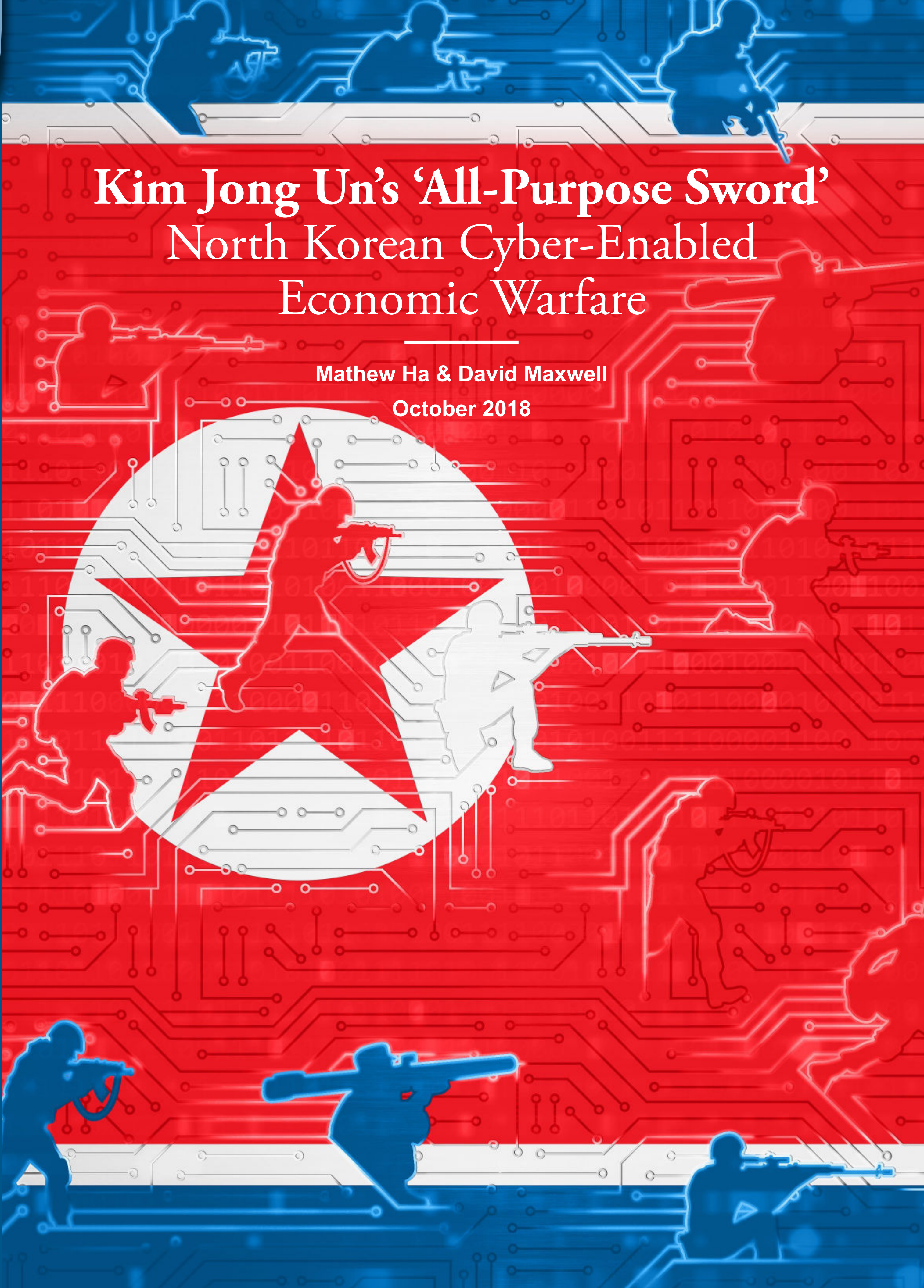
Kim Jong Un's 'All-Purpose Sword'

North Korean Cyber-Enabled Economic Warfare

Mathew Ha & David Maxwell

October 2018



FOUNDATION FOR DEFENSE OF DEMOCRACIES

Kim Jong Un's 'All-Purpose Sword'
North Korean Cyber-Enabled Economic Warfare

Mathew Ha

David Maxwell

October 2018

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

EXECUTIVE SUMMARY 6

CYBER IN THE CONTEXT OF NORTH KOREA'S STRATEGIC OUTLOOK 7

NORTH KOREAN CYBER PERSONNEL, TOOLS, RESOURCES, AND INTERNET INFRASTRUCTURE 10

Bureaucratic Structures 11

The Lazarus Group 13

Educational Institutions and Research Centers 14

Network and Internet Infrastructure 16

North Korea's IT Industry 17

NORTH KOREAN CYBER TACTICS AND CAPABILITIES: CASE STUDIES AND LESSONS LEARNED 18

Case Study 1: Economic Attacks – Ten Days of Rain (2011) and DarkSeoul Attack (2013) 19

Case Study 2: Cyber Terrorism – Sony Hack (2014) 20

Case Study 3: Extortion – Korea Hydro and Nuclear Power (2015) 22

Case Study 4: Cyber-enabled Theft – SWIFT and Cryptocurrency Exchanges (2016-2017) 23

Case Study 5: Cyber-enabled Theft – WannaCry (2017) 24

Case Study 6: Reconnaissance – Reaper and Operation GhostSecret (2018) 25

POLICY RECOMMENDATIONS 26

CONCLUSION 33

Executive Summary

North Korea pledged to "cease all hostile acts … in every domain" as part of the Panmunjom Declaration, which Kim Jong Un and South Korean President Moon Jae In signed in April.[1] When Kim met U.S. President Donald Trump in June, the North Korean leader committed to "build a lasting and stable peace."[2] Yet, even as diplomacy proceeded at the highest levels, Pyongyang continued to engage in cyber attacks against the national security and economic base of South Korea.[3] Experts estimate that South Korea suffers as many as 1.5 million attempted cyber intrusions from North Korean hackers every day.[4] Pyongyang uses cyber tools to support "active measures" and spread disinformation to sow division in South Korean society, and to undermine the Republic of Korea (ROK) government.[5]

The heavily sanctioned and cash-strapped North also uses cyber attacks to generate illicit funds from ransom payments,[6] cryptocurrency exchange hacks,[7] and fraudulent inter-bank transfer orders.[8] Cyber espionage has provided the regime with critical intelligence on its adversaries.[9] In September 2018, the Department of Justice pressed charges against a North Korean computer programmer, Park Jin Hyok, for not only working on behalf of the North Korean government, but also being involved in several infamous North Korean cyber operations such as the Sony Pictures hack, SWIFT Bangladesh Bank theft, and WannaCry, which will all be discussed in this report.[10] Attribution is often a tricky endeavor.[11] Yet, the Justice Department presents comprehensive evidence based on forensic technical analysis that link these major North Korean cyber intrusions back to Park.[12] This not only paints a clearer portrait of the Kim regime, but also the diverse range of offensive cyber capabilities Pyongyang employs.

[1] Panmunjom Declaration for Peace, Prosperity and Unification of the Korean Peninsula, Joint Security Area, April 27, 2018. (http://documents.latimes.com/panmunjom-declaration-peace/)

[2] The White House, "Joint Statement of President Donald J. Trump of the United States of America and Chairman Kim Jong Un," June 12, 2018. (https://www.whitehouse.gov/briefings-statements/joint-statement-president-donald-j-trump-united-states-america-chairman-kim-jong-un-democratic-peoples-republic-korea-singapore-summit/)

[3] Timothy W. Martin, "North Korea, While Professing Peace, Escalated Cyberattacks on South," *The Wall Street Journal*, May 25, 2018. (https://www.wsj.com/articles/north-korea-while-professing-peace-escalated-cyberattacks-on-south-1527239057?mod=e2twa&tesla=y); Adam Segal, "Whether the Kim-Trump Summit in Singapore Succeeds or Fails, North Korean Cyberattacks Likely to Continue," *Council on Foreign Relations*, June 7, 2018. (https://www.cfr.org/blog/whether-kim-trump-summit-singapore-succeeds-or-fails-north-korean-cyberattacks-likely-continue)

[4] Duk-Ki Kim, "The Republic of Korea's Counter-asymmetric Strategy," *Naval War College Review*, Winter 2012. (https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1447&context=nwc-review)

[5] Tae-jun Kang, "North Korea's Influence Operations, Revealed," *The Diplomat* (Japan), July 25, 2018. (https://thediplomat.com/2018/07/north-koreas-influence-operations-revealed/)

[6] "What you need to know about the WannaCry Ransomware," *Symantec*, May 23, 2017. (https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack)

[7] Luke McNamara, "Why Is North Korea So Interested in Bitcoin?" *FireEye*, September 11, 2017. (https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html)

[8] David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More." *The New York Times*, October 15, 2017. (https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html)

[9] Duk-Ki Kim, "The Republic of Korea's Counter-asymmetric Strategy," *Naval War College Review*, Winter 2012. (https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1447&context=nwc-review)

[10] U.S. Department of Justice, Press Release, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," September 6, 2018. (https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and)

[11] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: what Everyone Needs to Know* (New York: Oxford University Press, 2014), pages 72-75.

[12] Criminal Complaint, *United States of America v. Park Jin Hyok*, Case No. MJ18-1479 (C.D. Cal filed June 8, 2018), pages 13-22. (https://www.justice.gov/opa/press-release/file/1092091/download)

While Kim Jong Un's nuclear and missile arsenal present the most extreme threat, both the U.S. and ROK should take note of North Korea's growing cyber capabilities. These capabilities complement North Korea's conventional and unconventional military weapons in a highly effective manner. North Korea's cyber operations broaden the Kim family regime's toolkit for threatening the military, economic, and even the political strength of its adversaries and enemies.

Within the cyber domain, the United States and its allies should pay special attention to the emerging threat of cyber-enabled economic warfare (CEEW), or cyber attacks against an adversary "to weaken its economy and thereby reduce its political and military power."[13] CEEW attacks could compromise the networks of financial institutions, banks, and corporations that play an indispensable role in the nation's economy. Sustained or expanded North Korean cyber attacks on the critical infrastructure and economies of South Korea, the U.S., and other nations could threaten the foundation of their power. Even more insidious is how such cyber attacks, or even the threat of them, may change the policy calculus of dealing with North Korea going forward. Essentially, North Korea could hold military and diplomatic policy hostage by putting a country's industrial, financial, or energy sectors in its cyber cross hairs.

Although North Korea's cyber capabilities still cannot match those of Russia, China, and the U.S., they have improved substantially. Our case studies of six North Korean attacks show how their offensive tactics have evolved from basic distributed denial of service (DDoS) attacks to sophisticated use of malware. In 2013, the world witnessed the DarkSeoul attacks in South Korea in which Pyongyang first demonstrated its ability to inflict physical damage through cyber-enabled means against South Korean banks and media companies. A little over a year later, in November 2014, Pyongyang used these destructive capabilities against U.S.-based Sony Pictures. North Korea's cyber infiltration of more than a hundred private South Korea firms and government agencies between 2014 and 2016 foreshadows the battles to come. [14]

> **“Although North Korea's cyber capabilities still cannot match those of Russia, China, and the U.S., they have improved substantially. Our case studies of six North Korean attacks show how their offensive tactics have evolved from basic distributed denial of service (DDoS) attacks to sophisticated use of malware.”**

The case studies in this report are not all explicit examples of CEEW operations. However, each of has significant implications for the future of CEEW. As diplomatic efforts to dismantle North Korea's nuclear weapons program move forward – or even if they do not – the flexibility and plausible deniability of cyber capabilities may make them an even more attractive weapon for the Kim regime. To deal with this threat, the U.S., ROK, and other allies will have to enhance their resiliency while devising strategies to deter, thwart, and neutralize the North Korean threat.

