 8 percent of general medical practices.[129] The ransomware demanded $300 in Bitcoin per victim, but because of a flaw in the code, only $140,000 in ransom was actually paid.[130]

Phase Three: Cyber Bank Robbery

2015

- An unidentified bank in Guatemala reported a loss of $16 million.[131]

- In December, "having gained unauthorized access to [a] Vietnamese Bank's computer network," hackers "conducted false and fraudulent wire transfers totaling approximately €2 million to bank accounts in Slovenia and Bulgaria, and attempted to conduct fraudulent wire transfers of $3.4 million to Russia, A$1 million to Australia, and ¥90 million to Japan."[132]

2016

- North Korea gained deep access to the computer network of the Bangladesh Bank (Bangladesh's central bank) to steal approximately $81 million in fraudulent SWIFT transfers from the bank's accounts in the Federal Reserve Bank of New York to illicit accounts in the Philippines, Sri Lanka, and other banks in Asia. A bank official noticed a typographical error and prevented an additional $851 million from being stolen.[133] The U.S. Federal Reserve Bank authorized five of 35 fraudulent payments.[134]

- $9 million was stolen from Ecuador's Banco del Austro.[135]

- $18 million was stolen from the Standard Bank of South Africa. The Japanese government stated that the hackers used forged cards with customer information stolen from the Standard Bank of South Africa to withdraw cash from approximately 1,700 ATMs in Tokyo and 16 prefectures across Japan.[136]

- Union Bank of India thwarted a theft of $166 million. Hackers transferred money to banks in Cambodia, Thailand, Taiwan, and Australia, but authorities were able to recover the money.[137]

- There was an attempt to steal approximately $104.1 million from an unidentified African bank to bank accounts in Taiwan, Thailand, and Cambodia.[138]

- The South Korean online shopping mall Interpark was the target of a hack attack and blackmail of customer information. The National Police Agency reported that the hackers forced the transfer of $2.7 million.[139]

2017

- **FASTCash Campaign.** North Korean hacker groups stole tens of millions of dollars from bank ATMs in Africa and Asia. An attack in 2017 enabled cash withdrawals from ATMs in more than 30 countries, and a similar event in 2018 targeted banks in 23 countries.[140] In 2018, the Cosmos Bank in India was targeted, enabling $13.5 million to be withdrawn in more than 14,000 simultaneous ATM withdrawals by "money mules" with cloned ATM cards in 28 countries as well as in additional transfers to an account belonging to a Hong Kong–based company using SWIFT transfers.[141]

- An attempt was made to steal $60 million from a Tunisian bank.[142]

- An attempt was made to steal approximately $60.1 million from the Far Eastern International Bank of Taiwan and transfer the money to bank accounts in Sri Lanka, Cambodia, and the United States. The bank recovered all but $500,000.[143]

2018

- Approximately $110 million was fraudulently transferred from Mexico's Banco Nacional De Comercio Exterior (Bancomext) to bank accounts in the Republic of Korea.[144]

- $10 million was transferred from the Banco de Chile to accounts in Hong Kong.[145]

- Approximately $6.1 million was fraudulently withdrawn from BankIslami ATMs in Pakistan.[146]

- An attempt was made to steal $19 million in Costa Rica.[147]

- An attempt was made to steal $16.8 million from India's City Union Bank.[148]
- An attempt was made to steal $390 million using falsified SWIFT messages in Malaysia.[149]
- An attempt was made to steal $32 million in Liberia.[150]

2019

- An attempt was made to transfer "approximately $6.4 million and €7.1 million [from Malta's Bank of Valletta] to bank accounts in Hong Kong, the U.K., the United States, and the Czech Republic." The funds were retrieved.[151]
- There was an attempt to steal $10.8 million in Spain.[152]
- There was an attempt to steal $12.2 million in The Gambia.[153]
- In Nigeria, there was an attempt to steal $9.3 million.[154]
- $49 million was stolen in Kuwait.[155]

Phase Four: Cryptocurrency Exchanges

2017

- Bithumb (South Korea) was attacked at least four times. Attacks in February and July 2017 netted $7 million or more each, and subsequent attacks in June 2018 and March 2019 netted $31 million and $20 million, respectively.[156]
- Youbit (South Korea) suffered multiple attacks involving a $4.8 million loss in April 2017 and then 17 per cent of its overall assets in December 2017, forcing the exchange to file for bankruptcy.[157]
- Monero (South Korea) lost $25,000 from cryptojacking.[158]
- Coinis (South Korea) lost $2.19 million.[159]

- NiceHash (Slovenia) lost more than $70 million.[160]

- South Korean Cryptocurrency Company refused to pay a ransom of $16 million in cryptocurrency, so North Korean hackers released confidential customer information.[161]

- North Korean hackers extorted approximately $2.3 million in cryptocurrency from Central American Online Casino 1 and approximately $361,500 in cryptocurrency from Central American Online Casino 2 to prevent the release of confidential customer information.[162]

2018

- In **Operation AppleJeus,** North Korean hackers created a fake cryptocurrency company to deliver malware by means of a disguised regular application update to targets in China, the U.K., Poland, and Russia. The virus enabled the attacker to gain full control of the users' device and steal cryptocurrency.[163]

- The theft of USD$13 million was reported in India.[164]

- In Bangladesh, an attempt was made to steal $2.6 million.[165]

- In Japan, Coincheck declared that $532 million was stolen.[166]

- North Korean groups hacked into an unidentified digital currency exchange and stole nearly $250 million worth of digital currency. Two Chinese nationals who laundered the assets on behalf of the North Korean group received approximately $91 million (in addition to $9.5 million from a hack of another exchange).[167]

- The Indonesian Cryptocurrency Company was victimized by the fraudulent transfers of approximately $24.9 million in cryptocurrency.[168]

2019

- Dragonex (Thailand, Singapore, and Hong Kong) reported the theft of $7 million.[169]

- UpBit (South Korea) lost $49 million.[170]

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.[171]

- New York Financial Services Company lost approximately $11.8 million through fraudulent transfers of cryptocurrency.[172]

Phase Five: Alternative Currencies and DeFis

After successfully hacking into a financial target, operatives must eventually convert cryptocurrency into real currency and launder it to avoid detection. Cybersecurity experts have identified North Korean hackers moving money through hundreds or thousands of separate transactions in numerous countries to launder it before cashing out.

In 2019, North Korea began to use decentralized finance (DeFi) platforms and decentralized cryptocurrency exchanges (DEX) to launder cryptocurrency. The Lazarus group's use of DeFi platforms nearly doubled in 2020 as its use of mainstream cryptocurrency exchanges decreased.[173] The shift reflects North Korea's money-laundering adaptability in response to increasing security protocols or law enforcement focus on existing platforms. CipherTrace, a crypto intelligence company, assessed that cryptocurrency thefts and hacks declined in 2020 due to increased security procedures but that hacks against DeFis increased.[174]

Phase Six: Pharmaceutical Companies

North Korea took advantage of the COVID-19 crisis to target pharmaceutical companies for proprietary information on vaccine production as well as individuals and businesses seeking COVID relief funding.

