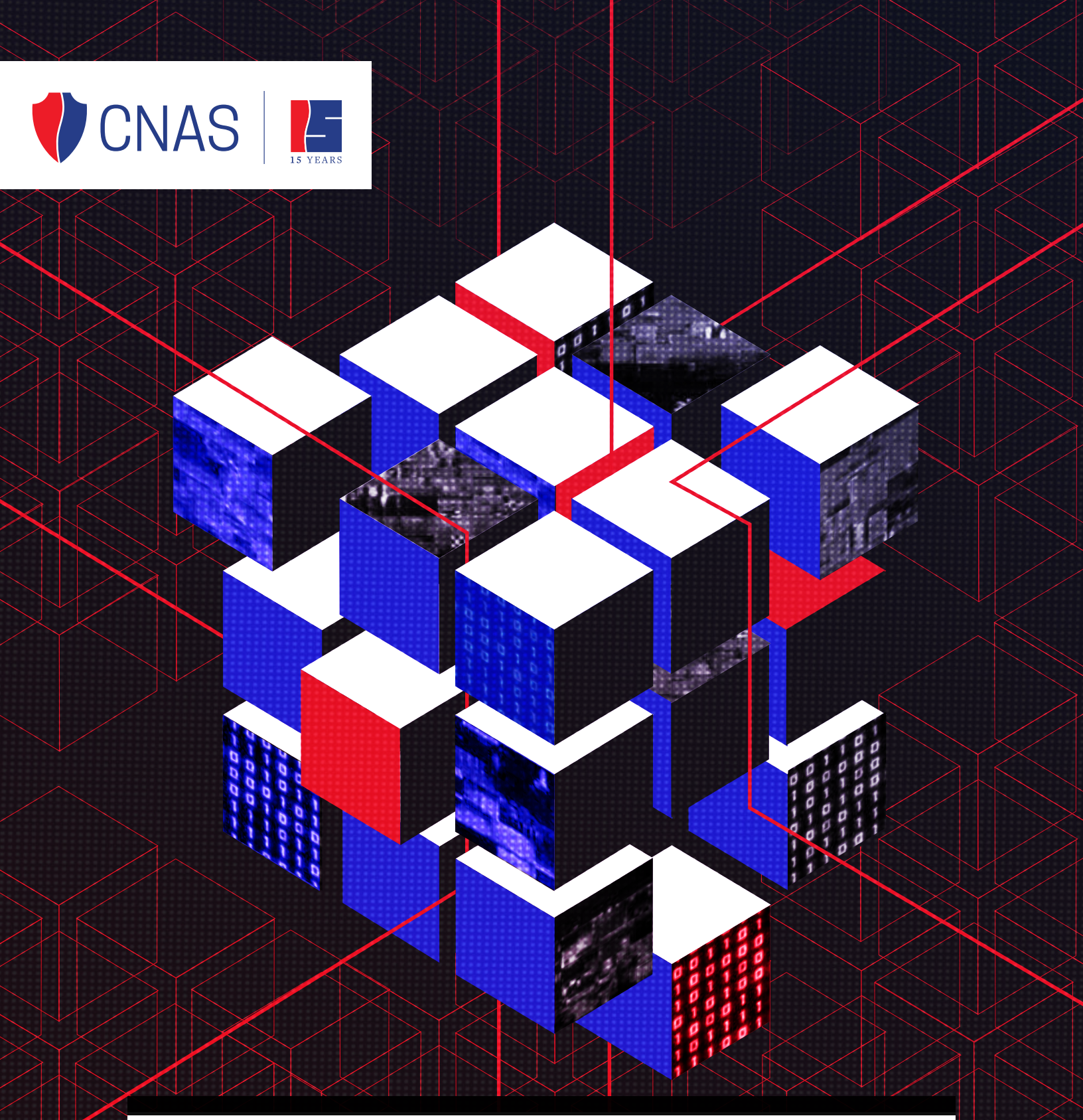
CNAS | 15 YEARS



NOVEMBER 2022

U.S.-ROK Strategy for Enhancing Cooperation on Combating and Deterring Cyber-Enabled Financial Crime

Jason Bartlett

About the Author

Jason Bartlett was a Research Associate for the Energy, Economics, and Security Program at CNAS. He analyzed developments and trends in sanctions policy and evasion tactics, proliferation finance, and cyber-enabled financial crime with a regional focus on North Korea and U.S.-ROK (Republic of Korea) cyber strategy. He also led research and writing for the program's *Sanctions by the Numbers* series and was the 2022 recipient of the 1LT Andrew J. Bacevich Jr., USA Award. Previously, Bartlett worked at several think tanks in Washington, D.C., and Seoul, South Korea, and he provided years of linguistic and administrative assistance to human rights groups resettling North Korean defectors in South Korea and the United States. Fluent in Korean and Spanish, Bartlett graduated from the Korean Language Institute at Yonsei University in Seoul, and also holds an MA in Asian Studies from the School of Foreign Service, a graduate certificate in Refugee and Humanitarian Emergencies from Georgetown University, and a BS in Spanish and BA in International Studies from the State University of New York at Oneonta. In addition to the Bacevich Award, Bartlett was a recipient of the Critical Language Scholarship (2018) and Boren Fellowship (2018–19) issued by the U.S. Departments of State and Defense, as well as a recipient of the South Korean National Institute for Unification Education Emerging Leaders Fellowship (2021) and the U.S.-ROK Next Generation Leaders Program (2021) at the National Bureau of Asian Research.

About the Energy, Economics, and Security Program

The Energy, Economics, and Security Program explores the changing global marketplace and implications for U.S. national security and foreign policy. In a highly interconnected global financial and trade system, leaders must increasingly leverage economic and financial assets to defend and promote U.S. national interests. The Energy, Economics, and Security Program develops practical strategies to help decisionmakers understand, anticipate, and respond to these developments.

Acknowledgments

The author would like to thank Emily Kilcrease, Nick Carlsen, Dr. John Park, David J. Park, Dr. Go Myong-Hyun, and Dr. So Jeong Kim for their feedback and review of this report, as well as Euihyun Bae and Michael Frazer for their contributed research and citation support. The author thanks all U.S. and South Korean researchers and government officials who participated in private roundtables and interview sessions, especially those affiliated with the U.S. Departments of State and the Treasury, TRM Labs, the Asan Institute for Policy Studies, the Institute for National Security Strategy, the Sejong Institute, the School of Cybersecurity at Korea University, the Embassy of the Republic of Korea in the USA, and the Republic of Korea's Ministry of Foreign Affairs. The author acknowledges the editorial and production efforts of the publications and communications team at CNAS, in particular Maura McCarthy, Melody Cook, Emma Swislow, Rin Rothback, and Anna Pederson. This report was made possible with the generous support of the Korea Foundation.

A Korean translation of this report is available.

TABLE OF CONTENTS

01 Executive Summary

02 Introduction

03 Current Challenges to Enhancing U.S.-ROK Cyber Coordination

07 Evolution of North Korea's Cyber Program

11 Policy Recommendations

13 Conclusion

14 Appendix: Understanding the Major U.S. and ROK Goverment Players to Combat and Deter State-Sponsored Cyber-Enabled Financial Crime

Executive Summary

The May 2022 U.S.-ROK Summit between President Joe Biden and President Yoon Suk-yeol revitalized previous bilateral commitments to establish a joint cyber working group to address the growing issue of cyber-enabled financial crime with specific emphasis on cryptocurrency, blockchain technology, and illicit North Korean cyber activity.[1] This report provides specific policy recommendations for Washington and Seoul to incorporate within the cyber working group to enhance cooperation on combating and deterring cyber-enabled financial crime, especially from state-sponsored actors.

North Korea has become the greatest state-sponsored threat to the global financial services sector. From 2021 to June 2022 alone, North Korean cyber operatives and their facilitators stole more than $1 billion (in U.S. currency, as throughout this report unless otherwise indicated) in digital assets through hacking cryptocurrency exchanges and laundering the stolen funds using various financial technologies and obfuscation techniques, including cryptocurrency mixers and foreign over-the-counter brokers.[2] Pyongyang will likely maintain this position as long as the potential gains of cyber operations against financial services are greater than the potential risks and resources needed to conduct these operations. Washington and Seoul must work together to change this reality.

This report compiles the findings of a year-long research project to generate actionable policy recommendations for Washington and Seoul to incorporate within their joint cyber working group to strengthen joint deterrence against state-sponsored cyber-enabled financial crime that continues to target both U.S. and South Korean social, financial, and cyber infrastructure. Based on intensive field research and interviews with U.S. and ROK stakeholders, this report outlines current challenges to enhancing U.S.-ROK cyber coordination, details the evolution of North Korea's cyber program and modern-day threats, provides policy recommendations for the joint cyber working group, and includes an appendix with all relevant U.S. and ROK agencies that can contribute valuable expertise to the group.

ROMANIZATION OF KOREAN NAMES

This report romanizes North Korean names from standard Korean into English according to the Democratic People's Republic of Korea's version of the McCune-Reischauer Korean language romanization system. For example, 김정은 is written as "Kim Jong Un" instead of "Kim Jong-un," without hyphenation. South Korean names are romanized from standard Korean into English according to the Republic of Korea's variant of the McCune-Reischauer Korean language romanization system. For example, 김대중 is written as Kim Dae-jung. However, in the case of external Korean reviewers for this report, the author has romanized their names according to the reviewer's personal preference.

METHODOLOGY

The project involved a series of private roundtables and structured interviews with leading U.S. and ROK legislators and policymakers, intelligence and law enforcement officers, national security experts, cybersecurity analysts, and private sector researchers dealing with North Korea, cyber-enabled financial crime, cryptocurrency, blockchain analytics, malware, and DeFi platforms. In order to ensure an equal balance between U.S. and ROK contributions, this project included overseas research in South Korea to gather information on current strategies within the South Korean government, private sector, and think tank community for researching and combating cyber-enabled financial crime. The author conducted all research and interviews in both English and Korean language to facilitate optimum engagement from U.S. and ROK counterparts, as well as to reinforce the importance of joint dialogues between Washington and Seoul.

Main Takeaways

- North Korea began developing a cyber program in the mid-1980s that was supported by both domestic innovation and foreign assistance.
- Starting in the late 2000s, Pyongyang launched offensive cyber operations against South Korean government agencies, businesses, research organizations, traditional financial institutions, North Korean defectors who had resettled, and ordinary South Korean citizens for mostly politically motivated reasons.
- North Korean cybercrime significantly evolved between 2015 and 2016, with a rapid increase in cyber operations targeting both traditional and non-traditional financial institutions and technology such as cryptocurrency, blockchain, and later, decentralized finance platforms.
- Washington and Seoul possess different, but complementary, expertise and capabilities related to curbing cyber-enabled financial crime that should be considered within the joint U.S.-ROK cyber working group revitalized during the May 2022 U.S.-ROK Summit.
- Key bureaucratic and logistical differences exist between Washington and Seoul regarding how they perceive and respond to North Korea–related threats that have prevented enhanced cooperation, including:
  - » Political oscillation in Seoul pertaining to North Korean policy;
  - » Discrepancies in U.S. and ROK government perception and resource allocation toward certain state-sponsored cyber threats;
  - » Difficulties in properly identifying U.S.-ROK government agency counterparts.