Cyber in the Context of North Korea's Strategic Outlook

After the Korean War, North Korea developed asymmetric capabilities and tactics to exploit its enemies' vulnerabilities and close the conventional capabilities gap.[15] To that end, North Korea prioritized nuclear, chemical, and biological weapons of mass destruction (WMD) as well as the unorthodox use of

[13] Mercy A. Kuo, "Cyber-enabled Economic Warfare: Assessing U.S. Strategy," *The Diplomat* (Japan), March 21, 2018. (https://thediplomat.com/2018/03/cyber-enabled-economic-warfare-assessing-us-strategy/)

[14] Jack Kim, "North Korea mounts long-running hack of South Korea computers, says Seoul," *Reuters*, June 12, 2016. (https://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE)

[15] Steven Metz and Douglas V. Johnson II, *Asymmetry and U.S. Military Strategy, Definition, Background, and Strategic Concepts* (U.S. Army War College, June 2001), page 1. (http://ssi.armywarcollege.edu/pdffiles/pub223.pdf)

artillery and other conventional capabilities.[16] South Korea's Ministry of National Defense also concluded that the North would employ hybrid warfare, guerilla warfare, and blitzkrieg tactics.[17] In the event of conflict, Pyongyang's objective would be to inflict a swift and devastating attack on the U.S. and/or South Korea to force a stalemate.[18]

"Experts believe that North Korea does not yet possess the capability to engage in sustained cyber warfare against military targets in a direct confrontation with the United States. Instead, they speculate that North Korean cyber attacks in a live-war scenario could target civilian entities whose paralysis would disrupt U.S. and South Korean military capabilities."

Cyber operations have become central components of North Korea's asymmetric military strategy, peacetime provocations, and illicit activities. Kim Jong Un has reportedly said, "Cyber warfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly."[19] Not only does cyber provide command and control advantages, but the flexibility of cyber weapons – especially compared to conventional and nuclear weapons – provides additional strategic options across the entire spectrum from peace (or armistice[20]) to war. In particular, the difficulty of attributing cyber attacks provides Pyongyang's leadership with plausible deniability, thereby reducing the risk of retaliation and allowing it to operate in the gray zone between peace and war.[21]

Kim Heung Kwang, a North Korean defector who taught computer science at Hamheung University, assessed that North Korea's military heavily integrates information warfare into contemporary warfighting plans.[22] North Korea's "quick war, quick end" strategy prioritizes compromising an enemy's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities. CSIS' Jenny Jun, Scott LaFoy, and Ethan Sohn note, "North Korean cyber doctrine, if one exists, may be premised on the idea that an extensively networked military is vulnerable to cyber capabilities."[23]

Experts believe that North Korea does not yet possess the capability to engage in sustained cyber warfare against military targets in a direct confrontation with the United States. Instead, they speculate that North Korean cyber attacks in a live-war scenario could target civilian entities whose paralysis would disrupt U.S. and South Korean military capabilities. For instance, Jason Healey of Columbia University suggests that

[16] Franz-Stefan Gady, "Military Stalemate: How North Korea Could Win a War With the US," *The Diplomat* (Japan), October 10, 2017. (https://thediplomat.com/2017/10/military-stalemate-how-north-korea-could-win-a-war-with-the-us/)

[17] "2016 Defense White Paper," Ministry of National Defense – Republic of Korea, December 31, 2016, 30-32

[18] Franz-Stefan Gady, "Military Stalemate: How North Korea Could Win a War With the US," *The Diplomat* (Japan), October 10, 2017. (https://thediplomat.com/2017/10/military-stalemate-how-north-korea-could-win-a-war-with-the-us/)

[19] Leekyung Ko, "North Korea as a Geopolitical and Cyber Actor," *New America*, June 6, 2018. (https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/north-korea-geopolitical-cyber-incidents-timeline/)

[20] Note the Korean War has only been temporarily suspended by the July 27, 1953 Armistice and technically both Koreas remain in a state of civil war.; The Korean War Armistice Agreement, Panmunjom, Korea, July 27, 1953, Article 2. (http://www.usfk.mil/Portals/105/Documents/SOFA/G_Armistice_Agreement.pdf)

[21] Emma Chanlett-Avery, Liana W. Rosen, John W. Rollins, and Catherine A. Theohary, "North Korean Cyber Capabilities: In Brief," *Congressional Research Service*, August 3, 2017, page 3. (https://fas.org/sgp/crs/row/R44912.pdf)

[22] James Cook, "A defector says North Korea's hacker army is capable of 'destroying cities,'" *Business Insider*, May 29, 2015. (http://www.businessinsider.com/north-korean-defector-professor-kim-heung-kwang-hackers-claim-destroy-city-bureau-21-2015-5); "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, pages 27-28. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape)

[23] Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Response," *Center for Strategic and International Studies (CSIS)*, December 2015, page 5. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf)

North Korean cyber attacks in wartime would focus on American shipping and airports to disrupt the transport of additional forces to the region. Similarly, for South Korea, the North's cyber forces could target transportation and financial infrastructure to increase public panic and delay evacuation of Seoul. Such operations would only require rudimentary disruptive capabilities, such as DDoS attacks and ransomware, which North Korean operators have used in the past.[24] In short, North Korea likely cannot win a cyber war, but it could hobble the U.S. and its allies using disruptive capabilities in a wartime scenario.

> **"The North could extort concessions by simply posing the threat of a CEEW attack on a target critical to its adversaries' economic strength and vitality. If North Korea agrees to limit its nuclear weapons program, cyber-enabled economic warfare will likely become an even larger component of this peacetime provocation strategy."**

Cyber operations also play a crucial role in North Korea's "peacetime provocations" strategy: North Korea incites unrest and disrupts the status quo without crossing the threshold of war to win political and economic concessions that ensure the survival of the Kim family regime.[25] Peacetime provocations force Pyongyang's targets to choose between escalating tensions and acquiescing to North Korean demands.[26] Showcasing and testing nuclear weapons and ballistic missiles was the cornerstone of this strategy.[27] The North Korean government also relied on violence and state-sponsored crime, such as the assassination raids and attempted bombings of the 1960s.[28] Today, cyber-enabled economic warfare operations potentially provide a low-cost, alternative tool to diversify these peacetime provocations. The North could extort concessions by simply posing the threat of a CEEW attack on a target critical to its adversaries' economic strength and vitality. If North Korea agrees to limit its nuclear weapons program, cyber-enabled economic warfare will likely become an even larger component of this peacetime provocation strategy. And unlike the North's development of nuclear weapons, which did not stop the growth of South Korea's economy from one of the poorest in the world in 1960 to one of the richest today, a purposeful campaign of CEEW could potentially curtail the greatest advantage the South holds over the North.

Another component of the strategy to ensure the survival of the Kim regime is the generation of hard currency. For decades, North Korea has used illicit financial activities to fund the regime's military capabilities and the lavish lifestyle of the Kim family. These activities include narcotics production and distribution, trafficking of endangered species, counterfeiting currency, and manufacturing counterfeit cigarettes.[29] Cyber crime is another way the regime illicitly funds

[24] **24.** Franz-Stefan Gady, "Military Stalemate: How North Korea Could Win a War With the US," *The Diplomat* (Japan), October 10, 2017. (https://thediplomat.com/2017/10/military-stalemate-how-north-korea-could-win-a-war-with-the-us/)

[25] **25.** Jung H. Pak, "Kim Jong-un's tools of coercion," *Brookings*, June 21, 2018. (https://www.brookings.edu/blog/order-from-chaos/2018/06/21/kim-jong-uns-tools-of-coercion/)

[26] **26.** Richard J. Andres, "Cyber Gray Space Deterrence," *Prism*, December 21, 2017. (http://cco.ndu.edu/News/Article/1401927/cyber-gray-space-deterrence/)

[27] **27.** Victor Cha and David Kang, *Nuclear North Korea: A Debate on Engagement Strategies* (New York, NY: Columbia University Press, 2003), pages 72-75.

[28] **28.** Joshua Stanton, *Arsenal of Terror: North Korea, State Sponsor of Terrorism* (The Committee for Human Rights in North Korea, 2015), pages 12-14. (https://www.hrnk.org/uploads/pdfs/4_27_15_Stanton_ArsenalofTerror.pdf)

[29] **29.** Sheena Chestnut Greitens, *Illicit: North Korea's Evolving Operations to Earn Hard Currency* (The Committee for Human Rights in North Korea, 2014). (https://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf)

itself. The cyber heist targeting the Bank of Bangladesh stole $81 million.[30] If such heists were common, cyber crime could become Pyongyang's primary source of illicit revenue.

> **"As North Korea continues to advance and fine-tune its destructive cyber tools and capabilities, Kim Jong Un may see an advantage in shifting from revenue generation to destructive cyber attacks against U.S. and allied targets, including critical infrastructure, industrial supply chains, and systemically important firms in key industries."**

This pursuit of revenue likely aligns with broader trends in North Korea's malicious cyber activities. According to security experts at Cisco, "Revenue generation is still the top objective of most threat actors." They warn, however, that "some adversaries now have the ability—and often now, it seems, the inclination—to lock systems and destroy data as part of their attack process," calling this "new and devastating type of attack" a "Destruction of Service (DeOS)."[31] As North Korea continues to advance and fine-tune its destructive cyber tools and capabilities, Kim Jong Un may see an advantage in shifting from revenue generation to destructive cyber attacks against U.S. and allied targets, including critical infrastructure, industrial supply chains, and systemically important firms in key industries.

The limited scope of Pyongyang's observed cyber attacks suggests that Kim Jong Un and his cyber operators may currently believe that destructive operations create more risks than benefits. However, if the regime were to experience a drastic crisis in relations with its adversaries, it may conclude that destructive cyber attacks would enhance deterrence and promote survival.

North Korean Cyber Personnel, Tools, Resources, and Internet Infrastructure

The South Korean Ministry of National Defense reported in 2014 that North Korea has approximately 6,000 cyber operatives who conduct "cyber warfare, including the interruption of military operations and attacks against major national infrastructure."[32] For comparison, that is roughly the same number of troops in U.S. Cyber Command's mission force. Though such comparisons are imprecise at best, the most important considerations are North Korea's capabilities and intentions, which are difficult to assess.[33] Despite the common view that North Korea is so impoverished it has minimal technical capabilities, Pyongyang has devoted substantial time and resources to advancing its cyber power. Defector Kim Heung Kwang suggested the North Korean government allocates 10 to 20 percent of its military budget to cyber operations, a figure that has not been verified.[34] Ultimately, one can

[30] Ju-min Park and James Pearson, "Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West," *Reuters*, May 20, 2017. (https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020)

[31] "Cisco 2017 Midyear Cybersecurity Report," *Cisco*, July 2017, page 3. (https://www.automation.com/pdf_articles/cisco/Cisco_2017_MCR_Embargoed_til_072017_5_AM_PT_8_AM_ET.pdf)

[32] Republic of Korea Ministry of National Defense, "2014 Defense White Paper," December 31, 2014, page 27. (http://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201704260250138940.pdf)

[33] Mark Pomerleau, "Here's how to ensure readiness of cyber forces," *Fifth Domain*, May 29, 2018. (https://www.fifthdomain.com/dod/cybercom/2018/05/29/heres-how-to-ensure-readiness-of-cyber-forces/)

[34] Daye Lee and Nick Kwek, "North Korean hackers 'could kill,' warns key defector," *BBC* (UK), May 29, 2015. (https://www.bbc.com/news/technology-32925495)

only speculate about the extent of North Korea's cyber personnel and their funding.[35]

Bureaucratic Structures

The Reconnaissance General Bureau (RGB) is the regime's primary agency responsible for cyber activity.[36] Established between 2009 and 2010 amidst a restructuring of the country's intelligence and national security organs,[37] the RGB is independent of the North Korean conventional military, the Korean People's Army (KPA), and reports directly to the regime's highest decision-making body, the State Affairs Commission led by Kim Jong Un.[38] According to the Pentagon, the State Affairs Commission tasks the RGB with North Korea's terrorist, clandestine, and illicit activities.[39] The bureau's autonomy from the regular military and its inclusion of cyber specializing in clandestine and terrorist activities suggests that North Korea sees cyber capabilities as extending beyond military assets.