In 2020, the Lazarus group planned a large-scale phishing campaign against more than 5 million individuals and businesses in India, Japan, Singapore, South Korea, the U.K., and the United States. The hackers would pose as local authorities dispersing government COVID support funds and direct the targets to fake websites where they would divulge personal and financial information.[175]

North Korean hackers targeted at least six pharmaceutical companies in the U.S., the U.K. and South Korea that were working on COVID treatments, including Johnson & Johnson, Novavax, AstraZeneca, Genexine, Shin Poong, and Celltrion. It was unclear whether North Korea was attempting to create its own vaccine or to sell obtained vaccine information to a foreign pharmaceutical company.[176] In some cases, the hackers sent spear-phishing emails representing themselves as job recruiters or World Health Organization representatives.[177]

The Lazarus group also targeted government agencies conducting COVID research, including the U.S. Department of Health and Human Services and the European Medicines Agency. The Kaspersky computer security company assessed that some computers at government agencies and companies had been breached.[178]

In 2021, a member of the South Korean National Assembly asserted that intelligence reporting indicated that North Korea had targeted Pfizer to gain COVID vaccine information. It was uncertain whether the attack was successful.[179]

Appendix 3: U.S. Government Responses to the North Korean Cyber Threat

In recent years, the U.S. government has issued numerous warning notices to highlight the growing danger of North Korean cyberattacks.[180] The notices provide detailed technical information to enable companies and financial institutions to develop defensive responses. Washington also has issued indictments and imposed sanctions on North Korean individuals and entities in response to illicit cyber activities. Specifically:

- In 2014, the U.S. Treasury Department imposed sanctions on the Reconnaissance Guidance Bureau after the Sony hack.

- In 2016, the United States designated North Korea as a money-laundering concern, precluding it from accessing the U.S. financial system for international financial transactions.[181]

- In September 2018, the Treasury Department's Office of Foreign Assets Control (OFAC) and the Department of Justice sanctioned and unsealed criminal charges against Park Jin-hyok and the Chosun Expo Joint Venture for their involvement in the Sony hack, Bangladesh bank robbery, and WannaCry ransomware attack.[182]

- In June 2019, the U.S. District Court for the District of Columbia affirmed the U.S. government's authority under the Patriot Act to subpoena records from foreign banks with correspondent accounts in the United States as well as to cut off access by foreign banks to the U.S. financial system or dollar-denominated transactions.[183] The ruling was in response to a Chinese company's use of three Chinese banks to launder millions of dollars on behalf of North Korea's sanctioned Foreign Trade Bank. The court ruling "caused a ripple effect throughout the Chinese financial sector. Stock prices for the three banks...plummeted shortly after the publication of the circuit court's opinion."[184]

- In September 2019, OFAC announced sanctions against the Lazarus, Andariel, and Bluenoroff hacking groups for cyberattacks to support North Korea's illicit nuclear and missile programs. The legal action blocks any property or interests of these entities in the United States. Any transactions by U.S. persons or foreign financial institutions using correspondent accounts in the United States would be subject to sanctions.[185]

- In February 2020, the Pentagon, the FBI, and the Department of Homeland Security issued a series of messages warning of a North Korean cyber-espionage hacking campaign to "conduct illegal activity, steal funds & evade sanctions."[186]

- In March 2020, a grand jury indicted and the Treasury Department imposed sanctions on two Chinese nationals (Tian Yinyin and Li Jiadong) for laundering more than $100 million in cryptocurrency stolen by North Korean agents in a 2018 hack of a cyberexchange that netted $250 million. The individuals were also linked to a North Korean cybertheft of $48.5 million from a South Korean currency exchange in 2019.[187]

- In May 2020, the Justice Department charged 28 North Korean and five Chinese individuals with laundering more than $2.5 billion in illegal payments for Pyongyang's nuclear weapons and missile programs. The unsealed indictment accused the individuals of acting as agents of North Korea's Foreign Trade Bank, the regime's primary foreign currency bank and under U.S. sanctions for facilitating nuclear proliferation.[188] The case was the largest U.S. sanctions violations case against North Korea and reveals the extent to which the United States believes China has assisted North Korea's illicit network to evade international sanctions.[189]

- In August 2020, the U.S. government warned of a North Korean group targeting government defense contractors to gather intelligence surrounding key military and energy technologies. The group used fake job postings from leading defense contractors as lures to install a data-gathering implant on the victim's system.[190]

- In August 2020, the U.S. Department of Justice filed a civil complaint for forfeiture of 280 cryptocurrency accounts linked to North Korean hacking of two cryptocurrency exchanges in July 2019 and September 2019 that netted millions of dollars' worth of cryptocurrency for the regime. "The complaint follows related criminal and civil actions announced in March 2020 pertaining to the theft of $250 million in cryptocurrency through other exchange hacks by North Korean actors" and "exposes the ongoing connections between North Korea's cyber-hacking program and a Chinese cryptocurrency money laundering network."[191]

- In August 2020, the U.S. government issued a warning about the compromise of ATMs by the North Korean–linked BeagleBoyz and Operation FastCash. In February 2020, North Korea had resumed its targeting of banks in multiple countries for fraudulent international money transfers and ATM cashouts, ending "a lull in bank targeting since late 2019." BeagleBoyz overlaps with other North Korean cyber groups and has been involved in attempts to steal nearly $2 billion at least since 2015.[192]

- In September 2020, leaked U.S. government documents revealed that North Korea laundered $174.8 million in illicit funds from 2008 to 2017 through prominent U.S. banks in New York, including JP Morgan Chase and Bank of New York Mellon. The documents also showed that Chinese companies were involved.[193]

- In October 2020, the U.S. government issued a warning alert on North Korean cyber group Kimsuky. The U.S. said the group was "engaged in ongoing cyber operations against worldwide targets to gain intelligence for North Korea, specifically on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions."[194] The group specifically targets experts, think tanks, and government agencies in South Korea, Japan, and the United States.

- In February 2021, the U.S. government issued an alert about the Lazarus group's targeting of individuals and companies, including cryptocurrency exchanges and financial service companies, with malware to steal cryptocurrency. Lazarus targeted cryptocurrency organizations in more than 30 countries during 2020 using cryptocurrency malware, referred to as AppleJeus. North Korea has used AppleJeus malware posing as cryptocurrency trading platforms since at least 2018. The malware appears to be from a legitimate cryptocurrency trading company to fool individuals into downloading it from what appears to be a legitimate website. Lazarus also uses phishing, social networking, and social engineering techniques to lure users into downloading the malware.[195]

- In February 2021, the U.S. government unsealed a December 2020 indictment against three North Korean hackers (Jon Chang-hyok, Kim Il, and Park Jin-hyok) accused of committing a series of cyberattacks and attempting to steal or extort more than $1.3 billion worth

of money and cryptocurrency from cyber heists and forced ATM cashouts. The case was an expansion of a 2018 case involving the Sony and WannaCry hacks. An accompanying case related to a Canadian-American citizen who pled guilty to money laundering.[196]

- In March 2021, for the first time, the U.S. extradited a North Korean intelligence operative from overseas. Mun Chol-myong, affiliated with the Reconnaissance General Bureau, was accused of defrauding banks and laundering money through the U.S. financial system "in transactions valued at over $1.5 million" by using "a web of front companies and bank accounts registered to false names and remov[ing] references to [North Korea] from international wire transfer and transactional documents."[197]