Summary of Recommendations

The following policy recommendations seek to offer guidance to the joint U.S.-ROK cyber working group to enhance bilateral cooperation on combating and deterring cyber-enabled financial crime, with specific emphasis on state-sponsored cybercrime from actors such as North Korea. Washington and Seoul should:

1. Establish a research agenda for the U.S.-ROK cyber working group to identify exploitable vulnerabilities in state-sponsored cybercrime strategy, with an initial focus on North Korea.
2. Identify specific representatives from relevant U.S. and ROK government agencies to participate in the joint cyber working group. This will improve routine information sharing and joint investigations.
3. Consider the joint cyber working group as a U.S.-ROK partnership to protect against *any* state-sponsored cyber-enabled financial crime operations.
4. Issue a joint advisory guidance document on potential cybersecurity and financial risks related to social engineering hacks. This will build trust and rapport with the private sector while attempting to stymie cyber-enabled financial crime tactics.
5. Organize an external advisory team of leading U.S. and ROK nongovernment researchers and private sector analysts who work on issues pertaining to the agenda of the joint working group and can offer outside assistance and advice.

Introduction

The United States and South Korean governments have developed significantly different approaches to address state-sponsored cyber-enabled financial crime with specific regard to North Korea. Actors such as North Korea have rapidly adopted cryptocurrency and related financial technology as an increasingly preferred tool to facilitate cyber-enabled financial crime, and this development has highlighted the need for enhanced cooperation between Washington and Seoul. Given Pyongyang's national priority to evade economic sanctions and expand its nuclear weapons arsenal, this massive influx of currency into North Korea raises significant security concerns for both the United States and South Korea.

While a rapidly growing number of illicit North Korean cyber activity targets the financial sector, other cybercrime state sponsors, including China and Russia, present different cybersecurity risks to the United States and South Korea, as they often target government agencies and infrastructure for information espionage, technology theft, and system shutdowns. Although the current focus of the U.S.–Republic of Korea (ROK) joint cyber working group is on North Korea–sponsored cyber-enabled financial crime efforts, Washington and Seoul should consider future research that includes cyber threats from other state-sponsored actors.

Current Challenges to Enhancing U.S.-ROK Cyber Coordination

Since the Korean War began in 1950, Washington and Seoul have enjoyed a strong social, economic, and military alliance that continues into the modern day. However, significant political, logistical, and bureaucratic challenges impede enhanced joint government-level cooperation to address current cybersecurity threats. When pursuing enhanced cooperation on any security issue related to Pyongyang, the United States and South Korea must fully understand variations in how they perceive and respond to North Korean threats. For example, the political oscillation of North Korean policy within Seoul, discrepancies in U.S. and ROK government perception and resource allocation toward certain state-sponsored cyber threats, and difficulties in properly identifying U.S.-ROK government counterparts are three major challenges to overcome.

Political Oscillation of North Korea Policy within Seoul

While U.S. foreign policy toward Pyongyang has been relatively the same under both Republican and Democratic presidents, Seoul's foreign policy toward Pyongyang varies significantly under left-leaning and right-leaning presidents. This naturally leads to difficulties in securing a long-lasting joint U.S.-ROK response to North Korean aggression. Although conservative South Korean president Yoon Suk-yeol currently occupies the Blue House (the South Korean equivalent of the White House), Seoul will likely rethink any hardline policies targeting North Korea after a left-leaning president is elected.[3] This was recently shown when left-leaning former ROK President Moon Jae-in suggested in 2017 and later decided to postpone and reduce joint U.S.-ROK military drills to demonstrate good faith to North Korean leader Kim Jong Un during peace talks.[4] Previous left-leaning presidents such as Kim Dae-jung and Roh Moo-hyun also pursued active engagement with North Korean leaders, while former conservative presidents, such as Lee Myung-bak and Park Geun-hye, sought to strengthen joint military deterrence with the United States and engage with North Korea only after Pyongyang had satisfied certain conditions and agreements with Seoul. To ensure the longevity of the U.S.-ROK cyber working group, it is crucial for Washington and Seoul to categorize the group as joint deterrence against *any* state-sponsored cyber-enabled financial crime, not only that from North Korea, to remove any possible stigmatization of the working group because of perceptions that it serves a primarily anti–North Korea purpose.

Discrepancies in Government Perception and Resource Allocation

The U.S. and South Korean governments perceive the North Korean cyber threat in different ways, especially by comparison with how they see other state-sponsored cyber actors. This difference will impact the amount of government resources allocated to relevant agencies tasked with responding to the issue. In terms of North Korean cyber threats, typically the United States takes a more reactive approach, while South Korea tends to adopt more preventive measures to brace against inevitable North Korean cyberattacks.

To ensure the longevity of the U.S.-ROK cyber working group, it is crucial for Washington and Seoul to categorize the group as joint deterrence against *any* state-sponsored cyber-enabled financial crime, not only that from North Korea.

In the United States, repelling cyberattacks from Moscow and Beijing has traditionally dominated cybersecurity resource expenditure and bandwidth.[5] Pyongyang often falls into a "second tier" category within high-risk state-sponsored cyber threats, behind Moscow and Beijing, for several potential reasons: Russian and Chinese offensive cyber capabilities more evenly match those of the United States; Russia and China enjoy a wider spy network with more potential permeability into the U.S. government; and both countries have a more robust weapons arsenal and technological threat currently unmatched by North Korea.[6] Also, and perhaps most importantly, Russian and Chinese state-sponsored hackers tend to target U.S. government agencies, officials, and infrastructure, while North Korean hackers more commonly target the South Korean government and global financial institutions. Current U.S. Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger challenged this narrative in late July during a CNAS event in which she refused to categorize North Korea beneath other cyber actors, claiming that the country "uses cyber to gain, we estimate, up to a third of their funds for their missile program."[7] However, it is unclear whether North Korea will remain a major cyber priority for the White House in the event of increased cyberattacks from Russia and China.

In contrast, South Korea views North Korea as its largest cyber, military, and financial security threat. Russia and China have also targeted South Korean social, technological, and economic infrastructure through disruptive cyberattacks, but not with the same frequency as North Korea. In 2020, South Korean government officials estimated that North Korea was responsible for approximately 90 percent of all cyberattacks against South Korea, with 40 percent of North Korean cyber operations targeting South Korean financial institutions and cryptocurrency.[8] In the same year, the South Korean National Intelligence Service (NIS) indicated that North Korea had launched an average of 1.5 million cyberattacks a day on South Korean financial and social infrastructure, marking a dramatic increase from 410,000 in 2016, when Pyongyang first began to heavily target the financial services sector.[9] The sheer volume of constant North Korean cyberattacks has significantly contributed to South Korea's understanding of North Korean tactics, techniques, and procedures (TTPs) and cyber strategy, and this likely informs Seoul's cybersecurity posture. Given that South Korean financial, social, and cyber infrastructure has not collapsed under relentless North Korean cyberattacks, South Korea can likely offer effective solutions to foreign nations, including the United States, as it looks to improve its own national deterrence against state-sponsored cyberattacks.

Difficulties in Properly Identifying U.S.-ROK Government Agency Counterparts

Key bureaucratic and logistical differences between how Washington and Seoul perceive and address North Korea–related security threats have led to decision stalemates, reduced information sharing, and delayed joint responses that can present more opportunities for illicit cyber actors to exploit.

Unlike Washington, which can access expertise from a wide range of U.S. government agencies dealing with threats related to North Korea, cybersecurity, and financial crime, Seoul mainly responds to all North Korean threats through a single intelligence agency, the National Intelligence Service (국가정보원). This can restrict the diversity of South Korea's response to evolving North Korean threats, such as cyber-enabled financial crime. Although South Korea possesses many other government agencies that provide supportive security expertise regarding cybersecurity and financial crime, such as the Korean National Police Agency (KNPA) and Korea Financial Intelligence Unit (KoFIU), all security threats to South Korea that involve North Korea are typically handled under the umbrella of the NIS. While the NIS does have separate offices and units that focus on various national security threats, this bottleneck effect on responding to North Korea can prevent helpful coordination and exacerbate logistical difficulties in addressing the diverse cyber threats that North Korea poses.

Key bureaucratic and logistical differences between how Washington and Seoul perceive and address North Korea–related security threats have led to decision stalemates, reduced information sharing, and delayed joint responses that can present more opportunities for illicit cyber actors to exploit.

This system significantly differs from the U.S. approach, which leverages the capabilities of various U.S. government agencies, including organizations outside of the intelligence community, to share the logistical burden of responding to the unique threats North Korea poses, including cybercrime. However, this report does not suggest a restructuring of South Korean bureaucracy or the NIS, but rather seeks to highlight the importance of a joint U.S.-ROK cyber working group to facilitate enhanced cooperation on cyber-enabled financial crime outside of typical South Korean bureaucratic and logistical restrictions.

Another major hurdle to enhancing U.S.-ROK coordination is related to cross-government information sharing. Since there is no single U.S. counterpart that deals with North Korea like the NIS, Seoul has difficulty identifying the correct U.S. government channel, agency, or department to relay important security-related information. As a result, this reduces the speed of sharing crucial, time-sensitive information on illicit cyber activity with the correct corresponding U.S. agency. Additionally, this can create underlying tension and unnecessary caution between U.S. and ROK government agencies. From South Korea's perspective, when its primary intelligence agency, the NIS, shares top secret clandestine information with a foreign non-intelligence agency, it may be seen more like "information taking" than "information sharing." Several former South Korean government officials mentioned this specific terminology during interviews for this report.

Domestic Innovation and Foreign Assistance[16]
1984–2017

1984–1986

MIRIM COLLEGE

Kim Jong Il ordered the establishment of Mirim College (미림대학) to educate and train "cyber warriors" for the regime. North Korea also signed a cooperation agreement with the Soviet Union and invited about 40 Soviet professors to teach computer science at Mirim College.

1988

CHINESE UNIVERSITIES

Dating back to 1988, universities such as the Harbin Institute of Technology have maintained and renewed educational partnerships with leading North Korean universities known to produce state-sponsored hackers, for example Kim Il Sung University and Kim Chaek University of Technology.

Early 1990s

CYBER WARRIORS

The first 100 cyber warriors graduated from Mirim College and entered their assigned intelligence offices within the government and military with training on cyber warfare, technical reconnaissance, and software engineering and coding.

1999

THE YEAR OF SCIENCE

Kim Jong Il declared 1999 as "The Year of Science," emphasizing the importance of software program development over hardware. North Korean state media also reported that the Korea Computer Center (KCC) had developed "comprehensive computing technology including software development and production process control," adding that it had employed about 800 people for research and development.[17]

2002

U.S.-DPRK ACADEMIC PARTNERSHIP

Starting in 2002, U.S. university professors and North Korean computer science scholars engaged in more than 10 joint training programs in Pyongyang and New York. This was the first, and only, official educational partnership between U.S. and North Korean universities.