The U.S. Treasury Department sanctioned the RGB twice for its activities, first in 2010 under Executive Order 13551[40] for facilitating North Korean arms trading, money laundering, and other illicit activities,[41] as well as in 2015 under Executive Order 13687 for being an entity controlled by the North Korean government[42] to hold the Kim family regime accountable for the Sony Pictures hack.[43] The United Nations also sanctioned the RGB following Pyongyang's fourth nuclear test on January 6, 2016.[44]

[35] **35.** Emma Chanlett-Avery, Liana W. Rosen, John W. Rollins, and Catherine A. Theohary, "North Korean Cyber Capabilities: In Brief," *Congressional Research Service*, August 3, 2017. 3-4. (https://fas.org/sgp/crs/row/R44912.pdf)

[36] **36.** Karen Deyoung, Ellen Nakashima, and Emily Rauhala, "Trump signed presidential directive ordering actions to pressure North Korea," *The Washington Post*, September 30, 2017. (https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html?utm_term=.f18ccc1ae178)

[37] **37.** For more information on the reorganization, see: Joseph S. Bermudez, "A New Emphasis on Operations Against South Korea? A Guide to North Korea's Intelligence Reorganization and the General Reconnaissance Bureau," *38 North*, June 11, 2010. (https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf)

[38] **38.** Prior to 2016, RGB reported directly to the senior leadership of the National Defense Commission. When the State Affairs Commission replaced the National Defense Commission, RGB began reporting to this organ; "North Korea reorganizes security services," *IHS Janes*, 2016. (http://www.janes360.com/images/assets/196/66196/North_Korea_reorganises_security_services.pdf); Kim So-hyun, "Kim visits army unit spying on S. Korea," *The Korea Herald* (South Korea), April 27, 2010. (http://www.koreaherald.com/view.php?ud=20100427000663); Joseph S. Bermudez Jr., "A New Emphasis on Operations Against South Korea? A Guide to North Korea's Intelligence Reorganization and the General Reconnaissance Bureau," *38 North*, June 11, 2010, page 4. (https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf); Fydoor Tertitskiy, "How the North is run: the State Affairs Commission," *NK News* (South Korea), February 2, 2018. (https://www.nknews.org/pro/the-history-and-evolution-of-north-koreas-state-affairs-commission/)

[39] **39.** U.S. Department of Defense, Office of the Secretary of Defense, "Military and Security Developments Involving the Democratic People's Republic of Korea – Report to Congress," December 15, 2017. (https://fas.org/irp/world/dprk/dod-2017.pdf)

[40] **40.** President Obama signed Executive Order 13551 on August 30, 2010, which authorized the Treasury Department to sanction any persons engaged in importing or exporting North Korean arms and arms-related material, money laundering, illicit economic activity, trafficking, and luxury goods sanctions evasion. This EO was in response to North Korea sinking the *Cheonan* South Korean naval corvette and its 2009 nuclear test. Executive Order 13551, "Blocking Property of Certain Persons With Respect to North Korea," August 30, 2010. (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/Executive%20Order%2013551.pdf)

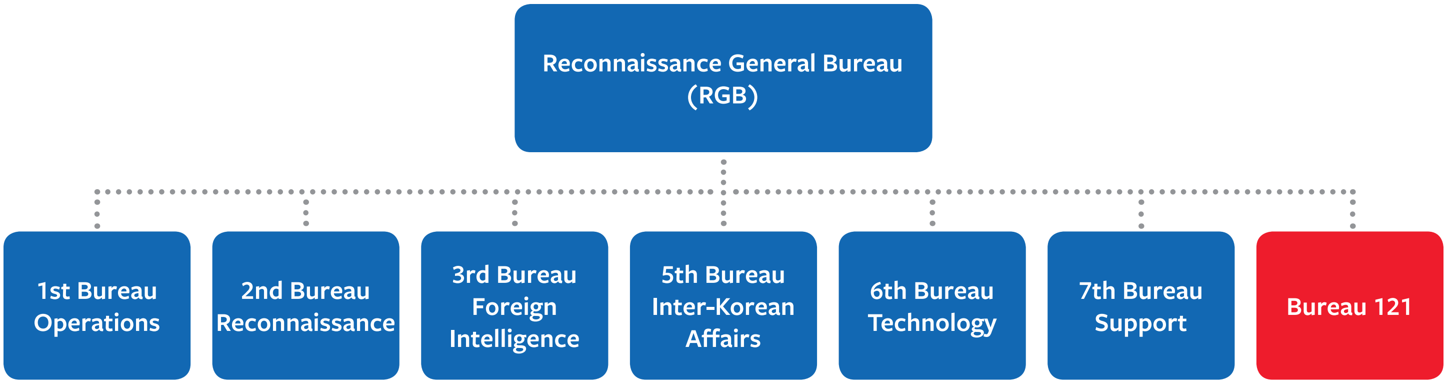
[41] **41.** U.S. Department of the Treasury, "Recent OFAC Actions - August 30, 2010," August 30, 2010. (https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20100830.shtml.aspx)

[42] **42.** U.S. Department of the Treasury, Press Releases, "Treasury Imposes Sanctions Against the Government of the Democratic People's Republic of Korea," January 2, 2015. (https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx)

[43] **43.** Executive Order 13551, "Blocking Property of Certain Persons with Respect to North Korea," August 30, 2010. (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/Executive%20Order%2013551.pdf); U.S. Department of the Treasury, Press Release, "Treasury Imposes Sanctions Against the Government of The Democratic People's Republic of Korea," January 2, 2015. (https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx)

[44] **44.** United Nations Security Council, Press Release, "Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Unanimously Adopting Resolution 2270 (2016)," March 2, 2016. (https://www.un.org/press/en/2016/sc12267.doc.htm)

Reconnaissance General Bureau (RGB)[45]


Reconnaissance General Bureau (RGB)
1st Bureau Operations
2nd Bureau Reconnaissance
3rd Bureau Foreign Intelligence
5th Bureau Inter-Korean Affairs
6th Bureau Technology
7th Bureau Support
Bureau 121

Bureau 121 is the primary RGB office for cyber duties.[46] Bureau 121 is instrumental in technical reconnaissance tasks as well as disruptive operations, such as infiltrating computer networks, hacking to extract foreign intelligence, and deploying viruses on adversary computer networks.[47] Additionally, the bureau allegedly tasked its hackers with attacking South Korean businesses.[48] The RGB created it "sometime after" 2013, according to threat intelligence firm Recorded Future.[49] The Korean Institute of National Unification (KINU), a South Korean government-funded think tank, assessed the bureau is made up of approximately 300 agents.[50] However, there are conflicting estimates. For instance, Jang Se Yul, a North Korean defector who studied computer science at North Korea's University of Automation, stated there were 1,800 agents in Bureau 121.[51]

Bureau 121 is based at the main RGB headquarters in the Moonshin-dong area of Pyongyang, according to the Center for Strategic and International Studies.[52] Until recently, Bureau 121 also operated

[45] **45.** "North Korea Cyber Activity," Recorded Future, J*une 14, 2017. (*https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf); Joseph S. Bermudez Jr., "A New Emphasis on Operations Against South Korea? A Guide to North Korea's Intelligence Reorganization and the General Reconnaissance Bureau," 38 North, June 11, *2010. (*https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf); Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Response," *Center for Strategic and International Studies, December 2015. (*https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf)

[46] **46.** Ju-min Park and James Pearson, "In North Korea, hackers are a handpicked, pampered elite," *Reuters*, December 5, 2014. (https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205)

[47] **47.** Kuyoun Chung and Kitae Lee, "Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicle," *Korea Institute for National Unification*, 2017, page 21.

[48] **48.** Lee Kil-seong, "N. Korean Hotel in China forced to close," *The Chosun Ilbo* (South Korea), January 10, 2018. (http://english.chosun.com/site/data/html_dir/2018/01/10/2018011001157.html?Dep0=twitter)

[49] **49.** "North Korea Cyber Activity," *Recorded Future*, June 14, 2017. (https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf)

[50] **50.** Kuyoun Chung and Kitae Lee, "Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicle," *Korea Institute for National Unification*, 2017, page 22.

[51] **51.** Ju-min Park and James Pearson, "In North Korea, hackers are a handpicked, pampered elite," *Reuters*, December 5, 2014. (https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205)

[52] **52.** Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Response," *Center for Strategic and International Studies*, December 2015, pages 40-42. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf)

a supplementary command post in the Chilbosan Hotel in Shenyang, the capital of Liaoning province in China.[53] In January, the Shenyang city government closed the hotel as part of Beijing's increased compliance with UN sanctions. According to South Korean newspaper *The Chosun Ilbo*, a notice on the hotel front door stated, "We've closed down according to an administrative order from the Shenyang city government. All business operations of the hotel have stopped."[54] It is unclear if the hackers operating out of the Chilbosan Hotel returned to North Korea or relocated to a third country. Previously, North Korean cyber attacks have originated from China, India, Malaysia, Vietnam, and New Zealand, to name a few.[55]

Unit 180 is another hacking unit allegedly responsible for attacking financial institutions. According to North Korea defector Kim Heung Kwang, Unit 180's cyber operations focus on stealing money from foreign banks.[56] Although he defected in 2004, Kim claims he still has contacts inside North Korea that provide him with current and relevant information. He notes that Unit 180 hackers generally operate overseas to make it harder to attribute their operations to North Korea.[57] Kim Heung Kwang did not specify whether this unit is independent of Bureau 121.

The North Korean military has also developed cyber capabilities separate from the RGB. Within the KPA, cyber programs are operated by the General Staff Department (GSD). The GSD is responsible for KPA's preparedness for war.[58] Its primary responsibility regarding cyber is to integrate emerging tools and weapons into North Korea's warfighting strategy.[59] The KPA does not have a single cyber command but rather divides information warfare, electronic warfare, psychological warfare, and related tasks between its Operations Bureau, Communications Bureau, Electronic Warfare Bureau, and Enemy Collapse Sabotage Bureau.[60] The GSD's Command Automation Bureau is responsible for conducting cyber warfare operations.[61]

The Lazarus Group

In 2016, the private cyber security company Novetta identified Lazarus Group in connection with the Sony Pictures attack. Novetta noted that the group "has been active since at least 2009, and potentially as early as 2007,

[53] "In China's Shadow: Exposing North Korean Overseas Networks," *Asan Institute and C4ADS*, August 2016, page 36 (http://en.asaninst.org/contents/in-chinas-shadow/); Lee Kil-seong, "N. Korean Hotel in China forced to close," *The Chosun Ilbo* (South Korea), January 10, 2018. (http://english.chosun.com/site/data/html_dir/2018/01/10/2018011001157.html?Dep0=twitter)

[54] Lee Kil-seong, "N. Korean Hotel in China forced to close," *The Chosun Ilbo* (South Korea), January 10, 2018. (http://english.chosun.com/site/data/html_dir/2018/01/10/2018011001157.html?Dep0=twitter)

[55] U.S. Computer Emergency Readiness Team, "Alert (TA17-318A): HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL," November 14, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-318A)

[56] Ju-min Park and James Pearson, "Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West," *Reuters*, May 20, 2017. (https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020); Kim Jaewon, "A cybersecurity defector warns of North Korea's 'hacker army,'" *Nikkei Asian Review* (Japan), May 25, 2017. (https://asia.nikkei.com/magazine/20170525/Politics-Economy/A-cybersecurity-defector-warns-of-North-Korea-s-hacker-army?page=2)

[57] Ju-min Park and James Pearson, "Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West," *Reuters*, May 20, 2017. (https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020)

[58] "General Staff Operations Bureau," *38 North*, March 17, 2018. (http://www.nkleadershipwatch.org/dprk-security-apparatus/general-staff-operations-bureau/)

[59] Donghui Park, "North Korea Cyber Attacks: A new Asymmetrical Military Strategy," *The Henry M. Jackson School of International Studies at the University of Washington*, June 28, 2016. (https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/)

[60] Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Response," *Center for Strategic and International Studies*, December 2015, pages 45-50. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf)

[61] Kuyoun Chung and Kitae Lee, "Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicle," *Korea Institute for National Unification*, 2017, page 23.

and was responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment." Novetta did not tie the Lazarus Group directly to the North Korean government, but noted that the Sony attack "was carried out by a single group, or potentially very closely linked groups, sharing technical resources, infrastructure, and even tasking."[62] Previously, the FBI had attributed the Sony attack to the North Korean government, noting that a group calling itself "Guardians of Peace" had claimed responsibility.[63] The FBI based its assessment on technical similarities in the code, encryption algorithms, data deletion methods, and infrastructure used in prior North Korea-affiliated attacks. Subsequent investigations of the same malware samples by Kaspersky Labs, McAfee, and Recorded Future found traces of Lazarus malware tools and shared network infrastructure.[64]

In 2017, the U.S. government determined that actors responsible for the "Hidden Cobra" campaign were also members of the Lazarus Group and the Guardians of Peace. Washington also linked the WannaCry attacks to this same group.[65] The U.S. government and private security firms have not specified, however, if Lazarus Group is affiliated with Bureau 121 or other offices in the North Korean bureaucracy.