Endnotes

1. Some experts initially rejected that North Korea had developed plutonium for nuclear weapons, had a uranium-based nuclear weapons program, had helped Syria build a nuclear reactor, had miniaturized nuclear weapons to put on missiles, and had produced ICBMs that could reach the continental United States.
2. 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 5, 2021).
3. Daniel R. Coats, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," statement before the Select Committee on Intelligence, U.S. Senate, January 29, 2019, p. 6, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (accessed August 5, 2021).
4. Stephanie Kleine-Ahlbrandt, "North Korea's Illicit Cyber Operations: What Can Be Done?" Henry L. Stimson Center, 38 North, February 2020, p. 8, https://www.38north.org/wp-content/uploads/pdf/2020-0228_SKA_NK-Cyber-Operations.pdf (accessed August 5, 2021).
5. 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 COE [Cooperative Cyber Defence Centre of Excellence] Publications, 2019), p. 144, https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf (accessed August 7, 2021). The conference was held in Tallinn, Estonia, May 28–31, 2019.
6. Alexandre Mansourov, "North Korea's Cyber Warfare and Challenges for the U.S.–ROK Alliance," Korea Economic Institute of America *Academic Paper Series*, December 2, 2014, p. 4, http://keia.org/sites/default/files/publications/kei_aps_mansourov_final.pdf (accessed August 5, 2021).
7. "Cyber Attack Retaliation Against Seoul's Move to Join 'Cyber Storm,'" *The Korea Herald*, March 30, 2010, http://www.koreaherald.com/view.php?ud=200907100065 (accessed August 5, 2021).
8. Duk-ki Kim, "The Republic of Korea's Counter-Asymmetric Strategy," *Naval War College Review*, Vol. 65, No. 1, Article 4, (Winter 2013), pp. 61–80, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1462&context=nwc-review (accessed August 6, 2021).
9. Kleine-Ahlbrandt, "North Korea's Illicit Cyber Operations: What Can Be Done?"
10. "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 5, 2021).
11. Ji-young, Jong-in, and Kyoung-gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," in proceedings, *11th International Conference on Cyber Conflict: Silent Battle*, p. 143.
12. Kartikay Mehrotra and David Voreacos, "U.S. Calls North Korean Hackers 'World's Leading Bank Robbers,'" Bloomberg, February 17, 2021, https://www.bloomberg.com/news/articles/2021-02-17/u-s-charges-3-north-koreans-linked-to-sony-hack-in-new-scheme (accessed August 5, 2021).
13. 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 (accessed August 5, 2021).
14. Observatory of Economic Complexity, "North Korea," https://oec.world/en/profile/country/prk (accessed August 6, 2021).
15. 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 6, 2021).
16. Charlie Campbell, "Why We Shouldn't Be Surprised If North Korea Launched the WannaCry Ransomware Cyberattack," *Time*, May 17, 2017, https://time.com/4781809/ransomware-attack-north-korea-wannacry/?xid=time_socialflow_twitter (accessed August 6, 2021).
17. David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *The New York Times*, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (accessed August 6, 2021).
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 (accessed August 6, 2021).
19. "Lazarus Group Pulled off 2020's Biggest Exchange Hack and Appears to Be Exploring New Money Laundering Options," Chainalysis Blog, February 9, 2021, https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack (accessed August 6, 2021).
20. *United States of America v. Park Jin-hyok*, United States District Court for the Central District of California, Case No. MJ 18-1479, Criminal Complaint, filed June 8, 2018, https://www.justice.gov/opa/press-release/file/1092091/download (accessed August 6, 2021), and news release, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," U.S. Department of Justice, February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and (accessed August 6, 2021).
21. News release, "Two Chinese Nationals Charged with Laundering over $100 Million in Cryptocurrency from Exchange Hack," U.S. Department of Justice, March 2, 2020, https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack (accessed August 7, 2021).

22. For a detailed description of North Korean government agencies and subordinate groups conducting cyber operations, see Appendix 1, *infra*.
23. In 2016, the State Affairs Commission replaced the National Defense Commission as North Korea's supreme policy-oriented leadership organization.
24. "[A]n advanced persistent threat (APT) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences." Kaspersky, "What Is an Advanced Persistent Threat?" https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats (accessed August 10, 2021).
25. SWIFT is the international financial messaging system for making digital financial transfers among banks.
26. *United States of America v. Park Jin-hyok*, *passim*, and Catalin Cimpanu, "North Korean Hackers Infiltrate Chile's ATM Network After Skype Job Interview," ZDNet, January 16, 2019, https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/ (accessed August 6, 2021).
27. The author can personally attest to this, having been repeatedly targeted by North Korean cyber organizations.
28. Information provided to the author.
29. Symantec Security Response Blog, "Attackers Target Dozens of Global Banks with New Malware," CSO, February 12, 2017, https://www2.cso.com.au/vendor_blog/11/symantec-security-response-blogs/15958/attackers-target-dozens-of-global-banks-with-new-malware/ (accessed August 6, 2021).
30. Nalani Fraser, Jacqueline O'Leary, Vincent Cannon, and Fred Plan, "APT38: Details on New North Korean Regime-Backed Threat Group," FireEye, October 3, 2018, https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html (accessed August 6, 2021), and Insikt Group, "How North Korea Revolutionized the Internet as a Tool for Rogue Regimes," *Cyber Threat Analysis* No. CTA-2020-0209, https://go.recordedfuture.com/hubfs/reports/cta-2020-0209.pdf (accessed August 6, 2021).
31. For a detailed compendium of North Korean cyberattacks, see Appendix 2, *infra*.
32. 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 (accessed August 12, 2021).
33. Andrew Salmon, "North Korea's Cyber Commandos Range Far, Strike Deep," *Asia Times*, March 2, 2021, https://asiatimes.com/2021/03/kims-cyber-commandos-range-far-strike-deep/ (accessed August 6, 2021), and Andrew Salmon, "Cyber Warrior's Glimpse into Kim's Operation Chaos," *Asia Times*, February 27, 2021, https://asiatimes.com/2021/02/cyber-warriors-glimpse-into-kims-operation-chaos/ (accessed August 6, 2021).
34. "N.Korea Boosting Cyber Warfare Capabilities."
35. FireEye, "North Korean Actors Spear Phish U.S. Electric Companies," Threat Research Blog, October 11. 2017, https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html (accessed August 6, 2021).
36. 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. 1, https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf (accessed August 6, 2021).
37. Society for Worldwide Interbank Financial Telecommunication, "SWIFT in Figures: December 2019 YTD," https://www.swift.com/sites/default/files/documents/sif_201912.pdf (accessed August 6, 2021).
38. H.R. 6395, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law No. 116-283, 116th Cong., January 1, 2021, Section 1752, https://www.congress.gov/bill/116th-congress/house-bill/6395/text (accessed August 6, 2021).
39. Cal Biesecker, "Biden Says Cyber Security Will Be a Top Priority; Requires Investments, Deterrence," IIoT Connection, December 17, 2020, https://www.iiotconnection.com/biden-says-cyber-security-will-top-priority-requires-investments-deterrence/ (accessed August 6, 2021).
40. 6 U.S. Code §§ 1501–1510, https://www.law.cornell.edu/uscode/text/6/chapter-6/subchapter-I (accessed August 10, 2021).
41. U.S. Department of Homeland Security and U.S. Department of Justice, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures Under the Cybersecurity Information Sharing Act of 2015*, October 2020, p. 3, https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf (accessed August 6, 2021). See also Brian Finch, "Additional Liability Protections Are Needed Against Cyberthreats," Heritage Foundation *Legal Memorandum* No. 283, March 24, 2021, https://www.heritage.org/cybersecurity/report/additional-liability-protections-are-needed-against-cyberthreats.
42. John Costello and Mark Montgomery, "How the National Cyber Director Position Is Going to Work: Frequently Asked Questions," Lawfare, February 24, 2021, https://www.lawfareblog.com/how-national-cyber-director-position-going-work-frequently-asked-questions (accessed August 6, 2021).
43. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 30, 2019, p. 30.
44. Jason Bartlett, "Exposing the Financial Footprints of North Korea's Hackers," Center for New American Security, November 18, 2020, https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers (accessed August 6, 2021), and news release, "FinCEN Launches 'FinCEN Exchange' to Enhance Public–Private Information Sharing," U.S. Department of the Treasury, Financial Crimes Enforcement Network, December 4, 2017, https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing (accessed August 6, 2021).