Mid-2000s

HACKER HOTSPOTS IN CHINA

North Korean cyber operatives reportedly used businesses in China, such as the Chilbosan Hotel, as internet-connected safe havens to train hackers and conduct cyberattacks against foreign targets.

2017

TELECOMMUNICATIONS DEAL WITH RUSSIA

After an alleged deal was signed in 2009 between Moscow and Pyongyang, in 2017 the Russian state-owned telecommunications company TransTeleCom provided an additional internet connection line to North Korea to improve its bandwidth and speed. TransTeleCom and Unicom reportedly handled roughly 60 percent and 40 percent respectively of North Korea's internet traffic during this year.

1986–1991

PYONGYANG INFORMATICS/INFORMATION CENTER (PIC)

Created in 1986 and expanded in 1991 with financial support from North Korean sympathizers in Japan and the United Nations Development Programme, the PIC became a major developer of North Korean software, ranging from word processing and embedding software into web applications to creating information firewalls.

1990

KOREA COMPUTER CENTER

The KCC began to play an important role in training North Koreans in computer science–related occupations, mainly information technology (IT). The U.S. Treasury sanctioned the KCC in 2017 for illegally dispatching North Korean IT workers abroad to earn currency for Pyongyang.

Late 1990s–Early 2000s

ROK SUNSHINE POLICY

Seoul and Pyongyang collaborated on information and communications technology (ICT) and computer training projects for almost 10 years. This included sending South Korean university professors and practitioners to Kim Il Sung University as well as the KCC, which was affiliated with the Kim Chaek University of Technology, to teach computer science, including operating systems design.

2000–2001

THE INTRANET

Pyongyang created the Kwangmyeong intranet and an associated firewall system with help from the Central Scientific and Technological Information Agency, the PIC, and KCC to control, monitor, and block outside flows of information into the country. This likely required Pyongyang to develop hacking techniques to test the system's resiliency, and North Korea later applied these techniques to cyberattacks on foreign targets.

2009

TELECOMMUNICATIONS DEAL WITH THAILAND

Pyongyang partnered with a Thai telecommunications company called Loxley Pacific to create the first fiber optic links to the internet.

2010

TELECOMMUNICATIONS DEAL WITH CHINA

The Chinese state-owned telecommunications company Unicom provided enhanced internet connection services to Pyongyang and reportedly began to manage most of North Korea's internet links.

KEY

- Domestic Innovation
- Foreign University Partnerships
- Foreign Business Partnershps
- Overseas Hacking Assistance

Washington and Seoul enjoy different logistical capabilities and legal authorities to apply against illicit state actors in the cyber space. The United States has the unique ability to leverage unilateral economic sanctions capable of isolating a target from the global financial market through restricting its access to the U.S. dollar. The Treasury alone has designated nearly 130 individuals and entities under North Korea–related sanctions programs specific to illicit cyber activity.[10] While South Korea does have its own government agencies that address illicit financial activity, Seoul does not enjoy the same level of economic influence as the United States, because it cannot levy unilateral economic sanctions. Rather, South Korea acts to comply with, and enforce, existing U.S. and U.N. economic sanctions related to North Korea. Therefore, South Korea must rely on other tools to curb the growth of North Korean cyberattacks, such as increased cyber deterrence strategies and collecting information on pending operations.

Seoul has a comparative advantage in collecting intelligence on North Korea for several reasons. North Korea is the primary security threat and aggressor toward South Korea, meaning that most South Korean intelligence collection efforts focus on North Korea, whereas the United States likely prioritizes collecting intelligence on Chinese and Russian operations. South Korea's constant exposure to illicit North Korean cyber activity has granted Seoul greater institutional knowledge regarding cyber behaviors and techniques indicative of North Korean involvement. North and South Korea share the same language, albeit with certain linguistic variations similar to the slight differences between American and British English, and this contributes to faster information collection and analysis. Lastly, the shared ethnicity between North and South Korea, much like the language, allows for easier acquisition of valuable human intelligence that can help inform South Korean intelligence officers and policymakers.

Evolution of North Korea's Cyber Program

Pyongyang has been developing an offensive cyber program within its education, military, and intelligence institutions for roughly 35 years. Understanding the origins and developments behind North Korean cybercrime, including its domestic and foreign contributors, is key to ensuring a multifaceted cybersecurity strategy that Washington and Seoul can successfully apply to the diverse cyber threats emanating from state-sponsored actors such as North Korean cyber operatives.

Major Milestones in North Korea's Cyber Program

North Korea began developing a cyber program in the mid-1980s, and it has evolved over time because of rapid domestic innovation and continuous foreign assistance from leading universities, institutions, businesses, and national governments.[11] In the initial stages of development, Pyongyang established three domestic institutions, Mirim College, the Korea Computer Center (KCC), and the Pyongyang Informatics/Information Center (PIC) to jumpstart the country's cyber program, and each later played major roles in transforming North Korean cyber capabilities into an illicit currency-generating scheme for Pyongyang.

While South Korea does have its own government agencies that address illicit financial activity, Seoul does not enjoy the same level of economic influence as the United States, because it cannot levy unilateral economic sanctions.

The first wave of North Korean cyberattacks mainly targeted South Korean government agencies, websites, and military infrastructure after Seoul and Washington returned to their defense posture following the collapse of the Sunshine Policy in the late 2000s.[12] In line with the steady increase of economic sanctions and the rising popularity of Bitcoin and other cryptocurrency coins in the mid-2010s, Pyongyang began to expand its illicit cyber operations to include more financial institutions and foreign targets outside the Korean Peninsula, with a notable shift toward cryptocurrency exchanges and blockchain technology starting in 2016–17.[13] Research has shown that North Korean hackers apply a wide range of intrusion and extortion tactics effective against financial institutions, such as spear phishing campaigns, ransomware, and bank drops, as well as denial of service and supply chain attacks.[14]

Under its current leader, Kim Jong Un, North Korea has become the greatest state-sponsored cyber threat to the global financial services sector. Pyongyang has improved its cyber capabilities through enhanced civil-military fusion projects and reduced operational gaps between the country's military agencies and its computer science institutions.[15] However, the most significant achievement for North Korea's cyber program under Kim Jong Un is its ability to procure billions of dollars' worth of stolen funds for Pyongyang, despite economic sanctions that have prevented significant growth in virtually all other commercial trade industries.

Continued Technical, Educational, and Industrial Support from Beijing and Moscow

Beijing has directly supported Pyongyang's illicit cyber operations through blatantly evading sanctions that would target North Korea. During the 2000s, North Korean cyber operatives reportedly used hotels in northeast China, such as the Chilbosan Hotel (沈阳七宝山饭店有限公司), to illicitly earn funds for Pyongyang through providing IT services to foreign customers.[18] During this time, North Korean actors also conducted overseas cyber operations using Chinese internet service providers, while Pyongyang was expanding its domestic capabilities.[19] This trend has continued, as Pyongyang has sent North Korean hackers abroad to China to moonlight as IT workers or in other professions at Chinese–North Korean front companies, while conducting state-sponsored illicit cyber activity. The most famous example is Park Jin Hyok (박진혁), a North Korean cyber operative affiliated with the Lazarus Group, a leading North Korean state-sponsored hacking agency under the direction of the country's primary intelligence service, the Reconnaissance General Bureau (정찰총국).[20] The FBI and the U.S. Department of Justice have attributed several destructive and disruptive North Korean cyber operations to Park, including the 2014 Sony Pictures Entertainment hack, the 2016 Bangladesh Central Bank heist, and the 2017 WannaCry 2.0 ransomware attack.[21] Both the U.S. government and the U.N. have claimed that China and Russia continue to employ North Korean laborers in violation of international sanctions. These countries have both hired North Korean IT workers who illicitly procure funds for the Kim regime and are positioned to contribute to offensive cyber operations such as those conducted by Park.[22]

Beijing has also continued to pursue academic partnerships with North Korean universities related to computer science and technology. Dating back to 1988, Chinese universities such as the Harbin Institute of Technology have maintained and renewed official exchange agreements with leading computer science universities in North Korea, including Kim Chaek University of Technology and Kim Il Sung University in 2013.[23] In 2019, North Korean computer science students representing Kim Chaek University earned a silver medal at the annual International Collegiate Programming Contest (ICPC), ranking in eighth place and outcompeting several prestigious universities from the United States, South Korea, and China, including Stanford University, the Korea Advanced Institute of Science and Technology, and Peking University.[24] The [North] Korean Central News Agency (KCNA) later honored their accomplishment during a national broadcast, highlighting the importance to Pyongyang of computer science excellency.[25] Although the Massachusetts Institute of Technology did earn a gold medal in the 2019 ICPC, the United States has not held first place since 1997. Since then, Russia and China (to a lesser extent) have continued to dominate the competition. As of 2022, North Korea holds the ranking of 33rd highest performing country out of the top 100 countries, with Kim Chaek University holding 42nd place out of the top 100 universities.[26]

Moscow and Beijing have also provided industrial support to North Korea. Over the years, telecommunication companies from various countries such as China, Russia, Thailand, and Egypt have provided internet connection lines and service providers to North Korea.[27] For example, in 2017 the Russian telecommunications company TransTeleCom and China's Unicom handled roughly 60 and 40 percent of North Korea's internet traffic, respectively.[28] As a result, telecommunication assistance from foreign countries has likely expanded North Korea's offensive cyber capabilities, which it continues to leverage within its illicit cyber operations targeting the United States and South Korea.

Most recently, North Korea has joined Russia and Syria in officially recognizing the "independence" of two Russian-occupied regions of eastern Ukraine, pledging to develop "state-to-state relations with those countries."[29] Pyongyang's decision allegedly involved discussions on illegally dispatching North Korean laborers to rebuild the region in exchange for wheat, coal, and industrial equipment from Russia.[30] This development further highlights the strong partnership between Pyongyang and Moscow to evade global sanctions and the rule of law.[31]

Historically, state-sponsored hackers from China and Russia have also targeted U.S. and South Korean infrastructure. For example, the U.S. government attributed the devastating 2019–20 SolarWinds hack and the 2021 Microsoft hack to Moscow and Beijing respectively, while Russia and China targeted South Korea in 2017 and 2018 for its decision to penalize Russian athletes for doping, as well as for the deployment of Terminal High Altitude Area Defense, a U.S. anti-ballistic missile defense system, on South Korean soil.[32] Washington assisted Seoul in tracking and responding to these state-sponsored cyberattacks, indicating that while the current joint U.S.-ROK cyber working group will initially focus on North Korean cyber threats against the financial sector, there is ample room and government interest to expand future collaboration on state-sponsored cyber threats from other countries.[33]

Major Cyber-Enabled Financial Crime Attributed to North Korea[34] 2015–Present

November 2015

FAILED HACK AGAINST FILIPINO BANK

Hackers gained unauthorized access to the Philippine Bank's computer network, but they failed in sending fraudulent wire transfers before authorities detected and mitigated their infiltration.