Educational Institutions and Research Centers

North Korea recruits and trains its cyber operators through the regime's education system. Within North Korea's primary schools, students that excel in mathematics and science are separated from others to pursue special training, according to defectors.[66] This training includes computer-related classes, but also foreign language study, such as Chinese, Japanese, and English.[67] The regime reportedly then selects the top 500 students from secondary schools for training at the university level.[68] Selected students attend universities such as Kim Il Sung University College of Computer Science, Kim Chaek University of Technology, Mirim University, and several others. Students train to become state-sponsored hackers as well as software and hardware developers for indigenous North Korean technology companies.[69]

Of the technology and cyber programs, Mirim University appears to be the most selective as it chooses only 100 students each year for its specialized five-year cyber intelligence and warfare program. The university's curriculum includes command

[62] **62.** "Operation Blockbuster: Unraveling the Long Thread of the Sony Attack," *Novetta*, 2016. (https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf)

[63] **63.** U.S. Federal Bureau of Investigation, Press Release, "Update on Sony Investigation," December 19, 2014. (https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation)

[64] **64.** Ryan Sherstobitoff, "Lazarus Resurfaces, Targets Global Banks and Bitcoin Users," *McAfee*, February 12, 2018. (https://securingtomorrow.mcafee.com/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/); Priscilla Moriuchi, "North Korea Embraces Cryptocurrency to Counter Global Financial Isolation," *Recorded Future*, February 14, 2018. (https://www.recordedfuture.com/north-korea-cryptocurrency/)

[65] **65.** U.S. Computer Emergency Readiness Team, "Alert (TA17-164A): HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure," June 13, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-164A); 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?noredirect=on&utm_term=.03c95a7714cc); Thomas P. Bossert, "It's Official: North Korea is Behind Wannacry," *The Wall Street Journal*, December 18, 2017. (https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537)

[66] **66.** Bruce Harrison, "How North Korea recruits its army of young hackers," *NBC News*, December 8, 2017. (https://www.nbcnews.com/news/north-korea/how-north-korea-recruits-trains-its-army-hackers-n825521)

[67] **67.** "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, pages 40-41. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape)

[68] **68.** Kim Jaewon, "A cybersecurity defector warns of North Korea's 'hacker army,'" *Nikkei Asian Review* (Japan), May 25, 2017. (https://asia.nikkei.com/magazine/20170525/Politics-Economy/A-cybersecurity-defector-warns-of-North-Korea-s-hacker-army?page=2)

[69] **69.** Bruce Harrison, "How North Korea recruits its army of young hackers," *NBC News*, December 8, 2017. (https://www.nbcnews.com/news/north-korea/how-north-korea-recruits-trains-its-army-hackers-n825521)

automation, programming, automated reconnaissance, and electronic warfare.[70] According to KINU, Mirim University serves as a direct conduit to the RGB, and the RGB accepts the top 10 graduates from the university each year.[71]

> **"The South Korean government indicted five South Korean nationals who distributed this software exploit after purchasing it from North Korean developers based in Heilongjiang, China. The South Korean investigation connected the North Korean developers in China to KCC and determined they were earning revenue for Office 39, which is the state entity in charge of amassing personal funds for the North Korean leader."**

Defectors have reported that among the 500 students selected annually for university-level training, some study abroad in China and Russia.[72] An anonymous North Korean defector, using the pseudonym Jong, reported that the regime selected him to study computer science at an early age based on his test scores. He went on to study abroad in China in his third year at university. After finishing his degree, Jong first worked for a state-owned software development agency and later in China as a state-sponsored hacker. According to Jong, the North Korean regime also sends newly trained hackers to China to earn money for the regime. Operatives study beta versions of video games and anti-virus software and create pirated versions to sell online through Chinese clients.[73]

The state-run Korea Computer Center (KCC) is the regime's premier IT research and development center. It also serves as the authority for production, management, distribution, and sale of its products. The KCC reportedly has nine production centers and 11 regional centers[74] and operates overseas offices in Germany, China, and Syria.[75] KCC has developed products such as Samjiyeon tablet PCs and the Linux-based Red Star operating system.[76]

KCC personnel have been involved in cyber crimes that directly benefitted the regime. In 2011, KCC employees operating in China collaborated with Chinese hackers to develop and sell software exploits for a popular South Korean online videogame called *Lin`age*.[77] The South Korean government indicted five South Korean nationals who distributed this software exploit after purchasing it from North Korean developers based in Heilongjiang, China. The South Korean investigation connected the North Korean developers in China to KCC and determined

[70] "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, pages 41-42. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape)

[71] Kuyoun Chung and Kitae Lee, "Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicle," *Korea Institute for National Unification*, 2017, page 21.

[72] Kim Jaewon, "A cybersecurity defector warns of North Korea's 'hacker army,'" *Nikkei Asian Review* (Japan), May 25, 2017. (https://asia.nikkei.com/magazine/20170525/Politics-Economy/A-cybersecurity-defector-warns-of-North-Korea-s-hacker-army?page=2)

[73] Sam Kim, "Inside North Korea's Hacker Army," *Bloomberg*, February 7, 2018. (https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army)

[74] Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Response," *Center for Strategic and International Studies*, December 2015, page 28. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf)

[75] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Suppliers of North Korea's Nuclear and Weapons Proliferation Programs," June 1, 2017. (https://www.treasury.gov/press-center/press-releases/Pages/sm0099.aspx)

[76] "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, page 13. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape)

[77] Sam Kim, "Inside North Korea's Hacker Army," *Bloomberg*, February 7, 2018. (https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army)

they were earning revenue for Office 39,[78] which is the state entity in charge of amassing personal funds for the North Korean leader. The U.S. Treasury Department sanctioned Office 39 on August 30, 2010 for engaging in illicit economic activity to support the North Korean government.[79] In June 2017, Treasury also sanctioned KCC for generating funds to support the Kim family regime and the U.S.- and UN-sanctioned Munitions Industry Department, which oversees ballistic missile development.[80]

Network and Internet Infrastructure

North Korea divides its domestic internet service between its nationwide *Kwangmyong* 'intranet' with no connection to the World Wide Web and a separate service that provides a limited outward facing internet connection.[81] The Ministry of Posts and Telecommunications is responsible for distributing North Korea's outward facing internet addresses through the Star Joint Venture Company.[82] Since 2010, Chinese internet provider Unicom has provided the first link that connects Star Joint Venture Company to the World Wide Web.[83] Intermittent electric power outages further limit the capacity of North Korea's internet and intranet networks.[84]

The regime reserves its outward facing connection for elites as well as students training to become Pyongyang's cyber warriors. It heavily monitors users for any subversive activity.[85] Following an extended U.S. Cyber Command campaign to cut off North Korean internet access,[86] North Korea opened a new outward facing internet connection in October 2017 provided by the Russian telecommunications company, TransTelecom.[87] The addition of this Russian network could strengthen Pyongyang's resilience against U.S. cyber actions.[88]

Given the regime's total control over the nation's internet activity, Hewlett-Packard's security experts conclude that North Korea's cyber operators "do not typically launch attacks directly from within North Korea." Attribution

[78] "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, page 54. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape)
[79] U.S. Department of the Treasury, "Recent OFAC Actions – August 30, 2010," August 30, 2010. (https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20100830.shtml.aspx)
[80] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Suppliers of North Korea's Nuclear and Weapons Proliferation Programs," June 1, 2017. (https://www.treasury.gov/press-center/press-releases/Pages/sm0099.aspx)
[81] Martyn Williams, "North Korea moves quietly onto the Internet," *Computer World*, June 10, 2010. (https://www.computerworld.com/article/2518914/enterprise-applications/north-korea-moves-quietly-onto-the-internet.html)
[82] "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, pages 12-13. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape); Ian Talley, "Cigarettes and Murky Joint Ventures Help North Korea evade crackdown," *The Wall Street Journal*, January 14, 2018. (https://www.wsj.com/articles/opaque-joint-ventures-help-north-korea-evade-crackdown-1515931201)
[83] Martyn Williams, "Russia Provides New Internet Connection to North Korea," *38 North*, October 1, 2017. (http://www.38north.org/2017/10/mwilliams100117/)
[84] "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, page 11. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape)
[85] Ibid.
[86] Karen DeYoung, Ellen Nakashima, and Emily Rauhala, "Trump signed presidential directive ordering actions to pressure North Korea," *The Washington Post*, September 30, 2017. (https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html?utm_term=.233e60bfcbc7)
[87] Adam Taylor, "North Korea appears to have a new Internet connection – thanks to help of a state-owned Russian firm," *The Washington Post*, October 2, 2017. (https://www.washingtonpost.com/news/worldviews/wp/2017/10/02/north-korea-appears-to-have-a-new-internet-connection-thanks-to-the-help-of-a-state-owned-russian-firm/?utm_term=.8523538b9c86)
[88] Martyn Williams, "Russia Provides New Internet Connection to North Korea," *38 North*, October 1, 2017. (http://www.38north.org/2017/10/mwilliams100117/)

would be too easy.[89] Defectors have corroborated that the North Korean government sends its hackers abroad so that Pyongyang can obfuscate their origin.[90] Indeed, Recorded Future detected a "near absence" of malicious cyber activity originating from inside North Korea between April and July of 2017, a time of increased hostility between North Korea and the United States.[91]

North Korea reportedly has a significant physical and virtual presence in China, India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, and Indonesia for launching malicious cyber operations. According to Recorded Future, 10 percent of all malicious North Korean cyber activity emanates from China, and another 20 percent from India.[92] Defectors have verified that North Korea deploys teams of hackers to carry out offensive cyber operations in Shenyang, China.[93] Recorded Future suggest there could be North Korean operatives, most likely students, operating from at least seven Indian universities and as research institutes.[94]

North Korea's IT Industry

In 2015, the Center for Strategic and International Studies assessed that North Korea prioritized the development of an indigenous information technology (IT) industry for software development.[95] The Ministry of Electric Power Industry and the Ministry of Posts and Telecommunications oversee North Korea's IT industry.[96]

North Korean firms now provide a wide range of products and services including "website and app development, administrative and business management software, radio and mobile communications platforms, IT security software, and biometric identification software for law enforcement," with customers across China, Russia, South Asia, the Middle East, and Africa.[97]

A notable company involved in North Korean IT exports is Malaysia-based Glocom, which the UN Panel

[89] "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, page 60. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape)

[90] Will Ripley, "North Korean defector: 'Bureau 121' hackers operating in China," *CNN*, January 7, 2015. (https://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html); Sam Kim, "Inside North Korea's Hacker Army," *Bloomberg*, February 7, 2018. (https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army); Adam Segal, "Whether The Kim-Trump Summit in Singapore Succeeds or Fails, North Korean Cyberattacks Likely to Continue," *Council on Foreign Relations*, June 7, 2018. (https://www.cfr.org/blog/whether-kim-trump-summit-singapore-succeeds-or-fails-north-korean-cyberattacks-likely-continue)

[91] "North Korea's Ruling Elite Are Not Isolated," *Recorded Future*, July 25, 2017. (https://www.recordedfuture.com/north-korea-internet-activity/); During this period, North Korea conducted eight short-, medium-, and intermediate-range ballistic missile launches and two inter-continental ballistic missile (ICBM) tests. Specific dates and details can be found here: "North Korean Provocations and U.S.-ROK Military Exercises," *Beyond Parallel*, April 3, 2017. (https://beyondparallel.csis.org/north-korean-provocations-us-rok-military-exercises/)

[92] "North Korea's Ruling Elite Are Not Isolated," *Recorded Future*, July 25, 2017. (https://www.recordedfuture.com/north-korea-internet-activity/); U.S. Computer Emergency Readiness Team, "Alert (TA17-318B): HIDDEN COBRA – North Korean Trojan: Volgmer," November 22, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-318B)

[93] Josh Horowitz, "Researchers have found an unexpected axis of North Korea's cyber activity: India," *Quartz*, October 22, 2017. (https://qz.com/1105149/india-is-an-unexpected-axis-of-north-koreas-suspect-cyber-activity/)

[94] "North Korea's Ruling Elite Are Not Isolated," *Recorded Future*, July 25, 2017. (https://www.recordedfuture.com/north-korea-internet-activity/)

[95] Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Response," *Center for Strategic and International Studies*, December 2015, page 52. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf)

[96] "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *Hewlett-Packard*, August 2014, pages 43-44. (https://www.slideshare.net/crash1980/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape)

[97] Andrea Berger, Cameron Trainer, Shea Cotton, and Catherine Dill, "The Shadow Sector: North Korea's Information Technology Networks," *James Martin Center for Nonproliferation Studies of the Middlebury Institute of International Studies at Monterey*, May 2018, page 1. (https://www.nonproliferation.org/wp-content/uploads/2018/05/op36-the-shadow-sector.pdf)

of Experts identified as a front for the RGB.[98] While Glocom is a defense firm that sells radios, military communications equipment, battle management systems, and command-and-control systems,[99] North Korean individuals affiliated with Glocom, such as Kim Chang Hyok, operate IT companies, such as Malaysia-based WCW Resources Sdn Bhd.[100] Kim Chang Hyok is the representative of a Singapore-based company called Pan Systems. Pan Systems allegedly operates Glocom, according to Reuters.[101] Analysts at the James Martin Center for Nonproliferation Studies of the Middlebury Institute of International Studies warn that North Korea could use indigenously developed software to disseminate malicious code, although no such reported incidents have yet occurred.[102] The revenue generated by these IT companies does, however, provides an alternative source of income for the Kim family regime and also undermines UN sanctions.