45. Andrea Mihailescu, "It's Time to Get Serious About a Pressure Strategy to Contain North Korea," Atlantic Council, Geoeconomics Center *Issue Brief*, March 2021, https://www.atlanticcouncil.org/wp-content/uploads/2021/03/North-Korea-IB-v3.pdf (accessed August 6, 2021).
46. H.R. 757, North Korea Sanctions and Policy Enhancement Act of 2016, Public Law No. 114-122, 114th Cong., February 18, 2016, https://www.congress.gov/bill/114th-congress/house-bill/757/text (accessed August 10, 2021)
47. 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 6, 2021).
48. Matthew Ha, "America Must Take North Korea's Cyber Warfare Capabilities Seriously," *The National Interest*, Korea Watch Blog, December 9, 2020, https://nationalinterest.org/blog/korea-watch/america-must-take-north-koreas-cyber-warfare-capabilities-seriously-174141 (accessed August 6, 2021).
49. 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 (accessed August 6, 2021.
50. H.R. 6395, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Division F—Anti-Money Laundering.
51. Zia M. Faruqui, Jessie K. Liu, and Noha K. Moustafa, "The Long Arm of U.S. Law: The Patriot Act, the Anti-Money Laundering Act of 2020 and Foreign Banks," Lawfare, February 23, 2021, https://www.lawfareblog.com/long-arm-us-law-patriot-act-anti-money-laundering-act-2020-and-foreign-banks (accessed August 6, 2021).
52. Annex 62, "Consolidated List of Recommendations," in United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 28, 2020, p. 210: "The Panel encourages Member States to implement the Financial Action Task Force standards, with special attention given to recommendation 15, that to manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for anti-money-laundering and counter-terrorist financing purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the Financial Action Task Force recommendations."
53. Biesecker, "Biden Says Cyber Security Will Be a Top Priority; Requires Investments, Deterrence."
54. Klon Kitchen and James Di Pane, "Cybersecurity: National Policies and Practices for Understanding Hacks and Reducing Vulnerabilities," Heritage Foundation *Backgrounder* No. 3512, July 24, 2020, https://www.heritage.org/cybersecurity/report/cybersecurity-national-policies-and-practices-understanding-hacks-and-reducing.
55. Reuters, "NATO Agrees Cyberattack Could Trigger Military Response," September 5, 2014, http://www.cnbc.com/id/101974720 (accessed August 6, 2021), and Steve Ranger, "NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict," ZDNet, June 30, 2014, http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict-7000031064/ (accessed August 6, 2021).
56. Government of Japan, Ministry of Foreign Affairs, "Japan–United States of America Relations: U.S. Japan–U.S. Security Consultative Committee (Japan–U.S. '2+2')," April 19, 2019, https://www.mofa.go.jp/na/fa/page3e_001008.html (accessed August 6, 2021).
57. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, S/2019/171, March 5, 2019, *passim*, https://www.undocs.org/S/2019/171 (accessed August 5, 2021).
58. Government of South Korea, Ministry of National Defense, *2018 Defense White Paper*, p. 27, https://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201908070153390840.pdf (accessed August 6, 2021).
59. HP Security Research, *HP Security Briefing, Episode 16, August 2014: Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*, p. 24, https://time.com/wp-content/uploads/2014/12/hpsr_securitybriefing_episode16_northkorea.pdf (accessed August 7, 2021).
60. Ji-young, Jong-in, and Kyoung-gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," in proceedings, *11th International Conference on Cyber Conflict: Silent Battle*, p. 150, and East Asia Forum, "North Korea's Evolving Cyber Warfare Strategy—Analysis," *Eurasia Review*, September 25, 2020, https://www.eurasiareview.com/25092020-north-koreas-evolving-cyber-warfare-strategy-analysis/ (accessed August 7, 2021).
61. HP Security Research, *HP Security Briefing, Episode 16, August 2014: Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*, pp. 22 and 23.
62. Kim, "The Republic of Korea's Counter-Asymmetric Strategy."
63. Steve Miller, "Where Did North Korea's Cyber Army Come From?" Voice of America, November 20, 2018, https://www.voanews.com/east-asia-pacific/where-did-north-koreas-cyber-army-come (accessed August 7, 2021).
64. Mansourov, "North Korea's Cyber Warfare and Challenges for the U.S.–ROK Alliance."
65. Ji-young, Jong-in, and Kyoung-gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," in proceedings, *11th International Conference on Cyber Conflict: Silent Battle*, p. 147.
66. Associated Press, "North Korean Army Suspected in Cyber Attacks," NBC News, July 11, 2009, https://www.nbcnews.com/id/wbna31866018 (accessed August 7, 2021).