December 2015

HACK AGAINST VIETNAMESE BANK

North Korea compromised the computer network of the Vietnamese Bank and conducted fraudulent wire transfers totaling about $2.4 million to bank accounts in Slovenia and Bulgaria.

February 2016

BANGLADESH BANK HEIST

North Korean operatives infiltrated the Bangladesh Central Bank's computer system by posing as bank officials and stole approximately $81 million from its account at the Federal Reserve Bank of New York. This was the largest known online bank heist in history.

June–July 2017

BITHUMB HACK

South Korea's NIS attributed to North Korea two consecutive hacks of a South Korean cryptocurrency exchange, Bithumb. A total of $31.6 million in cryptocurrency was stolen.

April 2018

GATE.IO HACK

North Korea employed an elaborate spear phishing and malware campaign to gain unauthorized access to a Cayman Islands–based cryptocurrency firm, Gate.io, and steal nearly $230 million in cryptocurrency. Previously, Gate.io was stationed in China but moved offshore after Beijing began to crack down on cryptocurrency mining and trading.

August–September 2018

FBI WARRANT & DEPARTMENT OF JUSTICE INDICTMENT

The FBI released a warrant for North Korean national Park Jin Hyok for his involvement in the 2014 Sony Pictures Entertainment hack and the 2016 Bangladesh Central Bank cyber heist. The U.S. Department of Justice indicted Park in September.

August 2020

PYONGYANG INFILTRATES U.S. FINANCIAL INSTITUTIONS

North Korean hackers used malicious applications disguised as trading software to infiltrate a New York financial institution where they transferred about $11.8 million in cryptocurrency from the company's digital wallets.

September 2020

KUCOIN HACK

North Korea gained unauthorized access to a Singapore-based cryptocurrency exchange, KuCoin, and stole more than $280 million in cryptocurrency. The hackers exploited financial technology, including decentralized finance platforms such as cryptocurrency mixers, to help launder the stolen funds.

February 2021

GLOBAL CRYPTO HACKING CAMPAIGN

The U.S. government attributed to North Korea a $1.3 billion global cryptocurrency heist campaign, citing the theft of $75 million from a Slovenian cryptocurrency exchange in 2017, nearly $25 million from an Indonesian exchange in 2018, and $11.8 million from financial institutions in New York City.

June 2022

HARMONY HACK

The Blockchain analysis firm Elliptic attributed to North Korean hackers the theft of nearly $100 million in digital assets from the U.S. decentralized blockchain-based platform Harmony, and held North Korea responsible for facilitating cryptocurrency transactions across different blockchains including Ethereum, Bitcoin, and Binance Chain.

August 2022

U.S. TREASURY SANCTIONS TORNADO CASH

The Treasury sanctioned another cryptocurrency mixer, Tornado Cash, for facilitating illicit North Korean cyber activity through laundering more than $7 billion in virtual currency and $20.5 million in stolen cryptocurrency since its creation in 2019.

March 2017

SOUTH KOREAN FINANCIAL INSTITUTIONS

North Korea launched a series of cyber intrusions against South Korean financial services, including traditional banks, automated teller machines, and cryptocurrency exchanges.

May 2017

WANNACRY RANSOMWARE ATTACK

The Lazarus Group used a U.S. National Security Agency exploit to infiltrate more than 300,000 computers across 150 countries by targeting vulnerabilities in the Microsoft Windows operating systems. North Korea encrypted victims' personal information and demanded ransom payments in the Bitcoin cryptocurrency.

June 2017

U.S. TREASURY SANCTIONS KCC

The Treasury sanctioned the Korea Computer Center for evading sanctions through dispatching IT workers abroad to China, Syria, Egypt, India, Germany, and the United Arab Emirates to earn currency for Pyongyang.

March 2019

DRAGONEX HACK

North Korea employed an elaborate spear phishing and malware campaign to gain unauthorized access to a Singapore-based cryptocurrency firm, DragonEx, and steal $7 million in cryptocurrency.

November 2019

UPBIT HACK

North Korean hackers stole about $50 million in Ethereum cryptocurrency through the South Korean cryptocurrency exchange UpBit.

March 2020

U.S. INDICTS & SANCTIONS TWO CHINESE NATIONALS

The U.S. government indicted and sanctioned two Chinese nationals, Tian Yinyin and Li Jiadong, for laundering more than $100 million in stolen cryptocurrency on behalf of North Korea.

December 2021

MASSIVE CRYPTO GAINS

The blockchain analysis firm Chainalysis confirmed that North Korean hackers stole nearly $400 million in digital assets from seven cryptocurrency platforms in 2021 alone.

March 2022

PLAY-TO-EARN (P2E) CRYPTO GAMES

North Korea used a spear phishing and social engineering hacking technique to gain access to Axie Infinity, a popular P2E crypto game, from which it stole roughly $600 million in digital assets.

May 2022

U.S. TREASURY SANCTIONS BLENDER.IO

The Treasury sanctioned a cryptocurrency mixer, Blender.io, for facilitating illicit North Korean cyber activity through laundering more than $20.5 million in stolen virtual currency related to the Axie Infinity hack.

KEY

- Failed Hacking Attempt
- Bank Hacks
- Cryptocurrency Hacks
- Mix of Bank and Cryptocurrency Exchange Hacks
- U.S. Government Response

Policy Recommendations

The following recommendations provide Washington and Seoul with actionable policies to incorporate in their joint cyber working group to ensure a successful strategy against the diverse security issues presented by state-sponsored cyber-enabled financial crime—specifically by North Korea.

Washington and Seoul should:

Establish a research agenda for the U.S.-ROK cyber working group to identify exploitable vulnerabilities in state-sponsored cybercrime strategy, with an initial focus on North Korea.

Identifying specific topics and goals for enhanced joint research is the first step to shift the working group from a primary planning phase to an actual enforcement and action phase. After setting the agenda and objectives, Washington and Seoul can delegate certain government agencies, and their representatives within the working group, to collaborate on tasks specific to their joint expertise and capabilities. This can also provide opportunities for both governments to ascertain any need for additional budget allocation or other potential logistical costs related to the working group and the enactment of its future policies.

The most relevant research fields to include within the working group involve continued investigations into cyber-enabled sanction evasion tactics and the location of illicit cyber operatives abroad, as well as specific hacking signatures and TTPs that can help attribute illicit cyber activity to certain countries. This should include a joint investigation to locate overseas cyber agents, malware development and deployment, and the misuse of evolving financial technology to exploit, steal, and launder digital assets.[35] For years, Pyongyang has successfully incorporated such activities into its cybercrime and sanctions evasions operations, and this calls for enhanced U.S.-ROK research to craft a more effective joint deterrence against these crimes. Additionally, the joint cyber working group will benefit from research that maps major milestones in the evolution of North Korea's cyber program, because this will better highlight vulnerabilities and facilitators related to North Korean cybercrime.[36]

Identify specific representatives from relevant U.S. and ROK government agencies to participate in the joint cyber working group. This will improve real-time information sharing and joint investigations.

Washington and Seoul should choose representatives from relevant government agencies to participate in the joint cyber working group. These representatives should bring unique expertise and in-depth subject matter knowledge on state-sponsored cyber-enabled financial crime efforts. Washington should include cybersecurity and cyber policy experts from the intelligence community, such as the FBI, National Security Agency (NSA), and CIA; as well as the National Cryptocurrency Enforcement Team (NCET) of the Department of Justice, the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security, the Bureau of Cyberspace and Digital Policy of the Department of State, and the Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury. Seoul should consider cyber units within the NIS, the KNPA, the Korea Internet & Security Agency (KISA), and KoFIU.

Every government agency listed here possesses an office and/or subunit with expertise dealing with cryptocurrency, cybersecurity, or financial crime; all three fields of research are relevant to enhancing joining U.S.-ROK strategy against cyber-enabled financial crime. A more detailed explanation of the impactful contributions each agency can make is included in the appendix section of this report.

Consider the joint cyber working group as a U.S.-ROK partnership to protect against any state-sponsored cyber-enabled financial crime operations.

The cyber working group can act as a coordinating mechanism to reduce governmental and bureaucratic processes that prevent real-time information sharing between U.S. and ROK government agencies. It can also allow South Korean agencies outside the NIS that have advanced cybersecurity, cryptocurrency, and finance-related investigatory capabilities and knowledge to actively contribute to joint security against state-sponsored cyberattacks without crossing bureaucratic boundaries established between the NIS and other South Korean agencies when dealing with North Korea. Washington and Seoul should approve their own government representatives from each

previously identified agency. In addition to real-time information sharing when relevant, the cyber working group should convene quarterly to discuss any major trends, research findings, and new strategies to combat cyber-enabled financial crime from state-sponsored actors, including but not limited to North Korea.

This partnership should include government-industry information sharing on *any* state-sponsored or major advanced persistent threat (APT) group that conducts cyber-enabled financial crime. Although North Korean hackers are the primary state-sponsored APT targeting the financial services sector, expanding the research scope to *any* state-sponsored group will reduce stigmatization of the cyber working group because of potential perceptions that it serves primarily an anti–North Korea purpose—under a future left-leaning presidential administration, this will not be a popular approach.

Issue a joint advisory guidance document on potential cybersecurity and financial risks related to social engineering hacks. This will build trust and rapport with the private sector while attempting to stymie cyber-enabled financial crime tactics.

Washington and Seoul can take immediate action to issue an official, joint guidance document through the cyber working group addressing the potential cybersecurity and financial risks related to growing social engineering hacks. Over the years, North Korea has improved its false online presence through creating seemingly legitimate websites, job postings, and social media profiles on Facebook, Twitter, YouTube, and LinkedIn, to entice both researchers on North Korea and ordinary citizens seeking employment into clicking on links and documents infected with malware. Like previous joint U.S. government documents on cyber threats, this advisory document should include past examples and screenshot images of North Korean social engineering campaigns, email correspondences, and fake job postings that led to the 2022 Axie Infinity hack of hundreds of millions of dollars' worth of cryptocurrency.[37] For cash-driven Pyongyang, the private sector dealing with financial technology is a major target for continued cyber operations. The joint U.S.-ROK cyber working group has a unique opportunity to partner with private sector entities and individuals before they become victims.

Organize an external advisory team of leading U.S. and ROK nongovernment researchers and private sector actors who work specifically on issues pertaining to the agenda of the joint working group and can offer outside assistance and advice.

The joint cyber working group should also promote enhanced information sharing through government, industrial, and educational partnerships by organizing an outside advisory team of leading non-government-affiliated U.S. and ROK researchers who work on cybersecurity and cryptocurrency-related issues. They can offer advice and additional bandwidth to the official working group. In the future, this partnership can expand government-industry information sharing to encompass research on any state-sponsored or major APT group—including from China, Russia, and Eastern Europe—that creates, distributes, or sells malware.