North Korean Cyber Tactics and Capabilities: Case Studies and Lessons Learned

North Korea first demonstrated its emerging cyber capabilities in July 2009 when its operators carried out a series of DDoS attacks on 27 different South Korean and American websites belonging to government agencies, banks, and major corporations. The goal was to slow down and disrupt web services in both the U.S. and South Korea.[103] North Korea's cyber capabilities have improved significantly since then, with Pyongyang attacking a diversified range of targets, using various methods. The case studies below cover the range of North Korea's evolving cyber capabilities. While the majority of North Korea's current cyber activity is focused on making – or stealing – money or collecting data for the regime, the technical capabilities that the regime is perfecting could be leveraged in cyber-enabled economic warfare operations.

Since 2011, North Korea's cyber capabilities have moved beyond DDoS attacks. With each subsequent operation, North Korea has demonstrated new ways its hackers can use cyber-enabled tools to not only disrupt and destroy, but also to steal money, steal data, and impose terror on its victims. Increasingly, North Korea has used cyber operations to steal data and engage in intelligence operations. For instance, in 2016, North Korea stole 235 gigabytes of data containing classified wartime contingency plans for the U.S. and South Korean forces.[104]

[98] **98.** United Nations Security Council, "Final report of the Panel of Experts submitted pursuant to resolution 2276 (2016)," February 27, 2017. (http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150)

[99] **99.** James Pearson and Rozanna Latiff, "North Korea spy agency runs arms operation out of Malaysia, U.N. says," *Reuters*, February 26, 2017. (https://uk.reuters.com/article/uk-northkorea-malaysia-arms-insight/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-u-n-says-idUKKBN1650YG)

[100] **100.** Andrea Berger, Cameron Trainer, Shea Cotton, and Catherine Dill, "The Shadow Sector: North Korea's Information Technology Networks," *James Martin Center for Nonproliferation Studies of the Middlebury Institute of International Studies at Monterey*, May 2018, page 6. (https://www.nonproliferation.org/wp-content/uploads/2018/05/op36-the-shadow-sector.pdf)

[101] **101.** James Pearson and Rozanna Latiff, "North Korea spy agency runs arms operation out of Malaysia, U.N. says," *Reuters*, February 26, 2017. (https://uk.reuters.com/article/uk-northkorea-malaysia-arms-insight/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-u-n-says-idUKKBN1650YG)

[102] **102.** Andrea Berger, Cameron Trainer, Shea Cotton, and Catherine Dill, " The Shadow Sector: North Korea's Information Technology Networks," *James Martin Center for Nonproliferation Studies of the Middlebury Institute of International Studies at Monterey*, May 2018, pages 2-3. (https://www.nonproliferation.org/wp-content/uploads/2018/05/op36-the-shadow-sector.pdf)

[103] **103.** Ryan Sherstobitoff, Itai Liba, and James Walter, "Dissecting Operation Troy: Cyberespionage in ROK," *McAfee*, November 28, 2012. (https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/dissecting-operation-troy.pdf)

[104] **104.** Choe Sang-Hun, "North Korean Hackers Stole U.S.-South Korean Military Plans, Lawmaker Says," *The New York Times*, October 10, 2017. (https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html)

The South Korean government suffers an estimated 1.5 million cyber intrusions every day.[105] South Korean police authorities reported between 2014 and 2016 that North Korean cyber operators successfully infiltrated more than 140,000 computers across 160 South Korean private firms and government agencies in order to plant malicious code that is "laying the groundwork for a massive cyber-attack."[106]

These North Korean cyber operations hold dangerous implications for CEEW. As the world conducts its financial and commercial activity through computer-based software and systems, bad actors can exploit this technology. North Korea's hackers could use cyber-enabled means to disrupt or cause lasting damage to the online financial infrastructure that helps modern economies function. Targeting the South Korean, or even American, economy fits into Pyongyang's asymmetric security strategy.

Although it is important to consider the potential threat of CEEW attacks, one cannot be certain the Kim regime has the intent to do so. Pyongyang's primary strategic objective is prolonging the Kim regime's survival, according to the U.S. Department of Defense.[107] Pyongyang thus calibrates its offensive cyber activity to remain in the "gray zone," which U.S. Special Operations Command defines as a realm of "competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality."[108] "Gray zone" operations are also often asymmetric attacks enemy "in venues in which it cannot easily respond in kind," according to Richard Andres of the National Defense University.[109] In response to North Korea's current cyber theft, espionage, and reconnaissance operations, the U.S. and other victim nations often have few options for proportionate retaliation, resulting in a difficult choice between appeasement and escalation.

North Korea may avoid conducting sustained CEEW operations because of its desire to remain within the gray zone. However, this could change with North Korea's perception of its security environment. Tensions have receded for the moment as the result of the Trump-Kim summit and subsequent return to negotiations, yet analyst Victor Cha assesses that a breakdown in the diplomatic process could bring the U.S. and North Korea closer to war since it would leave "no other recourse for diplomacy."[110] The following case studies highlight the North's capabilities and how it could leverage them if tensions rise.

Case Study 1: Economic Attacks – Ten Days of Rain (2011) and DarkSeoul Attack (2013)

In March 2013, North Korean state-sponsored hackers unleashed a major cyber attack, known as DarkSeoul, against three major South Korean banks and three media companies. Hackers used malware to damage thousands of computers and disrupt critical

[105] Kelly Kasulis, "The South Korean government experiences 1.5 million cyberattacks a day, security experts say," *Mic*, November 28, 2017. (https://mic.com/articles/186373/the-south-korean-government-experiences-15-million-cyberattacks-a-day-security-experts-say#.rQzeuVx42)

[106] Jack Kim, "North Korea mounts long-running hack of South Korea computers, says Seoul," *Reuters*, June 12, 2016. (https://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE)

[107] U.S. Department of Defense, Office of the Secretary of Defense, "Military and Security Developments Involving the Democratic People's Republic of Korea – Report to Congress," December 15, 2017. (https://fas.org/irp/world/dprk/dod-2017.pdf)

[108] U.S. Special Operations Command, "White Paper: The Gary Zone," September 9, 2015. (http://www.soc.mil/swcs/ProjectGray/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf)

[109] Richard J. Andres, "Cyber Gray Space Deterrence," *Prism*, December 21, 2017, page 96. (http://cco.ndu.edu/News/Article/1401927/cyber-gray-space-deterrence/)

[110] Victor Cha, "What Will Trump Give Up for Peace with North Korea?" *The New York Times*, March 9, 2018. (https://www.nytimes.com/2018/03/09/opinion/trump-kim-summit-korea.html)

servers.[111] The virus deployed a complex type of wiper malware that irreversibly deleted and wrote over the compromised target's master boot record, considered the "most important data structure" of the computer,[112] rendering the affected computers useless.

The DarkSeoul attacks marked a new phase in North Korea's cyber operations. Not only did the malware's destructive power inflict financial costs estimated at $800 million,[113] it caused major delays and confusion for 10 days in South Korea's financial system.[114] The attack also shut down the three target banks' operations for days.[115] A South Korean task force of military, government, and civilian experts analyzed the codes and supporting network infrastructures to conclude that North Korean government-backed hackers perpetrated the attack.[116]

The DarkSeoul attack is the clearest example of a potential North Korean cyber-enabled economic warfare operation. The 2013 attack not only imposed significant costs to restore banks and media companies' lost computer hardware, but also temporarily undercut South Korea's banking and financial infrastructure. DarkSeoul, however, was not the first time North Korea used cyber-enabled means to disrupt South Korea's banking sector. In 2011, the Ten Days of Rain DDoS campaign took down Nonghyup Bank's nationwide branches, automated devices, and online banking services for 10 days.[117] This incident, however, was part of a broader disruption campaign that not only targeted Nonghyup Bank, but also South Korea's government, military, and private industry.[118]

Both the DarkSeoul cyber attack and earlier 2011 incident was to test the regime's capabilities and tools to someday undermine Seoul's national power. The North Korean cyber operatives' ability to disrupt the South's financial sector suggests Pyongyang could do it again in the future, and perhaps at a larger scale as capabilities improve.

Case Study 2: Cyber Terrorism – Sony Hack (2014)

On November 24, 2014, a hacker group calling themselves the Guardians of Peace broke into the computer systems of Sony Pictures and threatened to release company data if Sony did not cancel the release of an upcoming film, "The Interview," a

[111] Kang Jin-kyu, "Major computer network meltdown," *Korea JoongAng Daily* (South Korea), March 27, 2018. (http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2968916); Nigel Inkster, "Cyber Attacks in La-La Land," *Survival*, February 5, 2015, page 108; Kim Duk-Ki, "The Republic of Korea's Counter Asymmetric Strategy," *Naval War College Review*, Winter 2012, page 67. (https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1447&context=nwc-review); Kyoung Jae Park, Sung Mi Park, and Joshua I. James, "A Case Study of the 2016 Korea Cyber Command Compromise," *Hallym University*, accessed June 25, 2018. (https://arxiv.org/ftp/arxiv/papers/1711/1711.04500.pdf)

[112] For an explanation, see: "Master Boot Record," *Microsoft*, accessed on March 27, 2018. (https://technet.microsoft.com/en-us/library/cc976786.aspx)

[113] Nigel Inkster, "Cyber Attacks in La-La Land," *Survival*, February 5, 2015, page 108; Kim Duk-Ki, "The Republic of Korea's Counter Asymmetric Strategy," *Naval War College Review*, Winter 2012, page 67. (https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1447&context=nwc-review)

[114] Jin-kyu Kang, "Major computer network meltdown," *Korea JoongAng Daily* (South Korea), March 21, 2013. (http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2968916)

[115] Kyoung Jae Park, Sung Mi Park, and Joshua I. James, "A Case Study of the 2016 Korea Cyber Command Compromise," *Hallym University*, accessed June 25, 2018. (https://arxiv.org/ftp/arxiv/papers/1711/1711.04500.pdf)

[116] "Evidence in Hacker Attack Points to North Korea," *Chosun Ilbo* (South Korea), April 11, 2013. (http://english.chosun.com/site/data/html_dir/2013/04/11/2013041100648.html)

[117] Chico Harlan and Ellen Nakashima, "Suspected North Korean cyber attack on a bank raises fears for S. Korea, allies," *The Washington Post*, August 29, 2011. (https://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html?utm_term=.9d1c2d350cde)

[118] "Ten Days of Rain," *McAfee*, July 2011. (https://securingtomorrow.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf)

comedy depicting a farcical plot to assassinate Kim Jong Un. The hackers also threatened 9/11-style terror attacks on theaters that screened the film.[119] Although Sony Pictures canceled the film's theatrical release, the hackers still released the data and used malware to destroy approximately 70 percent of Sony Pictures' computers.[120]

The wiper malware and phishing campaigns in this operation had similar characteristics to the ones the DarkSeoul hackers employed. In the Sony attack, hackers gained access through both phishing emails and software vulnerabilities on the company's website to access backend databases housing IT blueprints and employee private information.[121] Hackers then used wiper malware called Destover to erase the data.