67. McAfee, "Examining Code Reuse Reveals Undiscovered Links Among North Korea's Malware Families," August 9, 2018, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families/ (accessed August 7, 2021).
68. East Asia Forum, "North Korea's Evolving Cyber Warfare Strategy—Analysis."
69. Ji-young, Jong-in, and Kyoung-gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," in proceedings, *11th International Conference on Cyber Conflict: Silent Battle*, p. 148, and Jenny Jun, Scott LaFoy, and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Response*, A Report of the CSIS Korea Chair, Center for Strategic and International Studies, December 2015, pp. 45–50, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperationsWeb.pdf (accessed August 7, 2021.
70. "N.Korea Boosting Cyber Warfare Capabilities."
71. HP Security Research, *HP Security Briefing, Episode 16, August 2014: Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*, pp. 24 and 32.
72. Kim, "The Republic of Korea's Counter-Asymmetric Strategy," and Mansourov, "North Korea's Cyber Warfare and Challenges for the U.S.–ROK Alliance," p. 6.
73. Press release, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," U.S. Department of the Treasury, September 13, 2019, https://home.treasury.gov/news/press-releases/sm774 (accessed August 6, 2021), and FireEye, "APT37 (Reaper): The Overlooked North Korean Actor," *Special Report*, 2018, p. 6, https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf (accessed August 7, 2021).
74. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Alert (AA20-301A): North Korean Advanced Persistent Threat Focus: Kimsuky," October 27, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-301a (accessed August 6, 2021).
75. FireEye, "APT38: Un-usual Suspects," *Special Report*, 2018, p. 6, https://content.fireeye.com/apt/rpt-apt38 (accessed August 7, 2021). See also Figure 4, "APT38 Operations and North Korea's Worsening Financial Situation," in ibid., p. 13.
76. Press release, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups."
77. Ibid.
78. Aleksander Atamaov and Aleksander Mamaev, "North Korea: How DPRK Created World's Most Effective Cyber Forces," Russian International Affairs Council, 2018, p. 13, https://russiancouncil.ru/papers/RIAC-CyberNorthKorea-en.pdf (accessed August 7, 2021).
79. Novetta, *Operation Blockbuster: Unraveling the Long Thread of the Sony Attack*, pp. 20–21, https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf (accessed August 7, 2021), and Kelly Jackson Higgins, "Sony Hackers Behind Previous Cyberattacks Tied to North Korea," Dark Reading, February 24, 2016, https://www.darkreading.com/threat-intelligence/sony-hackers-behind-previous-cyberattacks-tied-to-north-korea-/d/d-id/1324422 (accessed August 7, 2021).
80. Park Bo-ram, "N. Korea's State-Sponsored Hackers Emerge as Global Threat," Yonhap News Agency, March 21, 2013, https://en.yna.co.kr/view/AEN20130321006700315 (accessed August 7, 2021).
81. Ryan Sherstobitoff, Itai Liba, and James Walter, "Dissecting Operation Troy: Cyberespionage in South Korea," McAfee *White Paper*, 2013, https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/dissecting-operation-troy.pdf (accessed August 7, 2021); Group-IB, "Lazarus Arisen: Architecture / Tools / Attribution," May 30, 2017, https://www.group-ib.com/blog/lazarus (accessed August 8, 2021); Matthew Weaver, "Cyber Attackers Target South Korea and US," *The Guardian*, July 8, 2009, http://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack (accessed August 8, 2021); Bo-ram, "N. Korea's State-Sponsored Hackers Emerge as Global Threat;"; and Mark Clayton, "In Cyberarms Race, North Korea Emerging as a Power, Not a Pushover," *The Christian Science Monitor*, October 19, 2013, https://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover (accessed August 8, 2021).
82. "Massive GPS Jamming Attack by North Korea," *GPS World*, May 8, 2012, https://www.gpsworld.com/massive-gps-jamming-attack-by-north-korea/ (accessed August 7, 2021).
83. McAfee, "Ten Days of Rain," McAfee *White Paper*, 2011, https://www.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf (accessed August 8, 2021), and A L Johnson, "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," Symantec Endpoint Protection, June 26, 2013, http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war (accessed August 8, 2021).
84. Lee Chul-jae and Moon Gwang-lip, "Incheon Airport Cyberattack Traced to Pyongyang," *Korea JoongAng Daily*, June 4, 2012, https://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2953940 (accessed August 8, 2021).
85. "S.Korean Accused of Doing Business with N.Korean Hackers," *The Chosun Ilbo*, May 6, 2011, http://english.chosun.com/site/data/html_dir/2011/05/06/2011050600827.html (accessed August 8, 2021), and Choe Sang-Hun, "Seoul Warns of Latest North Korean Threat: An Army of Online Gaming Hackers," *The New York Times*, August 4, 2011, https://www.nytimes.com/2011/08/05/world/asia/05korea.html (accessed August 8, 2021).
86. "Massive GPS Jamming Attack by North Korea," and Editorial, "N.Korea's GPS Jamming Is Terrorism Pure and Simple," *The Chosun Ilbo*, May 11, 2012, http://english.chosun.com/site/data/html_dir/2012/05/11/2012051101175.html (accessed August 8, 2021).

87. Kim Hee-jin, "North Behind Hacking Attack on JoongAng Ilbo," *Korea JoongAng Daily*, January 16, 2013, https://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2965629 (accessed August 8, 2021), and "N.Korea Uses Coordinates to Threaten SK Media Outlets," *The Donga-A Ilbo*, June 5, 2012, https://www.donga.com/en/List/article/all/20120605/403965/1/N-Korea-uses-coordinates-to-threaten-SK-media-outlets (accessed August 8, 2021).
88. Press release, "South Korea Identified Who's Behind the Cyber Attack," IssueMakersLab, April 10, 2013, https://docs.google.com/file/d/0B6CK-ZBGuMe4dGVHdTZnenJMRUk/preview?pli=1 (accessed August 8, 2021).
89. Steve Kroft, "The Attack on Sony," CBS News, *60 Minutes*, April 12, 2015, https://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/ (accessed August 7, 2021).
90. Dmitry Tarakanov, "The 'Kimsuky' Operation: A North Korean APT?" Kapersky SecureList, September 11, 2013, https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/ (accessed August 8, 2021).
91. Choe Sang-hun, "North Korean Hackers Stole U.S.–South Korean Military Plans, Lawmaker Says," *The New York Times*, October 10, 2017, https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html (accessed August 8, 2021), and Lee Sung-eun and Lee Chul-jae, "Hackers in North Korea Got Access to Oplan 5027," *Korea JoongAng Daily*, April 4, 2017, https://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3031822 (accessed August 8, 2021).
92. Yonhap News Agency, "Military Info Leaked in N. Korea's Cyberattack: Seoul Policy," *The Korea Herald*, June 13, 2016. http://www.koreaherald.com/view.php?ud=20160613000765 (accessed August 8, 2021).
93. Kyle Mizokami, "North Korea Is Jamming GPS Signals," *Popular Mechanics*, April 5, 2016, https://www.popularmechanics.com/military/weapons/a20289/north-korea-jamming-gps-signals/ (accessed August 8, 2021).
94. Paula Hancocks and K. J. Kwon, "North Korea Hacked Government Officials' Smartphones, South Korea Says," CNN, March 8, 2016, https://www.cnn.com/2016/03/08/asia/south-korea-smartphone-hack (accessed August 8, 2021).
95. Press release, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups."
96. Haejin Choi, "North Korea Hacked Daewoo Shipbuilding, Took Warship Blueprints: South Korea Lawmaker," Reuters, October 31, 2017, https://www.reuters.com/article/us-northkorea-missiles-cybercrime/north-korea-hacked-daewoo-shipbuilding-took-warship-blueprints-south-korea-lawmaker-idUSKBN1D00EX (accessed August 8, 2021), and Yu Yong-weon, "N.Korean Hackers Target S.Korean Submarine Data," *The Chosun Ilbo*, June 21, 2021, http://english.chosun.com/site/data/html_dir/2021/06/21/2021062101201.html (accessed August 8, 2021).
97. Arjun Kharpal, "North Korean Hackers Target US Electric Companies with Malicious Email Attack," CNBC, October 11, 2017, https://www.cnbc.com/2017/10/11/north-korean-hackers-target-us-electric-companies-with-malicious-emails.html (accessed August 8, 2021).
98. Byung-Chul Won, "APT Attack Disguised as Korean Security Product Icon Emerges," BOA News, November 2, 2018, https://www.boannews.com/media/view.asp?idx=74270 (accessed August 8, 2021).
99. Palo Alto Networks, Unit 42, "New BabyShark Malware Targets U.S. National Security Think Tanks," February 22, 2019, https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/ (accessed August 8, 2021).
100. AhnLab, "Operation Kabar Cobra," Security Emergency-Response Center *Analysis Report*, February 28, 2019, https://global.ahnlab.com/global/upload/download/techreport/[Analysis_Report]Operation%20Kabar%20Cobra%20(1).pdf (accessed August 8, 2021).
101. NSHC Group, Red Alert, "The Double Life of SectorA05 Nesting in Agora (Operation Kitty Phishing)," 2019, https://redalert.nshc.net/2019/01/30/operation-kitty-phishing/ (accessed August 8, 2021).
102. AhnLab, "Security Issue: Analysis Report on Operation Red Salt," *ASEC Report*, Vol. 96, Q3 2019, pp. 4–15, https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.96_ENG.pdf (accessed August 7, 2021).
103. Pill (Alyac), "Kimsuky Organization, Operation Stealth Power Silent Operation," ESTsecurity, April 3, 2019, https://blog.alyac.co.kr/2234 (accessed August 7, 2021).
104. Pill (Alyac), "U.S.–Korea APT Campaign 'Smoke Screen' Kimsuky Entity Unveiled," ESTsecurity, April 17, 2019, https://blog.alyac.co.kr/2243 (accessed August 7, 2021).
105. Kacy Zurkus, "Stolen Pencil Targets Academic Institutions," *InfoSecurity*, December 6, 2018, https://www.infosecurity-magazine.com/news/stolen-pencil-targets-academic/ (accessed August 7, 2021).
106. Ryan Sherstobitoff and Asheer Malhotra, "Operation Sharpshooter," McAfee Advanced Threat Research, December 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf (accessed August 7, 2021), and Cyware Hacker News, "Operation SharpShooter Attacks Nuclear, Defense, Energy, and Financial Companies," Cyware, December 13, 2018, https://cyware.com/news/operation-sharpshooter-attacks-nuclear-defense-energy-and-financial-companies-acd05566/ (accessed August 7, 2021).
107. Raj Samani, "Global Malware Campaign Pilfers Data from Critical Infrastructure, Entertainment, Finance, Health Care, and Other Industries," McAfee, April 24, 2018, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/global-malware-campaign-pilfers-data-from-critical-infrastructure-entertainment-finance-health-care-and-other-industries (accessed August 7, 2021), and Ryan Sherstobitoff, "Hidden Cobra Targets Turkish Financial Sector with New Bankshot Implant," McAfee, March 8, 2018, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/#:~:text=The%20US%20government%20reports%20that,also%20known%20as%20Trojan%20Manuscript (accessed August 7, 2021).