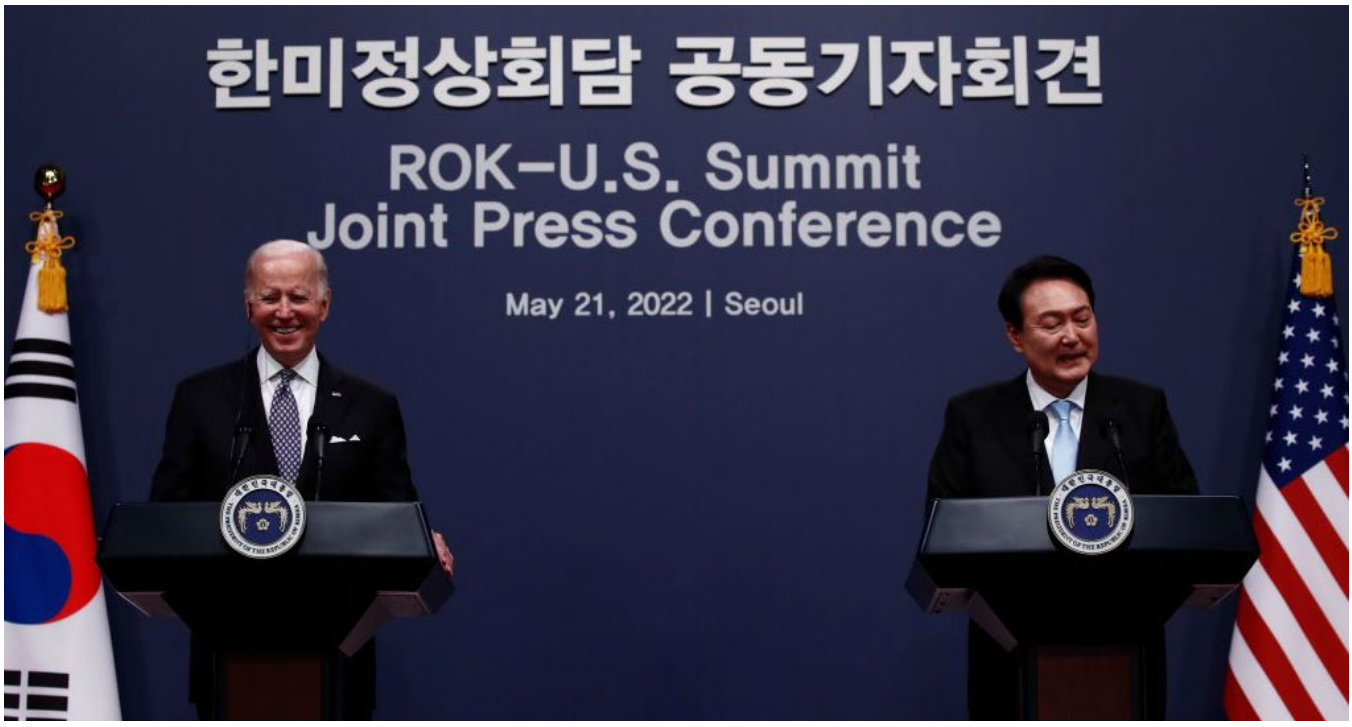
Independent and nongovernment-affiliated analysts investigating similar cybercrime-related activity are free, without heavy political consequences, to openly publish research that attributes to state-sponsored actors and third-party facilitators any breaches, TTPs, and use of certain financial technologies. This enhanced "freedom to attribute" allows nongovernmental analysts to more openly share information with one another, because they are not viewed as government officials needing approval or clearances to share certain information. Numerous U.S. and South Korean reports from think tanks and the private sector highlight the evolution of state-sponsored cybercrime, including from North Korea; this research can provide adequate stepping-stones for a joint U.S.-ROK government effort to fill in knowledge gaps using classified information that is otherwise not publicly available. To protect the classified nature of information gathered and shared within the cyber working group, the auxiliary advisory team should provide to the group only delegated research assistance and feedback; it should not be involved in classified briefings not deemed necessary for independent research. The auxiliary advisory team can offer real-time advice and feedback, while also meeting with the official U.S.-ROK joint cyber working group biquarterly.

Conclusion

Pyongyang is acutely aware of growing financial trends abroad and how best to exploit them to its benefit.[38] The global adoption of evolving financial technology has likely accelerated North Korea's efforts to expand its offensive cyber program to include more operations targeting cryptocurrency, blockchain technology, and other vulnerable financial tools and platforms. While North Korea has suffered massive fiscal loses totaling hundreds of millions of dollars from the ongoing "crypto winter" slump as of November 2021 to July 2022, Pyongyang will likely continue to incorporate cryptocurrency-related hacks into its sanctions evasions, money laundering, and illicit cyber operations because the potential gains still outweigh the logistical costs.[39] The joint U.S.-ROK cyber working group can potentially stymie the rapid growth of state-sponsored cyber-enabled financial crime from dangerous actors such as North Korea, while increasing the logistical costs for countries to continue funding this kind of illicit cyber activity.

Historically, state-sponsored hackers from China and Russia have also targeted U.S. and South Korean infrastructure. For example, the U.S. government attributed the devastating 2019–20 SolarWinds hack and the 2021 Microsoft hack to Moscow and Beijing respectively, while Russia and China targeted South Korea in 2017 and 2018 for its decision to penalize Russian athletes for doping and for the deployment of THAAD, a U.S. anti-ballistic missile defense system, on South Korean soil.[40] Washington assisted Seoul in tracking and responding to these state-sponsored cyberattacks, indicating that the current joint U.S.-ROK cyber working group will initially focus on North Korean cyber threats against the financial sector, but there is ample room and government interest to expand future collaboration on state-sponsored cyber threats from other countries.

Both the United States and South Korea are well-equipped to tackle this grave national security threat that weakens vital social, financial, and cyber infrastructure, but a joint deterrent will prove effective only if Washington and Seoul can establish a long-lasting cybersecurity strategy that addresses cyber-enabled financial crime. Removing logistical and bureaucratic boundaries that prevent enhanced coordination and information sharing is the first step in finding ways to leverage the different expertise and capabilities that Washington and Seoul can bring to bear against the vulnerabilities of Pyongyang. A successful joint U.S.-ROK strategy to combat and deter cyber-enabled financial crime can help advance international norms on bilateral and multilateral cybersecurity frameworks, as well as global regulations on virtual financial security, sanctions evasions tactics, money laundering, state-sponsored cyberattacks, and other illicit cyber activity.



On May 21, 2022, U.S. President Joe Biden and South Korean President Yoon Suk-yeol met in Seoul to discuss a range of national security issues, including North Korea and cybercrime. (Jeon Heon-Kyun/Pool/Getty Images)

Appendix: Understanding the Major U.S. and ROK Government Players to Combat and Deter State-Sponsored Cyber-Enabled Financial Crime

This appendix provides Washington and Seoul with a brief description of relevant government entities that can offer expertise to the joint U.S.-ROK cyber working group. While there are no exact counterparts for each entity, both countries possess a wide range of government agencies that can provide valuable assistance in tracking, preventing, and combating cyber-enabled financial crime committed by state-sponsored actors.

U.S. GOVERNMENT AGENCIES

The Intelligence Community (IC)

U.S. intelligence agencies such as the FBI, CIA, Defense Intelligence Agency, and NSA play an important role in gathering and analyzing information about North Korea's domestic and foreign operations, including illicit cyber activity. Incorporating representatives from relevant cyber units within the IC will be crucial to the success of any joint cyber working group with Seoul, as the IC can obtain and distribute classified information at a higher level than most other U.S. government agencies. The IC has been crucial in identifying North Korean hackers and pending cyberattacks, as well as attributing certain malware and intrusions to North Korean actors.[41]

The Department of Justice (DOJ)

The DOJ can issue federal-level indictments against illicit state-sponsored cyber actors and their facilitators to curb the growth of North Korean cybercrime. While successful extraditions to the United States of North Korean criminals are certainly not common, the DOJ has been helpful in leveraging charges against both domestic and foreign actors, including from the United States, Canada, and China, who have aided illicit North Korean cyber operations.[42] The DOJ has also been instrumental in publicizing certain cryptocurrency wallets, mixers, and other blockchain technology that North Korean actors and their facilitators use to support illicit cyber operations, such as laundering stolen funds related to ransomware attacks and cryptocurrency hacks. When DOJ indictments are paired with economic sanctions and travel bans levied by the Departments of the Treasury and State, the United States has a powerful coercive edge that can freeze and seize the financial assets of targeted individuals and entities to economically isolate them from the global financial market through restricting their access to the U.S. dollar.

In particular, the U.S. National Cryptocurrency Enforcement Team can assume a lead role in organizing U.S. cyber strategy aimed at cryptocurrency-motivated North Korean cybercrime.[43] A recent DOJ document explaining the role of the NCET mentioned its proposed collaboration with the DOJ Criminal Division's Computer Crime and Intellectual Property Section and Money Laundering and Asset Recovery Section, as well as the FBI's new Virtual Asset Exploitation Unit, which could be expanded to include the Departments of the Treasury and State.

The Department of the Treasury

The U.S. Treasury wields unmatched economic coercive power due to the international adoption of the U.S. dollar as the world's reserve currency, making U.S. sanctions some of the most powerful economic tools in the world. South Korea does not enjoy the same coercive economic power, nor can it levy impactful unilateral sanctions against North Korea to the same degree as the United States. Since the start of the Korean War in 1950, the U.S. government has incorporated economic sanctions and other sanctioning tools into its foreign policy toward North Korea.[44] After the North Korea–led cyberattack against Sony Pictures Entertainment in 2014, the White House expanded the Treasury's sanctioning authority to include targets responsible for cybercrime with a specific sanctions program for North Korean cybercrime in 2016.[45] In recent years, the OFAC within the Treasury has taken significant steps toward curbing the growth of North Korean cybercrime through designating roughly 130 individuals and entities pursuant to cyber-specific sanctions programs, including two Chinese nationals who laundered more than $100 million in cryptocurrency on behalf of North Korea, and two cryptocurrency mixers that North Korean hackers have used to launder billions of dollars' worth of stolen virtual currency.[46]

In addition to expanding designations on North Korea–related targets engaging in illicit cyber activity, OFAC has also issued advisory documents on potential sanctions risks for facilitating ransomware payments, as well as guidance for victims of ransomware to follow.[47] A unit within the Treasury known as the Financial Crimes Enforcement Network also plays a major role in responding to North Korea–sponsored cybercrime through issuing official public guidance on sanctions evasions tactics, including money laundering efforts and red flag indicators of illicit North Korea activity.[48] Because sanctions on North Korean targets alone will not likely coerce Pyongyang into ceasing illicit cyber activity, the Treasury must continue to work with fellow U.S. government agencies and allied countries to identify and designate foreign actors that provide North Korea with the expertise and ability to skirt current sanctions regimes.