The FBI attributed the attacks to Pyongyang. Technical analysis revealed links to other malware attributed to the North Korean government. North Korean-related IP addresses were in communication with the IP addresses hard coded into the data deletion malware, thereby revealing a significant overlap in the cyber infrastructure between the Sony attack and other malicious activity linked to the North Korean government. The attack also shared structural and tactical similarities with the DarkSeoul attacks.[122]

The stated objective of the Sony hackers was to prevent the release of the disputed film because it harmed Kim Jong Un's public image.[123] Only a month earlier, in October 2014, North Korean cyber operatives targeted British film production firm Mammoth Screen, which was set to produce a new television drama involving a British nuclear scientist taken hostage in North Korea. North Korea cyber operatives infiltrated Mammoth Screen but did not deploy destructive malware. Despite this, BBC reporting suggested that "the presence of North Korean hackers on the system caused widespread alarm over what they might do." This prompted the firm to delay the release of the series, which it eventually scrapped due to complications in funding.[124] In both cases, Pyongyang targeted a noncombatant and nongovernment entity and used threats to compel them to take specific actions. *The Washington Post* reported that anonymous analysts assessed that the Sony Pictures attack set a "worrying new precedent for cyberterrorism."[125] The reason analysts classified the Sony hack as cyber terror was because the attackers threatened both the company employees and theatergoers.[126] The political intent of the coercive action, i.e. protecting the perceived legitimacy of Kim Jong Un, is also consistent with terrorism.

[119] Andrea Peterson, "Sony Pictures hackers invoke 9/11 threatening theaters that show, "The Interview," *The Washington Post*, December 16, 2014. (https://www.washingtonpost.com/news/the-switch/wp/2014/12/16/sony-pictures-hackers-invoke-911-while-threatening-theaters-that-show-the-interview/?utm_term=.a4f035960921)

[120] David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More." *The New York Times*, October 15, 2017. (https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news)

[121] Kim Zetter, "Sony Got Hacked Hard: What We Know and Don't Know So Far," *Wired*, December 3, 2014. (https://www.wired.com/2014/12/sony-hack-what-we-know/)

[122] U.S. Federal Bureau of Investigation, Press Release, "Update on Sony Investigation," December 19, 2014. (https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation)

[123] Andrew Griffin, "Sony Hack: Who are the Guardians of Peace, and is North Korea Really Behind the Attack?" *The Independent* (UK), December 17, 2014. (https://www.independent.co.uk/life-style/gadgets-and-tech/news/sony-hack-who-are-the-guardians-of-peace-and-is-north-korea-really-behind-the-attack-9931282.html)

[124] Gordon Corera, "UK TV drama about North Korea hit by cyber-attack," *BBC* (UK), October 16, 2017. (http://www.bbc.com/news/technology-41640976)

[125] Ellen Nakashima, "White House says Sony hack is a serious national security matter," *The Washington Post*, July 9, 2014. (https://www.washingtonpost.com/world/national-security/white-house-says-sony-hack-is-a-serious-national-security-matter/2014/12/18/01eb8324-86ea-11e4-b9b7-b8632ae73d25_story.html?utm_term=.5f119358a7f9)

[126] David Auerbach, "The Sony Hackers are Terrorists," *Slate*, December 17, 2014. (http://www.slate.com/articles/technology/bitwise/2014/12/sony_pictures_hack_why_its_perpetrators_should_be_called_cyberterrorists.html)

Were North Korea to unleash a similar attack on U.S. or South Korean infrastructure, there would be significant national security implications. North Korea has already used spear-phishing campaigns against U.S. electric power companies as part of "early-stage reconnaissance," according to experts at FireEye,[127] and in November 2017, the U.S. Department of Homeland Security and FBI issued a joint technical alert warning that North Korean cyber actors were targeting aerospace, telecommunications, and finance industries.[128] Some of the malware North Korea used in the Sony attack provided backdoor access to compromised systems, while other malware served as a remote access tool that could execute multiple commands the hacker can issue from a central command-and-control server.[129] These capabilities would likely play a key role in any attack on critical infrastructure.

Case Study 3: Extortion – Korea Hydro and Nuclear Power (2015)

In 2015, the South Korean government revealed that civil nuclear company Korea Hydro and Nuclear Power (KHNP) had suffered a cyber attack the prior December. This attack bore the traits of a North Korean operation, specifically the Sony Pictures hack. It is unclear why the South Korean government did not formally attribute the attack to anyone.[130] Cyber operatives infiltrated the company's networks through spear-phishing emails that targeted 3,571 employees. The hackers then released the personal information of 10,799 employees.[131] The hackers also posted a ransom notice on Twitter claiming they stole proprietary information regarding South Korea's nuclear reactors and then posted the stolen documents online.[132] The hackers threatened to sell this information to "many countries from Northern Europe, Southeast Asia, and South America."[133] Finally, the hackers threatened to cause physical destruction to the KHNP facilities unless the company shut down three of its 23 nuclear reactors. It is unclear what the hackers' motives were for demanding the shutdown, but they presented themselves as anti-nuclear activists. Demanding the shutdown reinforced the credibility of their self-presentation as activists and prevented the ROK from attributing the attack to the North Korean government.[134]

Given the conflicting demands for ransom payments and a reactor shutdown, it is unclear whether the goal was merely to extort money or to pursue CEEW. In

[127] "North Korean Actors Spear Phish U.S. Electric Companies," *FireEye*, October 10, 2017. (https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html)

[128] U.S. Computer Emergency Readiness Team, "Alert (TA17-318A): Hidden Cobra – North Korean Remote Administration Tool: FALLCHILL," November 22, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-318A); see also: U.S. Computer Emergency Readiness Team, "Alert (TA17-318B): HIDDEN COBRA – North Korean Trojan: Volgmer," November 14, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-318B); U.S. Computer Emergency Readiness Team, "Alert (TA17-318A): HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL," November 14, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-318A)

[129] U.S. Computer Emergency Readiness Team, "Alert (TA17-318A): HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL," November 14, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-318A); U.S. Computer Emergency Readiness Team, "Alert (TA17-318B): HIDDEN COBRA – North Korean Trojan: Volgmer," November 14, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-318B)

[130] Kevin Stahler and Stephan Haggard, "More Cyber: The Korea Hydro and Nuclear Power Company (KHNP) Hacks," *Peterson Institute for International Economics*, February 13, 2015. (https://piie.com/blogs/north-korea-witness-transformation/more-cyber-korea-hydro-and-nuclear-power-company-khnp-hacks)

[131] Sean Gallagher, "South Korea claims North hacked nuclear data," *ARS Technica*, March 17, 2015. (https://arstechnica.com/information-technology/2015/03/south-korea-claims-north-hacked-nuclear-data/)

[132] Kyoung Jae Park, Sung Mi Park, and Joshua I. James, "A Case Study of the 2016 Korea Cyber Command Compromise," *Hallym University*, accessed June 25, 2018. (https://arxiv.org/ftp/arxiv/papers/1711/1711.04500.pdf)

[133] "(LEAD) Hacker demands money for information on S. Korean nuclear reactors," *Yonhap News Agency* (South Korea), March 12, 2015. (http://english.yonhapnews.co.kr/national/2015/03/12/40/0302000000AEN20150312008051320F.html)

[134] Justin McCurry, "South Korean nuclear operator hacked amid cyber-attack fears," *The Guardian* (UK), December 23, 2014. (https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack)

their ransom note, the hackers warned that South Korea's government risked undermining its efforts to export nuclear reactors if it did not meet their demands. This incident revealed South Korea's civil nuclear plants and energy sector are vulnerable to cyber attacks. Furthermore, undermining a key economic sector of the South Korean economy would not only weaken the economic output of the nation, but also threaten broader national interests.

Case Study 4: Cyber-enabled Theft – SWIFT and Cryptocurrency Exchanges (2016-2017)

Cyber security firms have attributed 18 separate cyber attacks in countries such as Costa Rica, Ethiopia, Gabon, India, Indonesia, Iraq, Kenya, Malaysia, Nigeria, Poland, and several others to the North Korean hackers known as the Lazarus Group. The most notable attack occurred on February 4, 2016, when the group stole $81 million from Bangladesh's central bank. The hackers infiltrated the bank's network, stole its credentials for the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a financial messaging service, and issued requests through the Federal Reserve of New York to transfer funds from the Bangladeshi bank to accounts the hackers controlled.[135] In October 2017, BAE Systems reported a similar attack on Taiwan's Far Eastern International Bank after hackers gained access to the bank's SWIFT credentials.[136] BAE Systems' report suggested this attack was part of a wider campaign that also included a Vietnamese commercial bank. BAE noted the malware in its system had similarities to the malware characteristics used in the Sony Pictures hack.

The SWIFT global message platform connects more than 11,000 banking, finance, and corporate customers. Any disruption to this service could yield severe economic and political effects.[137] Although the Kim family regime appears to prioritize currency generation in its objectives, these attacks using the SWIFT system raise concerns that North Korean hackers may become more proficient at manipulating the data and systems that undergird the global financial system. While a large enough attack on a major bank might have global repercussions, attacks on the SWIFT network would shake the core of the system.

The explosion of the cryptocurrency market is also providing a new attack vector. Cyber security firms report that North Korea's cryptocurrency-generating operations include both hacking exchanges and mining currencies.[138] In September 2017, FireEye linked North Korea to a series of attacks on three ROK cryptocurrency exchange firms between April and July 2017. North Korean hackers used spear-phishing emails and their malware was similar to a virus used in prior North Korean cyber attacks on global banks in 2016.[139] In December 2017, North Korean hackers attacked the Youbit currency

[135] Jose Pagliery, "North Korea-linked hackers are attacking banks worldwide," *CNN*, April 4, 2017. (https://www.cnn.com/2017/04/03/world/north-korea-hackers-banks/index.html); Kevin Poulsen, "Are Cyber Crooks Funding North Korea's nukes?" *The Daily Beast*, May 8, 2017. (https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html); Syed Zain Al-Mahmood, "How Bangladesh's Central Bank Found $100 Million Missing After a Weekend Break," *The Wall Street Journal*, March 11, 2016. (https://blogs.wsj.com/indiarealtime/2016/03/11/how-bangladeshs-central-bank-found-100-million-missing-after-a-weekend-break/)

[136] Sergei Shevchenko, Hirman Muhammad bin Abu Bakar, and James Wong, "Taiwan Heist: Lazarus Tools and Ransomware," *BAE Systems*, October 16, 2017. (http://baesystemsai.blogspot.co.uk/2017/10/taiwan-heist-lazarus-tools.html)

[137] Lee Bell, "Cyber crooks are using SWIFT to launch new sophisticated attacks, security researchers warn," *IT Pro* (UK), February 22, 2018. (http://www.itpro.co.uk/security/30598/cyber-crooks-are-using-swift-to-launch-new-sophisticated-attacks-security-researchers)

[138] Juan Andres Guerrero-Saade and Priscilla Moriuchi, "North Korea targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign," *Recorded Future*, January 16, 2018. (https://www.recordedfuture.com/north-korea-cryptocurrency-campaign/); Ryan Sherstobitoff, "Lazarus Resurfaces, Targets Global Banks and Bitcoin Users," *McAfee*, February 12, 2018. (https://securingtomorrow.mcafee.com/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/)

[139] Luke McNamara, "Why is North Korea So Interested in Bitcoin?" *FireEye*, September 11, 2017. (https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html)

exchange and stole 17 percent of the exchange's total digital assets, which had a value of 7.6 billion Korean won or $7 million.[140] As a result of the attack, Youbit declared bankruptcy.

> **"North Korea has reportedly generated up to 11,000 bitcoins, or $120 million, from its attacks on cryptocurrency exchanges and currency mining. This could have significant residual effects on South Korea's financial infrastructure."**

North Korea has reportedly generated up to 11,000 bitcoins, or $120 million, from its attacks on cryptocurrency exchanges and currency mining.[141] This could have significant residual effects on South Korea's financial infrastructure. In December 2017, South Korea was ranked the world's third largest market for Bitcoin trading after Japan and the United States. Major South Korean corporations, including Nexon and Samsung, are reportedly investing in virtual currency businesses and supporting technologies.[142] As these businesses become more intertwined with South Korea's formal financial system, attacks on cryptocurrencies could target the stability of Seoul's banking system.