108. Catalin Cimpanu, "Hackers Breach and Steal Data from South Korea's Defense Ministry," ZDNet, January 16, 2019, https://www.zdnet.com/article/hackers-breach-and-steal-data-from-south-koreas-defense-ministry/ (accessed August 7, 2021).
109. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, S/2020/151, March 2, 2020, p. 65, https://undocs.org/S/2020/151 (accessed August 5, 2021).
110. Prabhjote Gill, "Here's Why North Korean Hackers Attacked India's Nuclear Power Plant, *Business Insider*, November 13, 2019, https://www.businessinsider.in/tech/news/heres-why-north-korean-hackers-attacked-indias-nuclear-power-plant/articleshow/72035492.cms (accessed August 7, 2021).
111. Jeff Stone, "Hacking Group Targets Organizations Focused on North Korea's Missile Program," CyberScoop, August 21, 2019, https://www.cyberscoop.com/north-korean-hacking-espionage-phishing/?category_news=news (accessed August 7, 2021).
112. Press release, "Kaspersky Finds Lazarus APT Targeting the Defense Industry," February 25, 2021, https://usa.kaspersky.com/about/press-releases/2021_kaspersky-finds-lazarus-apt-targeting-the-defense-industry (accessed August 7, 2021).
113. Ronen Bergman and Nicole Perlroth, "North Korean Hacking Group Attacks Israeli Defense Industry," *The New York Times*, updated August 14, 2020, https://www.nytimes.com/2020/08/12/world/middleeast/north-korea-hackers-israel.html?referringSource=articleShare (accessed August 7, 2021).
114. Shannon Vavra, "North Korean Hackers Reboot Espionage Operations Following December Takedown," CyberScoop, March 31, 2020, https://www.cyberscoop.com/apt37-geumseong121-north-korea-hackers-estsecurity/?category_news=news (accessed August 6, 2021), and Tara Seals, "North Korea-Backed Spy Group Poses as Reporters in Spearphishing Attacks, Feds Warn," Threatpost, October 28, 2020, https://threatpost.com/north-korea-spy-reporters-feds-warn/160622/ (accessed August 7, 2021).
115. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, March 2, 2020, pp. 51 and 156.
116. Lily Hay Newman, "North Korea Targets—and Dupes—a Slew of Cybersecurity Pros," *Wired*, January 26, 2021, https://www.wired.com/story/north-korea-hackers-target-cybersecurity-researchers/ (accessed August 7, 2021).
117. Michael Lee, "Nuclear Research Institute Hacked by North for 12 days," *Korea JoongAng Daily*, July 8, 2021, https://koreajoongangdaily.joins.com/2021/07/08/national/northKorea/North-Korea-hacking-nuclear/20210708190700374.html (accessed August 7, 2021).
118. Novetta, *Operation Blockbuster: Unraveling the Long Thread of the Sony Attack*.
119. Brent Lang, "Sony Hackers Threaten 9/11 Attack on Movie Theaters that Screen 'The Interview,'" *Variety*, December 16, 2014, https://variety.com/2014/film/news/sony-hackers-threaten-911-attack-on-movie-theaters-that-screen-the-interview-1201380712/ (accessed August 7, 2021).
120. 18 U.S. Code § 2331(1)(A)–(C), http://www.law.cornell.edu/uscode/text/18/2331 (accessed August 7, 2021).
121. "'An Act of War': North Korea Issues Warning Over 'Reckless' New James Franco Comedy About Kim Jong-un Assassination Plot," *Daily Mail,* June 25, 2014, https://www.dailymail.co.uk/news/article-2668733/North-Korean-agricultural-workers-vow-revenge-U-S-rally-eve-Korean-War-anniversary.html (accessed August 7, 2021).
122. Kroft, "The Attack on Sony."
123. Nate Silver, "Killing 'The Interview' Could Cost Sony $100 Million," FiveThirtyEight, December 17, 2014, http://fivethirtyeight.com/datalab/killing-the-interview-could-cost-sony-100-million/ (accessed August 7, 2021).
124. Mike Fleming Jr., "North Korea-Based Thriller with Gore Verbinski and Steve Carell Canceled," Deadline, December 17, 2014, https://deadline.com/2014/12/north-korea-thriller-gore-verbinski-steve-carell-canceled-new-regency-1201328532/ (accessed August 7, 2021).
125. Gordon Corera, "UK TV Drama About North Korea Hit by Cyber-Attack," BBC News, October 16, 2017, https://www.bbc.com/news/technology-41640976 (accessed August 7, 2021).
126. Yonhap News Agency, "N. Korea Behind Nuke Power Plant Data Leakage: Investigators," March 17, 2015, https://en.yna.co.kr/view/AEN20150317005500315 (accessed August 7, 2021).
127. Victoria Richards, "South Korea to Hold Nuclear Drills After Hack Threat," *The Times*, December 22, 2014, http://www.thetimes.co.uk/tto/news/world/asia/article4304722.ece (accessed August 7, 2021), and Jung Hyo-sik and Ser Myo-ja, "North Suspected in Nuke Hacking," *Korea JoongAng Daily*, December 25, 2014, http://koreajoongangdaily.joins.com/news/article/Article.aspx?aid=2998926 (accessed August 7, 2021).
128. Justin McCurry, "South Korean Nuclear Operator Hacked amid Cyber-Attack Fears," *The Guardian*, December 23, 2014, http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack (accessed August 6, 2021).
129. Press release, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups"; Eyerys, "WannaCry Infecting More Than 300,000 Computers in 150 Countries," December 5, 2017, https://www.eyerys.com/articles/timeline/wannacry-infecting-more-230000-computers-99-countries#event-a-href-articles-timeline-namewreck-exposes-hundreds-millions-iot-devices-security-risks039-name-wreck039-exposes-hundreds-of-millions-of-iot-devices-to-security-risks-a (accessed August 6, 2021); and Jonathan Berr, "'WannaCry' Ransomware Attack Losses Could Reach $4 Billion," CBS News, May 16, 2017, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ (accessed August 6, 2021).
130. Selena Larson, "Someone Has Emptied the Ransom Accounts from the WannaCry Attack," CNN, August 3, 2017, https://money.cnn.com/2017/08/03/technology/wannacry-bitcoin-ransom-moved/index.html (accessed August 6, 2021).
131. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 30, 2019, p. 109.