The Department of State

In addition to the Treasury, the Department of State possesses numerous authorities to support U.S. cybersecurity strategy. From issuing travel bans on U.S. and non-U.S. nationals supporting North Korean cyber operations to offering guidance to the international community and the private sector regarding Pyongyang's attempts to dispatch hackers overseas under the guise of foreign IT workers, the Department of State plays a major role in disseminating information to the general public.[49] The State Department can work with representatives at U.S. embassies located in high-risk jurisdictions, such as Southeast Asia, to help inform foreign leaders and their populations of the real risks behind wittingly, and unwittingly, employing North Korean IT workers. These risks include susceptibility to financially costly hacks and possible sanctions violations. The recently established Bureau of Cyberspace and Digital Policy, under the State Department, can incorporate specialized research on state-sponsored cybercrime within its portfolio, as North Korean cyber operatives pose a significant risk to cyberspace, digital technologies, and global cyber policy.[50]

Cybersecurity and Infrastructure Security Agency (CISA)

Under the auspices of the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency leads the U.S. national effort to "understand, manage, and reduce risk to our [U.S.] cyber and physical infrastructure."[51] In addition to providing overall cybersecurity support to the federal government, CISA works closely with other government agencies to construct a whole-of-government response to the North Korean cyber threat. In 2021, CISA partnered with the FBI and the Treasury to issue a joint cybersecurity advisory highlighting North Korean tactics related to cryptocurrency thefts.[52] It specifically mentioned North Korean cyber actors targeting the blockchain technology and cryptocurrency industry, decentralized finance protocols, P2E cryptocurrency video games, and individuals holding large amounts of cryptocurrency or other valuable digital assets, such as non-fungible tokens. Most recently, in July 2022, CISA released a joint Cybersecurity Advisory with the FBI and the Treasury to provide information on North Korean state-sponsored cyber actors using Maui ransomware to target the healthcare and public health sector. This indicates a North Korean trend to use ransomware against healthcare services, as seen during the 2017 WannaCry ransomware attacks.[53] Because CISA is instrumental in crafting, with other U.S. agencies, cybersecurity strategy and outreach, its engagement within a joint U.S.-ROK cyber working group is crucial.

SOUTH KOREAN GOVERNMENT AGENCIES

The National Intelligence Service (NIS – 국가정보원)

The NIS is the primary agency that collects and analyzes all information pertaining to security threats from North Korea, ranging from espionage and terrorism to cyberattacks.[54] The NIS also has the unique role of disseminating North Korea–related information to all other government agencies at its discretion, while other security agencies are expected to inform the NIS of any possible nexus to North Korea when detecting a threat. As such, the NIS has a large influence on Seoul's domestic and foreign politics. The NIS significantly contributes to South Korea's clandestine response to North Korean cybercrime, as well as its cybersecurity posture against all other state-sponsored cyberattacks. While the NIS does collect information on other foreign cyber threats, including China and Russia, most foreign intelligence collected is related to North Korea, because Pyongyang remains Seoul's largest existential threat. Under the NIS, the National Cyber Security Center (NCSC) provides five major roles related to South Korea's cybersecurity strategy: policy establishment and consulting, threat detection and response, incident investigation and damage control, information sharing and cooperation, and education and training for national and public organizations. The NCSC also publishes public reports to raise awareness of major cyber threats, and of its important role in ensuring national cyber defense for South Korea.[55] Under President Yoon, the NIS recently decided to join the 2022 NATO Cooperative Cyber Defense Centre of Excellence and the U.S.-led multilateral Cyber Flag cybersecurity exercise.[56] While the decision will likely draw criticism from Pyongyang, Beijing, and Moscow, these are necessary steps to cement Seoul's role in contributing to international cyber policy norms and multilateral capacity building.[57]

Korean National Policy Agency (KNPA – 경찰청)

The KNPA is the leading policy force in South Korea, tasked with enforcing national law through its 18 local police agencies. Similar to the FBI, the KNPA is also equipped with a cyberunit that collaborates closely with its internal Criminal Investigation Bureau and foreign police forces. According to media reports from 2015, the FBI and KNPA established a "practical cooperation system" that built on a previous memorandum of understanding (MOU) between the two agencies in prior years.[58] The KNPA has collaborated with numerous foreign and multilateral law enforcement agencies, including Interpol, to tackle a variety of cyber-enabled financial crime cases. Along with special cybercrime agents and officers within the U.S. Department of Justice and the Internal Revenue Service, the KNPA was instrumental in shutting down the world's largest known child pornography website, "Welcome to Video," in 2018, as well as working with U.S. and Ukrainian cyber police units in 2021 to arrest a group of cybercriminals in Ukraine responsible for the Clop ransomware that caused an estimated $500 million worth of damage to hundreds of victims, including the oil and gas company Shell, several U.S. universities, and South Korean e-commerce platforms.[59] In light of the ongoing Russian invasion of Ukraine, Kyiv has reportedly asked Seoul for cybersecurity assistance, which suggests a continued level of trust in South Korea's cyber capabilities.[60] However, there are key differences between the KNPA and the FBI that should be understood.

The FBI functions under the Department of Justice and typically enjoys greater levels of logistical and investigative autonomy than does the KNPA. Despite operating under the ROK Ministry of the Interior and Safety (행정안전부), all police-led investigative bureaus must report to the Commissioner General of the KNPA, and this can restrict logistical and investigative autonomy. Following a 2017 proposal from the KNPA to establish an investigate bureau independent from the national police force, in 2021 Seoul restructured the KNPA to include a new National Office of Investigation modeling the FBI.[61] However, the expertise of the KNPA has widely been unused when combating North Korean illicit activity, including cyber-enabled financial crime. To avoid igniting intergovernmental tensions, Seoul should include in the joint U.S.-ROK cyber working group equal representation from relevant cyber units within the NIS and KNPA.

Ministry of Science and Information and Communication Technologies (과학기술정보통신부)

Two sub-organizations support the ROK Ministry of Science and ICT through providing valuable cybersecurity expertise to the South Korean government: the Financial Services Institute (FSI - 금융보안원) and the Korea Internet & Security Agency (KISA - 한국인터넷진흥원). The FSI offers research and development expertise on cyber incident response, information sharing, vulnerability analysis and assessment, and general cybersecurity reviews for the South Korean government, as well as for private sector entities that engage in digital trade and evolving financial technology.[62] Complementary to FSI, KISA detects and analyzes malware and other computer viruses, ensures privacy protection of internet users, operates root certificate authority to verify the proper identity of a software or website owner, and

provides other crucial daily cybersecurity tasks. Unlike CISA, it does not issue official public guidance specifically on North Korean cyber threats, nor does it have a unit focused primarily on North Korea. However, KISA has indirectly contributed to both South Korean and global efforts tracking and identifying North Korean cybercrime. In 2013, KISA collaborated with other ROK agencies to help attribute a cyberattack in March to the previous "DarkSeoul" cyberattacks against South Korea through an IP address in North Korea. This cyber aggression proved that Pyongyang was now capable of launching cyberattacks from within its own jurisdiction, likely thanks to internet connection cables provided by China and other foreign countries in years prior.[63]

KISA continues to contribute to Seoul's cybersecurity strategy, as it has introduced new regulations in 2021 to advanced anti–money laundering (AML) requirements on virtual assets. Under these rules, all virtual asset service providers (VASPs), entities that facilitate the exchange, transfer, custody, offer, or sale of virtual assets such as cryptocurrency, are required to receive Information Security Management System certifications from KISA in order to legally operate within the South Korean market.[64] The expertise of KISA should be considered when conducting joint research on the distribution of malware and the use of certain technologies, such as VASPs and virtual private networks, to hide a true origin and identity behind a cyber intrusion. A more detailed account of the roles of the FSI, KISA, and the NCSC within South Korea's cybersecurity policy can be found in a report published by the Carnegie Endowment for International Peace: "The Korean Way with Data: How the World's Most Wired Country Is Forging a Third Way."[65]

Korea Financial Intelligence Unit (KoFIU - 금융정보분석원)

Similar to the U.S. FinCEN, the Korea Financial Intelligence Unit is the primary executive agency responsible for implementing effective AML and CFT (combating the finance of terrorism) protocols in South Korea. As such, KoFIU has contributed to Seoul's national cybersecurity capabilities, including those relevant to combatting North Korean cybercrime. In coordination with KISA, KoFIU has advanced government efforts to improve know-your-customer protocol for cryptocurrency transactions that allow for easier tracking of illicit cyber-enabled financial crimes.[66] As of late March 2021, KoFIU required all VASPs seeking to operate in South Korea to partner with a South Korean bank to create "real name" verified bank accounts for customers, instead of using anonymous cryptocurrency wallets.[67] Since North Korean cyber operatives continue to target cryptocurrency exchanges and associated technology, this requirement will likely raise the difficulty threshold for North Korean actors to exploit VASPs operating in South Korea.

KoFIU has also pursued bilateral and multilateral cooperation amid global AML and CFT efforts. As of July 2022, KoFIU has signed bilateral MOUs pertaining to the exchange of financial transaction information with 70 foreign countries, including the United States, and is a member of three major international organizations addressing global financial crime and evolving financial technologies: the Financial Action Task Force, the Asia/Pacific Group on Money Laundering, and the Egmont Group.[68] Washington and Seoul should leverage the preexisting information sharing mechanisms between FinCEN and KoFIU within the joint U.S.-ROK cyber working group to maximize visibility on suspicious and illicit financial activity possibly linked to state-sponsored actors such as North Korea. The United States has already signaled interest in enhancing coordination with KoFIU, as Under Secretary for Terrorism and Financial Intelligence of the Treasury Department Brian Nelson recently traveled to South Korea to discuss digital assets, cybersecurity, AML, and sanctions on North Korea.[69]

OTHER U.S. AND ROK AGENCIES

Additional U.S. and ROK government agencies possess varying levels of influence and capabilities related to national cybersecurity policy and enforcement. For the United States, these include cyber units within the National Security Council, White House, and Department of Defense, such as the U.S. Cyber Command; for South Korea, there are equivalent cyber-focused sub-divisions within the ROK Blue House and military. Given the current direction of the working group toward countering cyber-enabled financial crime, Washington and Seoul will likely lean more on the expertise of the U.S. and ROK agencies specifically mentioned in previous sections of this report. However, the United States and South Korea should consider the expertise of all relevant government agencies when deciding which entities to include within the joint cyber working group.

1. "United States–Republic of Korea Leaders' Joint Statement," The White House, press release, May 21, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/21/united-states-republic-of-korea-leaders-joint-statement/; "U.S.-ROK Leaders' Joint Statement," The White House, press release, May 21, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/21/u-s-rok-leaders-joint-statement/.

2. Jason Bartlett, "Why North Korea Is the Greatest State-Sponsored Threat to the Financial Services Sector," Korea on Point by the Sejong Institute, June 27, 2022, https://koreaonpoint.org/view.php?topic_idx=30&idx=95; Olga Kharif, Sidhartha Shukla, and Bloomberg, "Hackers Just Stole $100 Million in Crypto from Harmony's Horizon Bridge," Fortune, June 24, 2022, https://fortune.com/2022/06/24/hackers-steal-100-million-in-crypto-from-harmony-horizon-bridge-ethereum-binance/.