Case Study 5: Cyber-enabled Theft – WannaCry (2017)

Between February and May 2017, the WannaCry ransomware wreaked havoc worldwide. WannaCry infected more than 230,000 computers, including the National Health Service in the United Kingdom. Once this virus compromised a computer, it would find and encrypt 176 different file types, demanding a $300 payment in bitcoin to decrypt the locked files.[143] Prior to May, the effects were more limited because the virus relied on "stolen credentials to move through infected networks, while the May 12 version included the ability to self-propagate," according to experts at cyber security firm Symantec.[144] The final iteration of the virus was able to propagate itself across thousands of computers by leveraging a software vulnerability, known as the Eternal Blue exploit, allegedly stolen from the U.S. National Security Agency and publicly revealed in April 2017 by a Russian-linked hacker group called Shadow Brokers.[145]

Shadow Brokers released the Eternal Blue vulnerability into cyber space for use by any hacker, but the fact that North Korea quickly incorporated the exploit into its active operations suggests that North Korea is active on the malware black market. Although there is no documentation of North Korea facilitating cooperation between state-sponsored and private hackers, Pyongyang's track record of cooperation with organized crime[146] and

[140] **140.** "North Korean hackers behind attacks on cryptocurrency exchanges, South Korean newspaper reports," *Reuters*, December 15, 2017. (https://www.reuters.com/article/us-northkorea-southkorea-cryptocurrency/north-korean-hackers-behind-attacks-on-cryptocurrency-exchanges-south-korean-newspaper-reports-idUSKBN1EA02F)

[141] **141.** "NK estimated to have made up to U.S.$210 mln with bitcoin: report," *Yonhap News Agency* (South Korea), March 2, 2018. (http://english.yonhapnews.co.kr/northkorea/2018/03/02/28/0401000000AEN20180302005600315F.html)

[142] **142.** Yoochul Kim, "Behind South Korea's Cryptocurrency Boom," *MIT Technology Review*, December 7, 2017. (https://www.technologyreview.com/s/609561/behind-south-koreas-cryptocurrency-boom/)

[143] **143.** "What you need to know about the WannaCry Ransomware," *Symantec*, May 23, 2017. (https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack); "Attackers target dozens of global banks with new malware," *Symantec*, February 12, 2017. (https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0)

[144] **144.** Jeff Greene, "Empty Threat or Serious Danger? Assessing North Korea's Risk to the Homeland," *Testimony before the U.S. House Homeland Security Committee's Subcommittee on Oversight and Management Efficiency*, October 12, 2017, page 3. (http://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-GreeneJ-20171012.pdf)

[145] **145.** Scott Shane, "Malware Case is major Blow for the N.S.A.," *The New York Times*, May 16, 2017. (https://www.nytimes.com/2017/05/16/us/nsa-malware-case-shadow-brokers.html)

[146] **146.** Sheena Chestnut-Greitens, *Illicit: North Korea's evolving operations to earn Hard Currency* (The Committee for Human Rights in North Korea, 2014). (https://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf)

rogue states raises concerns that North Koreans could expand these efforts in cyber space.[147]

> **"Shadow Brokers released the Eternal Blue vulnerability into cyber space for use by any hacker, but the fact that North Korea quickly incorporated the exploit into its active operations suggests that North Korea is active on the malware black market."**

The North Korean government emerged as a likely suspect when Symantec found remnants of code linked to the Lazarus Group on computers infected with WannaCry, including malware used in the Sony hack.[148] In December 2017, the U.S. government publicly attributed the WannaCry attack to North Korean state-sponsored actors.[149]

Ultimately, even as the virus infected computers in more than 150 countries,[150] the hackers generated little income because a flaw in the code prevented them from collecting bitcoin payments.[151] Still, the attack cost the affected companies billions of dollars.[152] And as costly as the attack was, it could have been far worse if North Korea had paired the worm with wiper viruses, instead of malware, and aimed directly at U.S. and allied critical infrastructure. Microsoft also minimized the damaged when it issued a patch to address the Eternal Blue vulnerability two months prior to the attack.[153]

Case Study 6: Reconnaissance – Reaper and Operation GhostSecret (2018)

In February 2018, FireEye revealed the existence of an extended reconnaissance operation dubbed Advanced Persistent Threat 37, or Reaper, which engaged in covert intelligence gathering in support of a range of North Korean state interests.[154] In April 2018, McAfee exposed a North Korean global data reconnaissance operation targeting a broad range of industries in critical infrastructure, entertainment, finance, health care, and telecommunications. This extended campaign, dubbed Operation GhostSecret, began in mid-February 2018. The operation deployed several malware implants derived from prior North Korean attacks.[155] According to McAfee, the operation stole data from affected

[147] **147.** Bruce E. Bechtol, "North Korea's Illegal Weapons Trade: The Proliferation Threat From Pyongyang," *Foreign Affairs*, June 6, 2018. (https://www.foreignaffairs.com/articles/north-korea/2018-06-06/north-koreas-illegal-weapons-trade)

[148] **148.** Jeff Greene, "Empty Threat or Serious Danger? Assessing North Korea's Risk to the Homeland," *Testimony before the U.S. House Homeland Security Committee's Subcommittee on Oversight and Management Efficiency*, October 12, 2017. (http://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-GreeneJ-20171012.pdf)

[149] **149.** The White House, "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," December 19, 2017. (https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/)

[150] **150.** U.S. Computer Emergency Readiness Team, "Alert (TA17-132A): Indicators Associated with WannaCry Ransomware," May 19, 2017. (https://www.us-cert.gov/ncas/alerts/TA17-132A)

[151] **151.** Jeff Greene, "Empty Threat or Serious Danger? Assessing North Korea's Risk to the Homeland," *Testimony before the U.S. House Homeland Security Committee's Subcommittee on Oversight and Management Efficiency*, October 12, 2017. (http://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-GreeneJ-20171012.pdf)

[152] **152.** Thomas P. Bossert, "It's Official: North Korea is behind WannaCry," *The Wall Street Journal*, December 18, 2017. (https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537)

[153] **153.** "2018 Government Cybersecurity Report," *SecurityScorecard*, 2018. (https://explore.securityscorecard.com/rs/797-BFK-857/images/2018%20Government%20Cybersecurity%20Report.pdf)

[154] **154.** "APT 37 (Reaper): The Overlooked North Korean Actor," *FireEye*, February 20, 2018. (https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf)

[155] **155.** Ryan Sherstobitoff and Asheer Malhotra, "Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide," *McAfee*, April 24, 2018. (https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/)

systems, and the attackers designed their code to evade detection and "deceive forensic investigators."[156]

The operation reportedly began with a campaign known as Bankshot against the Turkish financial system, which bore similarities to North Korea's attacks on SWIFT.[157] Within two weeks, the operation had compromised telecommunications, health, finance, critical infrastructure, and entertainment companies across 17 different countries.[158]

GhostSecret was notable because of the extensive command structure that supported the malware implants. McAfee called the infrastructure "an extensive framework for data reconnaissance and exfiltration." The command and control infrastructure not only supported the data exfiltration but also had arbitrary command execution capabilities on a victim's system.[159]

North Korea's ongoing cyber reconnaissance operations, such as APT 37 Reaper and Operation GhostSecret, enable hackers to pre-position exploits and gain insights into the battlefield and into the vulnerabilities of the U.S. and its allies. These operations also enable the Kim family regime to develop contingency plans for direct conflict with its adversaries. Indeed, North Korea may now be scouting the battlefield in case diplomatic efforts reach the end of the road.

Policy Recommendations

China and Russia have conducted (and are conducting on an ongoing basis) a range of cyber operations against the United States – from information operations to cyber-enabled economic warfare. North Korea is no doubt taking notes. The North Korean regime is a "learning organization." It observes best practices and incorporates them into its arsenal.[160] Therefore, Washington's responses to combat, counter, thwart, and deter other malicious cyber actors will likely have an impact on North Korea's capabilities and strategies. For that reason, policymakers must adopt optimal cyber defense measures in addition to heeding recommendations specific to the threat from North Korea.

Enhancing U.S. cyber resilience and working cooperatively with the private sector are central to any effective cyber defense strategy. For example, the U.S. Computer Emergency and Readiness Team (US-CERT) issues technical alerts that inform critical infrastructure, financial, and aerospace companies how to address software vulnerabilities.[161] Ensuring that American businesses incorporate US-CERT technical recommendations may be one way to turn information sharing into effective resilience.

[156] **156.** Raj Samani, "Global Malware Campaign Pilfers Data from Critical Infrastructure, Entertainment, Finance, Health Care, and Other Industries," *McAfee*, April 24, 2018. (https://securingtomorrow.mcafee.com/mcafee-labs/global-malware-campaign-pilfers-data-from-critical-infrastructure-entertainment-finance-health-care-and-other-industries); Ryan Sherstobitoff, "Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant," *McAfee*, March 8, 2018. (https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/)

[157] **157.** Ryan Sherstobitoff, "Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant," *McAfee*, March 8, 2018. (https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/)

[158] **158.** Raj Samani, "Global Malware Campaign Pilfers Data from Critical Infrastructure, Entertainment, Finance, Health Care, and Other Industries," *McAfee*, April 24, 2018. (https://securingtomorrow.mcafee.com/mcafee-labs/global-malware-campaign-pilfers-data-from-critical-infrastructure-entertainment-finance-health-care-and-other-industries/)

[159] **159.** Ryan Sherstobitoff and Asheer Malhotra, "Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide," *McAfee*, April 24, 2018. (https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/)

[160] **160.** Peter Senge, *The Fifth Discipline: The Art & Practice of The Learning Organization* (New York: Double Day Business, 1990). "A learning organization is continually expanding its capacity to create its future. For such an organization, it is not enough merely to survive. 'Survival learning' is important but for a learning it must be joined by 'generative learning' learning that enhances our capacity to create." Although this is referring to businesses, it is an apt description for military and government organizations and even regimes such as North Korea.

[161] **161.** Frank J. Cilluffo, "Empty Threat or Serious Danger? Assessing North Korea's Risk to the Homeland," *Testimony before the U.S. House Homeland Security Committee's Subcommittee on Oversight and Management Efficiency*, October 12, 2017, page 4. (http://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-CilluffoF-20171012.pdf)

U.S. Computer Emergency Readiness Team (U.S.-CERT) Alerts and Reports on North Korea Malware[162]

TYPE AND TITLE	DATE	OBJECTIVE
Alert (TA17-132A) – Indicators Associated with WannaCry Ransomware	May 12, 2017	Provided a comprehensive overview of the vulnerabilities that WannaCry Ransomware exploits and recommended steps for prevention/protection
Alert (TA17-164A) –HIDDEN COBRA: North Korea's DDoS Botnet Infrastructure	June 13, 2017	Provided technical details on the infrastructure and cyber tools for North Korean government-sponsored hackers targeting media, aerospace, financial, and critical infrastructure sectors in U.S. and abroad
Malware Analysis Report (MAR-10132963) – Analysis of Delta Charlie Attack Malware	August 23, 2017	Provided file samples of the Delta Charlie Attack Malware to create defense systems for vulnerable devices and networks
Alert (TA17-318B) – HIDDEN COBRA– North Korean Trojan: VOLGMER	November 14, 2017	Provided information regarding capabilities, infrastructure, and response methods to the Volgmer malware that targets the government, financial, automotive, and media industries
Alert (TA17-318A) Hidden Cobra – North Korean Trojan: FALLCHILL	November 14, 2017	Provided information regarding capabilities, infrastructure, and response methods to the Fallchill malware that targets the aerospace, telecommunications and financial industries
Malware Analysis Report (MAR-10135536) – North Korean Trojan: BANKSHOT	December 21, 2017	Provided analysis and samples of seven malicious executable files related to the Bankshot malware
Malware Analysis Report (MAR-10135536-G) – North Korean Trojan: BADCALL	February 13, 2018	Provided analysis and samples of three malicious files related to the Badcall malware

[162] U.S. Computer Emergency Readiness Team, "HIDDEN COBRA - North Korean Malicious Cyber Activity," accessed September 21, 2018. (https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity)

U.S. Computer Emergency Readiness Team (U.S.-CERT) Alerts and Reports on North Korea Malware

TYPE AND TITLE	DATE	OBJECTIVE
Malware Analysis Report (MAR-10135536-F) – North Korean Trojan: HARDRAIN	February 13, 2018	Provided analysis and samples of three malicious files related to the Hardrain malware
Malware Analysis Report (MAR-10135536.11) – North Korean Trojan: SHARPKNOT	March 28, 2018	Provided analysis and a sample of a 32-bit Windows executable file related to the Sharpknot malware
Malware Analysis Report (MAR-10135536-3) – HIDDEN COBRA RAT/Worm	May 29, 2018	Provided analysis of four unique files, including an installer and additional malware that served as a Remote Access Trojan (RAT) and a malicious Dynamic Link Library (DLL) that served as a Server Message Block (SMB) worm that was on behalf of the North Korean government
Alert (TA18-149A) Hidden Cobra – Joanap Backdoor Trojan and Brambul Server Message Block Worm	May 29, 2018	Shared information on the IP addresses and indicators of compromise (IOCs) associated with the Joanap Remote Access Trojan (RAT) and a Server Message Block (SMB) worm Brambul, both of which targeted the media, aerospace, financial, and critical infrastructure sectors
Malware Analysis Report (10135536-12) – North Korean Trojan: TYPE FRAME	June 14, 2018	Provided analysis and samples of 11 malware related to the TYPEFRAME malware
Malware Analysis Report (10135536-17) – North Korean Trojan: KEYMARBLE	August 9, 2018	Provided analysis and a sample of the Remote Access Trojan malware variant named Keymarble in the form of a 32-bit Windows executable file

Additionally, the U.S. military must be able to continue operating during cyber attacks. The development and public demonstration of resilient capabilities may reduce the adversary's likelihood of conducting an attack if it knows the chances of success are lower. For example, capabilities already exist to protect the operations of financial markets during anomalies in market activity, as well as in a crisis. Future cyber attacks will no doubt test these capabilities.