132. *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, United States District Court for the Central District of California, CR 2:20-cr-00614-DMG, Indictment, filed December 8, 2020, pp. 16–17, https://www.justice.gov/opa/press-release/file/1367701/download (accessed August 6, 2021.
133. Robert Hackett, "Everything You Need to Know About North Korea's Suspected Bank Blitzkrieg," *Fortune*, June 23, 2016, https://fortune.com/2016/06/23/north-korea-hackers-banks/ (accessed August 6, 2021).
134. *United States of America v. Park Jin Hyok*, pp. 56–94.
135. Hackett, "Everything You Need to Know About North Korea's Suspected Bank Blitzkrieg."
136. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 30, 2019, p. 109.
137. Gogona Saikia, "Union Bank's July 2016 Crisis—$171mn Hacked," NewsBytes, April 17, 2017, https://www.newsbytesapp.com/news/business/how-union-bank-prevented-a-171mn-heist/story#:~:text=Business%20In%20July'16,%20Union%20Bank%20of%20India%20faced,to%20get%20back%20every%20cent%20within%2060%20hours (accessed August 6, 2021).
138. *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, p. 17.
139. Press release, "Interpark Personal Information Hacking Process Determined by North's Action," Government of the Republic of Korea, National Police Agency, July 28, 2016, https://www.korea.kr/news/pressReleaseView.do?newsId=156144599&pageIndex=1 (accessed August 6, 2021), and United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, March 5, 2019, p. 50.
140. Matthew Pennington, "NKorea Said to Have Stolen a Fortune in Online Bank Heists," Associated Press, October 3, 2018, https://apnews.com/article/north-america-hacking-ap-top-news-north-korea-pyongyang-f6822f1313e2499883348a5615d2dbed (accessed August 6, 2021), and U.S. Department of Homeland Security, Cyberstructure and Infrastructure Security Agency, "Alert TA18-275A): Hidden Cobra–FASTCash Campaign," last revised December 21, 2018, https://us-cert.cisa.gov/ncas/alerts/TA18-275A (accessed August 6, 2021).
141. Oleg Kolesnikov, "Securonix Threat Research: Cosmos Bank SWIFT/ATM US$13.5 Million Cyber Attack Detection Using Security Analytics," Securonix, August 27, 2018, https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/ (accessed August 6, 2021), and Ben Buchanan, "How North Korean Hackers Rob Banks Around the World," *Wired*, February 28, 2020, https://www.wired.com/story/how-north-korea-robs-banks-around-world/ (accessed August 6, 2021).
142. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 30, 2019, p. 109, and U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Alert (AA20-239A): FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," October 24, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a (accessed August 6, 2021).
143. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 30, 2019, p. 109, and *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, p. 17.
144. Michelle F. Davis, "Mexico Foiled a $110 Million Bank Heist, Then Kept It a Secret," Bloomberg, May 29, 2018, https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret (accessed August 6, 2021), and *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, p. 18.
145. Reuters, "Bank of Chile Trading Down After Hackers Rob Millions in Cyberattack," June 11, 2018, https://www.reuters.com/article/us-chile-banks-cyberattack/bank-of-chile-trading-down-after-hackers-rob-millions-in-cyberattack-idUSKBN1J72FC (accessed August 6, 2021).
146. *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*," p. 23.
147. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 30, 2019, p. 110.
148. Ibid.
149. Ibid.
150. Ibid.
151. *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, p. 18.
152. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 30, 2019, p. 110.
153. Ibid.
154. Ibid.
155. Ibid.
156. Ibid., pp. 111 and 112.
157. Ibid., p. 111.
158. Ibid.
159. Ibid.
160. Ibid.
161. *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, p. 18.