3. Christy Lee, "Biden, Yoon Embrace Policy of North Korea Denuclearization Backed by Deterrence, Not Concessions," VOA News, May 25, 2022, https://www.voanews.com/a/biden-yoon-embrace-policy-of-north-korea-denuclearization-backed-by-deterrence-not-concessions/6588368.html.

4. Justin McCurry, "South Korea President Suggests Joint Drills with U.S. Could Be Suspended," The Guardian, December 19, 2017, https://www.theguardian.com/world/2017/dec/20/south-korea-president-suggests-joint-drills-with-us-could-be-suspended; Byun Duk-kun, "Reducing Military Exercises for Dialogue with N. Korea a Proven Path to Failure: Harris," Yonhap News, April 22, 2022, https://en.yna.co.kr/view/AEN20220422000200325.

5. Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives, 113th Cong., 1st sess., Serial No. 113-9, March 20, 2013, https://www.govinfo.gov/content/pkg/CHRG-113hhrg82583/html/CHRG-113hhrg82583.htm.

6. Joseph Marks and Aaron Schaffer, "Is Russia or China the Biggest Cyber Threat? Experts Are Split," The Washington Post, January 20, 2022, https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/; Jim Garamone, "U.S. Intel Officials Detail Threats from China, Russia," U.S. Department of Defense, March 8, 2022, https://www.defense.gov/News/News-Stories/Article/Article/2960113/us-intel-officials-detail-threats-from-china-russia/; Stacie Pettyjohn and Jennie Matuschak, "Long Shadows: Deterrence in a Multipolar Nuclear Age" (CNAS, May 19, 2022), https://www.cnas.org/publications/reports/long-shadows-deterrence-in-a-multipolar-nuclear-age; Andrea Kendall-Taylor and David Shullman, "Navigating the Deepening Russia-China Partnership" (CNAS, January 14, 2021), https://www.cnas.org/publications/reports/navigating-the-deepening-russia-china-partnership.

7. "Cybersecurity Threats and Information Sharing," virtual event, CNAS, July 28, 2022, https://www.cnas.org/events/virtual-event-cybersecurity-threats-and-information-sharing-with-anne-neuberger; Ethan Jewel, "Cyberattacks Furnish Third of Funds for North Korean Missiles: U.S. Official," NK News, July 29, 2022, https://www.nknews.org/pro/cyberattacks-furnish-third-of-funds-for-north-korean-missiles-us-official/.

8. "北, 한국 공공분야 일평균 150만건 사이버 공격" (North Korea, Daily Average of 1.5 Million Cyberattacks on South Korea's Public Sector), 연합뉴스), Yonhap News, February 1, 2021, https://www.yna.co.kr/view/AKR20210201066400073.

9. North Korea, Daily Average of 1.5 Million Cyberattacks.

10. U.S. Department of the Treasury, Office of Foreign Assets Control, "Sanctions Search List," https://sanctionssearch.ofac.treas.gov/.

11. Jason Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program," The Diplomat, July 18, 2022, https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/.

12. DarunGrim, "North Korea Hacking Timeline," https://darungrim.com/intelligence/NK/Timeline.html#event-operation-flame.

13. Jason Bartlett and Francis Shin, "Sanctions by the Numbers: Spotlight on North Korea" (CNAS, February 8, 2021), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-north-korea; Kajol Aikat, "A Brief History of Bitcoin," TechGig, July 27, 2021, https://content.techgig.com/infographics/a-brief-history-of-bitcoin/articleshow/84791825.cms; Jason Bartlett, "Exposing the Financial Footprints of North Korea's Hackers" (CNAS, November 18, 2020), https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers.

14. Edward Kost, "The 6 Biggest Cyber Threats for Financial Services in 2022," UpGuard, June 26, 2022, https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services; "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks" Alert No. AA20-239A (Cybersecurity and Infrastructure Security Agency, August 26, 2020), https://www.cisa.gov/uscert/ncas/alerts/aa20-239a; Christopher Bing and Sarah N. Lynch, "U.S. Charges North Korean Hacker in Sony, WannaCry Cyberattacks," Reuters, September 6, 2018, https://www.reuters.com/article/us-cyber-northkorea-sony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacks-idUSKCN1LM20W; Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions," https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline; Global Research & Analysis Team, Kaspersky Lab, "APT Trends Report Q3 2021" (SecureList by Kaspersky, October 26, 2021), https://securelist.com/apt-trends-report-q3-2021/104708/.

15. Kong Ji Young, Lim Jong In, and Kim Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies" (paper presented at NATO 11th International Conference on Cyber Conflict: Silent Battle, 2019, https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf; Jeong Tae Joo, "Around 100 Top Technology University Graduates Join Military," Daily NK, May 18, 2020 (translated by Jason Bartlett), https://www.dailynk.com/english/around-100-top-technology-university-graduates-join-military/.

16. Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program."

17. Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program."

18. Jason Arterburn, "Dispatched: Mapping Overseas Forced Labor in North Korea's Proliferation Finance System" (C4ADS, 2018), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5bfc1b8ab8a045b4c0408779/1543248819621/Dispatched.pdf.

19. Will Ripley, "North Korean Defector: 'Bureau 121' Hackers Operating in China," CNN World, January 7, 2015, https://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html.

20. "United States v. Park Jin Hyok," U.S. Department of Justice, Criminal Complaint, June 8, 2018, https://www.justice.gov/opa/press-release/file/1092091/download.

21. "North Korean Regime–Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," U.S. Department of Justice Office of Public Affairs, press release No. 18-1452, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

22. U.S. Departments of the Treasury, State, and Justice, Guidance on the Democratic People's Republic of Korea Information Technology Workers (May 16, 2022), https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_advisory.pdf; Min Chao Choy, "North Korean IT Workers Are Illegally Making Big Money Abroad: Investigation," NK News, August 18, 2020, https://www.nknews.org/2020/08/north-korean-it-workers-are-illegally-making-big-money-abroad-investigation/.

23. Ning Zhai, "Vice President REN Meets North Korean Students Studying at HIT," Harbin Institute of Technology News, October 8, 2013, http://en.hit.edu.cn/news/index/2302.

24. International Collegiate Programming Contest (ICPC) Results, 2019, https://icpc.global/community/results-2019.

25. "Kim Chaek University at the ICPC Programming Contest," YouTube, June 6, 2019, https://www.youtube.com/watch?v=ys7PWS7yigI.

26. ICPC Rank List, North Korea, https://icpc.kattis.com/countries/PRK; ICPC University Profiles, Kim Chaek University of Technology, https://icpc.kattis.com/universities/kut.edu.kp.

27. Reporters without Borders, "Enemies of the Internet 2014—North Korea: The Web As a Pawn in the Power Game," Refworld, March 12, 2014, https://www.refworld.org/docid/533925b6b.html.

28. "Russian Firm Provides New Internet Connection to North Korea," Reuters, October 2, 2017, https://www.reuters.com/article/us-nkorea-internet/russian-firm-provides-new-internet-connection-to-north-korea-idUSKCN1C70D2.

29. "DPRK Officially Recognizes Donetsk and Lugansk," Korean Central News Agency, July 14, 2022, https://kcna.watch/newstream/1657751789-824945617/dprk-officially-recognizes-donetsk-and-lugansk/.

30. 조진우 (Cho Jinwoo), "도네츠크 '북한과 돈바스 재건 사업 추진' …전문가 "대북제재 회피 거점 될 것" (Donetsk "Promoting North Korea and Donbas Reconstruction Project"... Experts Say, "It Will Be a Base to Avoid Sanctions against North Korea"), Radio Free Asia, July 26, 2022, https://www.rfa.org/korean/in_focus/nk_nuclear_talks-07262022155748.html; "North Korean Builders to Help with Donbas Reconstruction," Russian Ambassador, The Moscow Times, July 19, 2022, https://www.themoscowtimes.com/2022/07/19/north-korean-builders-to-help-with-donbas-reconstruction-russian-ambassador-a78344.

31. Jason Bartlett, "Sanctions, Cyber, and Crypto: How Pyongyang Can Exploit the War in Ukraine," The Diplomat, July 27, 2022, https://thediplomat.com/2022/07/sanctions-cyber-and-crypto-how-pyongyang-can-exploit-the-war-in-ukraine/.

32. Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," National Public Radio, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack; Dina Temple-Raston, "China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying," National Public Radio, August 26, 2021, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying; Sunha Bae et al., "Cyberattack Severity Assessment (CASA) and National Response Matrix (NRM) in Korea," Journal of East Asian Affairs, 31 no. 2 (December 30, 2021), 67–98.

33. Emily Kilcrease, Jason Bartlett, and Mason Wong, "Sanc-

tions by the Numbers: Economic Measures against Russia Following Its 2022 Invasion of Ukraine" (CNAS, June 16, 2022), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-economic-measures-against-russia-following-its-2021-invasion-of-ukraine.

34. Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program."

35. U.S. Departments of the Treasury, State, and Justice, Guidance on the Democratic People's Republic of Korea Information Technology Workers.; Panel of Experts final report for distribution, pursuant to resolution 1874 (2009), Report No. S/2022/132 (United Nations Security Council, March 1, 2022), https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf; Sean Lyngaas, "Here's How North Korean Operatives Are Trying to Infiltrate U.S. Crypto Firms," CNN Politics, July 10, 2022, https://www.cnn.com/2022/07/10/politics/north-korean-hackers-crypto-currency-firms-infiltrate/index.html; Seongsu Park, "Andariel Evolves to Target South Korea with Ransomware" (SecureList by Kaspersky, June 15, 2021), https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/; Vyacheslav Kopeytsev and Seongsu Park, "Lazarus Targets Defense Industry with ThreatNeedle" (SecureList by Kaspersky, February 25, 2021), https://securelist.com/lazarus-threatneedle/100803/; Jason Bartlett, "Following the Crypto: Using Blockchain Analysis to Assess the Strengths and Vulnerabilities of North Korean Hackers" (CNAS, February 2022), https://www.cnas.org/publications/reports/following-the-crypto; Elliptic Research Team, "The $100 Million Horizon Hack: Following the Trail through Tornado Cash to North Korea," Elliptic Connect, June 29, 2022, https://hub.elliptic.co/analysis/the-100-million-horizon-hack-following-the-trail-through-tornado-cash-to-north-korea/; Jason Bartlett, "Why North Korea Is the Greatest State-Sponsored Threat to the Financial Services Sector," Korea on Point by the Sejong Institute, June 27, 2022, https://koreaonpoint.org/view.php?topic_idx=30&idx=95; Kharif, Shukla, and Bloomberg, "Hackers Just Stole $100 Million in Crypto from Harmony's Horizon Bridge."

36. Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program."

37. Ryan Weeks, "How a Fake Job Offer Took Down the World's Most Popular Crypto Game," The Block, July 6, 2022, https://www.theblock.co/post/156038/how-a-fake-job-offer-took-down-the-worlds-most-popular-crypto-game.

38. Bartlett, "Why North Korea Is the Greatest State-Sponsored Threat to the Financial Services Sector."

39. Martin Young, "Crypto Winter Threatens North Korea's Stolen Stash: Report," Crypto Potato, June 29, 2022, https://cryptopotato.com/crypto-winter-threatens-north-koreas-stolen-stash-report/; Josh Smith, "Crypto Crash Threatens North Korea's Stolen Funds As It Ramps Up Weapons Tests," Reuters, June 29, 2022, https://www.reuters.com/technology/crypto-crash-threatens-north-koreas-stolen-funds-it-ramps-up-weapons-tests-2022-06-28/.

40. Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack"; Temple-Raston, "China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying"; Sunha Bae et al., "Cyberattack Severity Assessment (CASA) and National Response Matrix (NRM) in Korea."

41. Jon Chang Hyok Wanted Poster, Federal Bureau of Investigation, https://www.fbi.gov/wanted/cyber/jon-chang-hyok; Park Jin Hyok Wanted Poster, Federal Bureau of Investigation, https://www.fbi.gov/wanted/cyber/park-jin-hyok; Kim Il Wanted Poster, Federal Bureau of Investigation, https://www.fbi.gov/wanted/cyber/kim-il; Ellen Nakashima, "The NSA Has Linked the WannaCry Computer Worm to North Korea," The Washington Post, June 14, 2017, https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html; James B. Comey, "Addressing the Cyber Security Threat" (International Conference on Cyber Security, Fordham University, New York, January 7, 2015), https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

42. "First North Korean National Brought to the United States to Stand Trial for Money Laundering Offenses," U.S. Department of Justice Office of Public Affairs, press release No. 21-230, March 22, 2021, https://www.justice.gov/opa/pr/first-north-korean-national-brought-united-states-stand-trial-money-laundering-offenses; "United States Citizen Pleads Guilty to Conspiring to Assist North Korea in Evading Sanctions," U.S. Department of Justice Office of Public Affairs, press release No. 21-254, September 27, 2021, https://www.justice.gov/usao-sdny/pr/united-states-citizen-pleads-guilty-conspiring-assist-north-korea-evading-sanctions; "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes across the Globe," U.S. Department of Justice Office of Public Affairs, press release No. 21-154, February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and; "Four Chinese Nationals and China-Based Company Charged with Using Front Companies to Evade U.S. Sanctions Targeting North Korea's Nuclear Weapons and Ballistic Missile Programs," U.S. Department of Justice Office of Public Affairs, press release No. 16-1097, September 26, 2016, https://www.justice.gov/opa/pr/four-chinese-nationals-and-china-based-company-charged-using-front-companies-evade-us.

43. "Justice Department Announces First Director of National Cryptocurrency Enforcement Team," U.S. Department of Justice Office of Public Affairs, press release No. 22-140, February 17, 2022, https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team.

44. Bartlett and Shin, "Sanctions by the Numbers: Spotlight on North Korea."

45. Joseph R. Biden Jr., "Notice on the Continuation of the National Emergency with Respect to North Korea," presidential action, June 13, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/06/13/notice-on-the-continuation-of-the-national-emergency-with-respect-to-north-korea-2/; Jason Bartlett and Megan Ophel, "Sanctions by the Numbers: Spotlight on Cyber Sanctions" (CNAS, May 4, 2021), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.

46. U.S. Department of the Treasury, Office of Foreign Assets Control, "Sanctions Search List"; "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," U.S. Department of the Treasury, press release, March 2, 2020, https://home.treasury.gov/news/press-releases/sm924; "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," U.S. Department of the Treasury, press release, May 6, 2022, https://home.treasury.gov/news/press-releases/jy0768; "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," U.S. Department of the Treasury, press release, August, 2022, https://home.treasury.gov/news/press-releases/jy0916.

47. U.S. Department of the Treasury, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (September 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

48. "FinCEN Further Restricts North Korea's Access to the U.S. Financial System and Warns U.S. Financial Institutions of North Korean Schemes," U.S. Department of the Treasury Financial Crimes Enforcement Network, press release, November 2, 2017, https://www.fincen.gov/news/news-releases/fincen-further-restricts-north-koreas-access-us-financial-system-and-warns-us; U.S. Department of the Treasury Financial Crimes Enforcement Network, Advisory on North Korea's Use of the International Financial System (November 2, 2017), https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf.

49. "Guidance on the Democratic People's Republic of Korea Information Technology Workers," U.S. Department of State, press release, May 16, 2022, https://www.state.gov/guidance-on-the-democratic-peoples-republic-of-korea-information-technology-workers/.

50. "Establishment of the Bureau of Cyberspace and Digital Policy," U.S. Department of State, press release, April 4, 2022, https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/.

51. "About CISA," Cybersecurity and Infrastructure Security Agency website, https://www.cisa.gov/about-cisa.

52. "TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies," Alert No. AA22-108A (Cybersecurity and Infrastructure Security Agency, April 18, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-108a.

53. "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector," Alert No. AA22-187A (Cybersecurity and Infrastructure Security Agency), July 06, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-187a; Sean Lyngaas, "North Korean Government Hackers Hit Health Services with Ransomware, U.S. Agencies Warn," CNN Politics, July 6, 2022, https://www.cnn.com/2022/07/06/politics/north-korea-ransomware-health-care/index.html.

54. "Intelligence on North Korea," National Intelligence Service website, https://eng.nis.go.kr/EAF/1_2.do.

55. "NCSC Annual Report 2021" (National Cyber Security Center, NCSC New Leap Forward, 2021), https://www.nis.go.kr/AF/1_7_7_1.do; Donghui Park, "Cybersecurity Spotlight: South Korea," East Asia Center, University of Washington, January 12, 2016, https://jsis.washington.edu/eacenter/2016/01/12/cybersecurity-spotlight-south-korea/.

56. Gabriel Honrada, "Eye on China, S. Korea Joins NATO Cyber Defense Unit," Asia Times, May 10, 2022, https://asiatimes.com/2022/05/eye-on-china-s-korea-joins-nato-cyber-defense-unit/; Ji Da-gyum, "S. Korean Military to Join U.S.-Led Major, Multinational Cyber Exercise for First Time," The Korea Herald, June 27, 2022, https://www.koreaherald.com/view.php?ud=20220627000667.

57. "싸이버범죄국의 주제넘은 망동" ([U.S.] Cyber Crime Agency's Impudent Fool), Korean Central News Agency, April 7, 2022, https://kcnawatch.org/newstream/1656907233-238023259/%ec%8b%b8%ec%9d%b4%eb%b2%84%eb%b2%94%ec%a3%84%ea%b5%ad%ec%9d%98-%ec%a3%bc%ec%a0%9c%eb%84%98%ec%9d%80-%eb%a7%9d%eb%8f%99/.

58. "경찰청-美 FBI MOU. . . 사이버범죄.정보.교육 등 실질 협력" (KNPA-U.S. FBI MOU. . . Cooperation on Cybercrime, Information Sharing, Training, etc.), June 25, 2015, https://www.fnnews.com/news/201506251640104734.

59. "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which Was Funded by Bitcoin," U.S. Department of Justice Office of Public Affairs, press release No. 19-1,104, October 16, 2019, https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child; "Кіберполіція викрила хакерське угруповання у розповсюдженні вірусу-шифрувальника та

нанесенні іноземним компаніям пів мільярда доларів збитків" "[The cyber police exposed a hacker group in the distribution of an encryption virus and causing half a billion dollars in losses to foreign companies]", Cyber Police Department of the National Police of Ukraine, Cyber Crimes and Cyber Security, June 16, 2021, https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/.

60. Hyonhee Shin, "Ukraine Asks for S. Korea Cybersecurity Aid Amid Russia Invasion," Reuters, February 25, 2022, https://www.reuters.com/world/ukraine-asks-skorea-cybersecurity-aid-amid-russia-invasion-2022-02-25/.

61. Yeon Kyu-wook, "Korean Police Suggest Creation of FBI-Like Independent Investigative Bureau," Pulse, June 28, 2017, https://pulsenews.co.kr/view.php?year=2017&no=433111; Kim Myong-sik, "Is Korean Police Ready for New Role?" The Korea Herald, January 28, 2021, http://www.koreaherald.com/view.php?ud=20210127000704.

62. 금융보안원 (Financial Security Institute), https://www.fsec.or.kr/fsec/index.do; "금융보안원 소개서" (Explainer on the Financial Security Institute), Financial Security Institute, http://www.fsec.or.kr; "FSI: Financial Security Institute," Financial Security Institute, https://www.fsec.or.kr/site/fseceng/upload/content/%5Be-Brochure%5DFSI_2019_FN.pdf; Kyung-min Lee, "[Interview] Financial CEOs Urged to Reform Mindset on Security," The Korea Times, Finance, January 5, 2020, https://www.koreatimes.co.kr/www/biz/2020/02/602_281203.html.

63. "해킹 북한IP의 등록주소는 '평양시 류경동" (Registered IP Address Linked to North Korea Hack Is in Ryugyong-dong, Pyongyang), April 11, 2013, https://www.yna.co.kr/view/AKR20130411000900017.

64. Norbert Gehrke, "Korea Regulations for Virtual Asset Service Providers," Medium, June 3, 2021, https://medium.com/tokyo-fintech/korea-regulations-for-virtual-asset-service-providers-b34c20efa58f.

65. Jang GyeHyun et al., "The Korean Way with Data: How the World's Most Wired Country Is Forging a Third Way," Evan A. Feigenbaum and Michael R. Nelson, eds. (Carnegie Endowment for International Peace, August 2021), https://carnegieendowment.org/files/202108-Korean-WayWithData_final5.pdf.

66. "AML/CFT Framework," Korea Financial Intelligence Unit website, https://www.kofiu.go.kr/eng/regime/framework.do.

67. Euihyun Bae, "South Korea Takes First Step to Regulate Virtual Asset Service Providers," The Diplomat, September 24, 2021, https://thediplomat.com/2021/09/south-korea-takes-first-step-to-regulate-virtual-asset-service-providers/.

68. "Bilateral Cooperation," Korea Financial Intelligence Unit website, https://www.kofiu.go.kr/eng/cooperation/bilateral.do; "Multilateral Cooperation," Korea Financial Intelligence Unit website, https://www.kofiu.go.kr/eng/cooperation/multilateral.do.

69. Danny Park, "U.S. Treasury Says Prioritize Sanctioning North Korea for Crypto Hacking," Yahoo, June 28, 2022; [단독] "北 가상화폐 사기 집중 파헤치는 중" . . . 한국 온 넬슨 美 차관 ([Exclusive] "Focusing on Virtual Currency Fraud in North Korea". . . U.S. Under Secretary Nelson), https://www.mk.co.kr/news/p

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.


Center for a
New American
Security