162. Ibid., p. 19.
163. Press release, "Kapersky Researchers Find Lazarus Enhances Capabilities in AppleJeus Cryptocurrency Attack," Kaspersky, January 8, 2020, https://usa.kaspersky.com/about/press-releases/2020_lazarus-enhances-capabilities-in-applejeus-cryptocurrency-attack (accessed August 6, 2021).
164. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 30, 2019, p. 112.
165. Ibid.
166. Huillet, "Report: North Korea-Sponsored Hacks Comprise 65 Percent of Total Crypto Stolen."
167. 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," p. 4.
168. *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, p. 22.
169. Mike Orcutt, "How the North Korean Hackers Behind WannaCry Got Away with a Stunning Crypto-Heist," *MIT Technology Review*, January 24, 2020, https://www.technologyreview.com/2020/01/24/276082/lazarus-group-dragonex-chainalysis/ (accessed August 6, 2021).
170. Caileam Raleigh, "UPbit Loses $49 Million Worth of Crypto in Major Hack," CryptoCurrencyNews, November 27, 2019, https://cryptocurrencynews.com/upbit-eth-crypto-hack/ (accessed August 6, 2021).
171. "Lazarus Group Pulled off 2020's Biggest Exchange Hack and Appears to Be Exploring New Money Laundering Options."
172. *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, p. 22.
173. "Lazarus Group Pulled off 2020's Biggest Exchange Hack and Appears to Be Exploring New Money Laundering Options."
174. Gertrude Chavez-Dreyfuss, "Crypto Crime Slows in 2020, But 'DeFi' Hacks Rise: CipherTrace Report," Reuters, November 10, 2020, https://www.businessinsider.com/crypto-crime-slows-in-2020-but-defi-hacks-rise-ciphertrace-report-2020-11?utm_source=markets&utm_medium=ingest (accessed August 6, 2021).
175. CYFIRMA, "Global Covid 19-Related Phishing Campaign by North Korean Operatives Group Lazarus Group Exposed by CYFIRMA Researchers," June 18, 2020, https://www.cyfirma.com/early-warning/global-covid-19-related-phishing-campaign-by-north-korean-operatives-lazarus-group-exposed-by-cyfirma-researchers/ (accessed August 6, 2021).
176. Andrew Jeong, "North Korean Hackers Are Said to Have Targeted Companies Working on Covid-19 Vaccines," *The Wall Street Journal*, updated December 2, 2020, https://www.wsj.com/articles/north-korean-hackers-are-said-to-have-targeted-companies-working-on-covid-19-vaccines-11606895026 (accessed August 6, 2021).
177. Tom Burt, "Cyberattacks Targeting Health Care Must Stop," Microsoft, November 13, 2020, https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (accessed August 6, 2021).
178. Shannon Vavra, "Pyongyang Hackers Eye More Coronavirus Research, Kaspersky Says," CyberScoop, December 23, 2020, https://www.cyberscoop.com/north-korea-lazarus-group-coronavirus-kaspersky/ (accessed August 6, 2021), and press release, "Kaspersky Reveals Two Lazarus Attacks Targeting Vaccine Research," Kaspersky, December 23, 2020, https://usa.kaspersky.com/about/press-releases/2020_kaspersky-reveals-two-lazarus-attacks-targeting-vaccine-research (accessed August 6, 2021).
179. Yoonjung Seo, Gawon Bae, and Joshua Berlinger, "South Korean Lawmaker and Spy Agency Dispute Whether North Korean Hackers Stole Pfizer Covid-19 Data," CNN, updated February 17, 2021, https://www.cnn.com/2021/02/17/asia/north-korea-pfizer-intl-hnk/index.html (accessed August 6, 2021).
180. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "North Korea Cyber Threat Overview and Advisories," February 17, 2021, https://us-cert.cisa.gov/northkorea (accessed August 6, 2021).
181. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Imposition of Special Measure Against North Korea as a Jurisdiction of Primary Money Laundering Concern," Final Rule, *Federal Register*, Vol. 81, No. 217 (November 9, 2016), pp. 78715–78722, https://www.federalregister.gov/documents/2016/11/09/2016-27049/imposition-of-special-measure-against-north-korea-as-a-jurisdiction-of-primary-money-laundering (accessed August 6, 2021).
182. Press release, "Treasury Targets North Korea for Multiple Cyber-Attacks," U.S. Department of the Treasury, September 6, 2018, https://home.treasury.gov/news/press-releases/sm473 (accessed August 6, 2021).
183. *In re Sealed Case*, No. 19-5068, United States Court of Appeals for the District of Columbia Circuit, Decided July 30, 1919, Reissued August 6, 2019, https://www.cadc.uscourts.gov/internet/opinions.nsf/6E2FAD8DB7F6B3568525844E004D7A26/$file/19-5068-1800815.pdf (accessed August 6, 2021).
184. Faruqui, Liu, and Moustafa, "The Long Arm of U.S. Law: The Patriot Act, the Anti-Money Laundering Act of 2020 and Foreign Banks.".
185. Press release, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups."
186. Shannon Vavra, "Pentagon, FBI, DHS Jointly Expose a North Korean Hacking Effort," CyberScoop, February 14, 2020, https://www.cyberscoop.com/hidden-cobra-malware-north-korea-fbi-dhs-dod-virus-total/ (accessed August 6, 2021).

187. News release, "Two Chinese Nationals Charged with Laundering over $100 Million in Cryptocurrency from Exchange Hack," U.S. Department of Justice, March 2, 2020, https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack (accessed August 6, 2021).

188. *United States of America, Plaintiff v. Ko Chol Man, Kim Song Ui, Han Ung, Ri Jong Nam, Jo Un Hui, O Song Hui, Ri Myong Jin, Ri Jong Won, Jong Suk Hui, Kim Tong Chol, Kim Chin a/k/a Kim Jin, Huang Hailin, Huang Yueqing, Jin Yonghe, Ri Chun Hwan, Sun Wei, Ri Chun Hwan, Kim Hui Suk, Han Yang Chol, Ri Chun Song, Ri Jong Chol, Kim Kwang Chol, Ri Yong Su, Ku Ja Hyong, Jin Yonghuan, Kwon Song Il, Ryu Myong Il, Hyon Yong Il, Hwang Won Jun, Han Ki Song, Han Jang Su, Ri Myong Hun, Kim Kyong Nam, and Kim Hyok Ju, Defendants*, United States District Court for the District of Columbia, Case 1:20-cr-00032-RC, Indictment, filed February 5, 2020, https://freekorea.us/wp-content/uploads/2020/05/show_temp-76-1.pdf (accessed August 6, 2021).

189. Spencer S. Hsu and Ellen Nakashima, "U.S. Brings Massive N. Korean Sanctions Case, Targeting State-Owned Bank and Former Government Officials," *The Washington Post*, May 28, 2020, https://www.washingtonpost.com/local/legal-issues/us-brings-largest-ever-n-korean-sanctions-case-targeting-state-owned-bank-and-senior-government-officials/2020/05/28/3b23f616-a02b-11ea-b5c9-570a91917d8d_story.html (accessed August 6, 2021).

190. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Malware Analysis Report (AR20-232A): MAR-10295134-1.v1–North Korean Remote Access Trojan: BLINDINGCAN," August 19, 2020, https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a (accessed August 6, 2021).

191. News release, "United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors," U.S. Department of Justice, August 27, 2020, https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges (accessed August 6, 2021).

192. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Alert (AA20-239A): FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks."

193. Andrew W. Lehren and Dan De Luce, "Secret Documents Show How North Korea Launders Money Through U.S. Banks," NBC News, September 20, 2020, https://www.nbcnews.com/news/world/secret-documents-show-how-north-korea-launders-money-through-u-n1240329 (accessed August 6, 2021).

194. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Alert (AA20-301A): North Korean Advanced Persistent Threat Focus: Kimsuky."

195. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Alert (AA21-048A): AppleJeus: Analysis of North Korea's Cryptocurrency Malware," last revised April 15, 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-048a (accessed August 6, 2021).

196. News release, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," and *United States of America, Plaintiff v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, Defendants*, pp. 4, 5, 16.

197. News release, "First North Korean National Brought to the United States to Stand Trial for Money Laundering Offenses," U.S. Department of Justice, March 22, 2021, https://www.justice.gov/opa/pr/first-north-korean-national-brought-united-states-stand-trial-money-laundering-offenses (accessed August 6, 2021), and *United States v. Mun Chol Myong*, United States District Court for the District of Columbia, Case No. 19-CR-00147 (RC), Motion to Unseal, March 21, 2021, https://www.nknews.org/wp-content/uploads/2021/03/Mun-Chol-Myong-indictment.pdf?t=1624377604227 (accessed August 6, 2021).

214 Massachusetts Ave., NE | Washington, DC 20002
(202) 546-4400 | heritage.org