Further, the United States needs to enhance societal resilience in the face of cyber attacks. The U.S. government should therefore explore education and training programs similar to the Cold War civil defense programs that entailed preparing for a nuclear attack. A 21st century cyber civil defense program would mitigate and reduce the risks of cyber attacks against critical infrastructure. For example, what should Americans do if they lose access to their bank accounts in a widespread cyber attack? A civil defense program could minimize public panic and potentially speed recovery.

In addition to such general measures, the U.S. government should consider the following recommendations aimed at addressing the specific cyber threats from North Korea.

Create a combined ROK-U.S. Cyber Task Force

Since the ROK and U.S. are the primary targets for North Korean cyber activities, the alliance should establish a task force of ROK and U.S. cyber experts to synchronize defenses and options for offensive operations. Although joint task forces are often ineffective, a combined entity should be pursued to ensure the alliance could adequately defend against the full range of North Korea's cyber threats, from CEEW to wartime cyber operations.

On June 21, the 5th U.S.-Republic of Korea Bilateral Cyber Consultations were held in Seoul "to discuss a wide range of cyber issues, including cooperation on deterring cyber adversaries, cybersecurity of critical infrastructure, capacity building, information sharing, military-to-military cyber cooperation, cybercrime, international security issues in cyberspace, and current threats and trends in the international cyber environment."[163] An agenda item for the next consultative meeting and for the ROK/U.S. security consultative meeting in fall 2018 should be the establishment of a permanent combined ROK/U.S. cyber task force to supplement periodic consultation. A permanent task force is necessary to defend economic infrastructure and address the full range of cyber threats, including CEEW.

The Cyber Task Force should develop a combined strategy for operations during both armistice and wartime. It should consist of military and civilian experts from across the U.S. and ROK governments and include private sector experts as well. This would not contradict the indefinite suspension of combined military exercises following the Singapore summit. In fact, given that North Korea is likely to continue or escalate aggressive cyber operations during nuclear negotiations, the task force's mission is only more urgent.

The new task force should include enhanced information sharing. For instance, South Korea's Korea Internet Safety Agency successfully prevented a spear-phishing campaign targeting 10 cryptocurrency exchanges earlier in 2017.[164] Sharing insights from such experiences will be instrumental in fortifying cyber defenses.

The United States National Cyber Strategy calls for developing international partner capacity to support a new cyber deterrence initiative. A Combined ROK-U.S.

[163] U.S. Department of State, "The 5th U.S.-Republic of Korea Bilateral Cyber Consultations," June 21, 2018. (https://www.state.gov/r/pa/prs/ps/2018/06/283418.htm)

[164] "North Korean hackers behind attacks on cryptocurrency exchanges, South Korean newspaper reports," *Reuters*, December 15, 2017. (https://www.reuters.com/article/us-northkorea-southkorea-cryptocurrency/north-korean-hackers-behind-attacks-on-cryptocurrency-exchanges-south-korean-newspaper-reports-idUSKBN1EA02F)

Task Force would be one example of operationalizing the strategy.[165]

Disable the Reconnaissance General Bureau (RGB)'s network of front companies

Sanctions have been an underutilized tool to respond to North Korea's cyber operations. Section 209 of the North Korea Sanctions and Policy Enhancement Act (NKSPEA) requires the president to sanction individuals and companies affiliated with North Korea's malicious cyber activity.[166] In September 2018, the Treasury and Justice Departments took a major step forward by sanctioning and pressing charges against a North Korean computer programmer, Park Jin Hyok, who had a role in the Sony Pictures hack, the SWIFT Bangladesh Bank theft operation, and WannaCry.[167] Prior to this, the Treasury Department had acted only once. That was in January 2015 when Treasury sanctioned the RGB, two North Korean companies, and 10 North Korean government officials under Executive Order 13687 in response to the Sony Pictures cyber attack.

The U.S. government could do more to build on this momentum and impose the necessary financial pressure to curb North Korean cyber operations.[168] The RGB and its funding sources for its cyber operations remain largely untouched. The RGB continues to operate front companies around the world.[169] For example, the RGB-affiliated Glocom sells battlefield radio equipment in Malaysia in breach of UN sanctions. The company operates from within the Pyongyang branch of Pan Systems, a Singaporean company.[170] The United Nations Panel of Experts determined that the company is engaged in "patterns of evasion" using multiple overseas accounts and trusted local partners to move funds as part of North Korea's illicit trade in "prohibited military communications technology."[171] The report identified the third parties and intermediaries that Glocom used as part of its schemes. The March 2018 report recommended the Security Council sanction the companies and individuals participating in Glocom's illicit activities, including Pan Systems, International Global System, and International Golden Service.[172]

[165] "BUILD A CYBER DETERRENCE INITIATIVE: The imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states. The United States will launch an international Cyber Deterrence Initiative to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior. The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors." The White House, "National Cyber Strategy of the United States," September 2018. (https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf)

[166] Mathew Ha and Trevor Logan, "Trump must still hold North Korea accountable for cyberattacks," *The Hill*, June 14, 2018. (http://thehill.com/opinion/national-security/392255-trump-must-still-hold-north-korea-accountable-for-continuing-cyber); North Korea Sanctions and Policy Enhancement Act of 2016, Pub. L. 114-122, 130 Stat. 93, codified as amended at 114 U.S.C. (https://www.congress.gov/bill/114th-congress/house-bill/757/text)

[167] U.S. Department of the Treasury, Press Releases, "Treasury Targets North Korea for Multiple Cyber-Attacks," September 6, 2018. (https://home.treasury.gov/news/press-releases/sm473)

[168] Mathew Ha, "U.S. Presses Criminal Charges and Sanctions against North Korean Cyber Operative," *Foundation for Defense of Democracies*, September 7, 2018. (http://www.defenddemocracy.org/media-hit/mathew-ha-us-presses-criminal-charges-and-sanctions-against-north-korean-cyber-oper/)

[169] U.S. Department of the Treasury, Press Release, "Treasury Imposes Sanctions Against the Government of The Democratic People's Republic Of Korea," January 2, 2015. (https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx)

[170] James Pearson and Rozanna Latiff, "North Korea spy agency runs arms operation out of Malaysia, U.N. says," *Reuters*, February 26, 2017. (https://uk.reuters.com/article/uk-northkorea-malaysia-arms-insight/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-u-n-says-idUKKBN1650YG)

[171] United Nations Security Council, "Report of the Panel of Experts established pursuant to resolution 1847 (2009)," March 5, 2018, page 64. (http://www.un.org/ga/search/view_doc.asp?symbol=S/2018/171)

[172] Ibid, page 77.

While Glocom is not directly involved in North Korea's malicious cyber activities, it generates support for the RGB, as well as the full range of Pyongyang's malign conduct. Sanctioning Glocom could therefore sever one of the RGB's financial lifelines. The U.S. government should investigate all companies named in the UN Panel of Expert report with the goal of adding all of these entities to U.S. sanctions lists, pending confirmation of the report's allegations.

> **"Washington should be more proactive in its engagement with foreign governments that host companies such as Glocom, Pan Systems, International Global System, and International Golden Service. If governments fail to investigate and act against RGB front companies, Washington should consider punitive measures such as secondary sanctions."**

Additionally, Washington should be more proactive in its engagement with foreign governments that host companies such as Glocom, Pan Systems, International Global System, and International Golden Service. If governments fail to investigate and act against RGB front companies, Washington should consider punitive measures such as secondary sanctions.

Pursue preparations for offensive measures to restrict Pyongyang's cyber capacity

The U.S. and its allies must develop options to conduct offensive cyber measures to overwhelm and disrupt North Korea's network infrastructure. Although classified plans are likely under development within specific government organizations, the use of offensive cyber capabilities remains a topic of debate and controversy. Given the threat posed by North Korea and the damage it can do to the U.S. and its allies, serious consideration must be given to offensive use of cyber capabilities to deter and defeat North Korean cyber operations. While pre-emptive use of offensive capabilities may be a dangerous provocation, such capabilities cannot be created after a cyber attack occurs and an immediate response is required.

Pressure foreign countries to dismantle North Korean networks in their jurisdictions

That the majority of North Korea's cyber attacks originate outside the country constitutes a significant operational weakness.[173] The U.S. and its allies should increase diplomatic engagement with foreign nations to monitor and restrict the activities of North Korean personnel on their soil or to expel those that are involved in malicious cyber activities. The U.S. should also encourage these nations to stop suspected North Korean operatives from attending certain universities or working in specific research institutes which might provide the training North Korea's hackers need.

If the foreign governments do not take steps to address malicious North Korean cyber operations emanating from their jurisdiction, the U.S. should be prepared to impose sanctions and other penalties on North Korea's cyber enablers to show that complicity has consequences.[174] Section 209 of the North Korea Sanctions Policy and Enhancement Act (NKSPEA) requires the president to submit a comprehensive report that not only describes the North Korean cyber security threat, but also "the identity and nationality of persons that have knowingly engaged in, directed, or provided material support to conduct significant activities undermining cybersecurity." Additionally, the legislation requires this presidential report to Congress to include a U.S. strategy that addresses how to "engage

173. "North Korea's Ruling Elite Are Not Isolated," *Recorded Future*, July 25, 2017. (https://www.recordedfuture.com/north-korea-internet-activity/)

174. Anthony Ruggiero, "Evaluating Sanctions Enforcement and Policy Options on North Korea," *Testimony for the Senate Committee on Banking, Housing, and Urban Affairs*, September 7, 2017. (http://www.defenddemocracy.org/content/uploads/documents/09-07-17_AR_Senate_Banking_Testimony-1.pdf) foreign governments to halt the capability of the Government of North Korea and persons acting for or on behalf of that Government."[175]

Both the executive and legislative branches should work together to ensure the White House issues this report every 180 days. This would not only fulfill NKSPEA's requirements, but also ensure the gathering of crucial information that could put pressure on foreign governments that are enabling North Korean cyber activity. While NKSPEA authorizes the president to impose unilateral sanctions on those individuals and entities highlighted in the 180-day report, Washington should first warn these individuals and/or governments to cease and desist. If the cyber activity continues, Washington should then resort to imposing punitive sanctions.

> **"Section 209 of the North Korea Sanctions Policy and Enhancement Act (NKSPEA) requires the president to submit a comprehensive report that not only describes the North Korean cyber security threat, but also 'the identity and nationality of persons that have knowingly engaged in, directed, or provided material support to conduct significant activities undermining cybersecurity.'"**

Currently, China is the only country that has verifiably hosted North Korean hacker teams and supported network infrastructure. The Department of Justice revealed that North Korean cyber operatives, such as the charged and sanctioned programmer Park Jin Hyok, operated from China.[176] Although Beijing could deny any direct involvement in North Korea's offensive cyber operations, China's tacit consent enabling the presence of North Korean cyber operatives warrants action.

Beyond China, analysis of data transfers coming from nations such as India, New Zealand, Malaysia, Thailand, and others suggest a North Korean presence. However, it is difficult to confirm whether these nations knowingly host North Korean hacker teams. In any case, the U.S. should prioritize intelligence efforts and joint investigations with the countries in question.

Finally, the Consolidated Appropriations Act of 2018 contained a provision prohibiting U.S. aid to any country supporting North Korean cyber attacks.[177] This is a measures that could cause host nations to dismantle the North Korean networks within their borders. Washington must remind these host nations, particularly China, that there is a price to pay for overlooking the presence of North Korean cyber operatives.

Include cyber as part of North-South negotiations and North Korea-U.S. security discussions

When negotiating with North Korea, the U.S. must seek a comprehensive deal that addresses more than just its nuclear program. An agreement dedicated to curbing solely North Korea's nuclear capabilities will leave key issues unaddressed. This includes human rights atrocities, WMD, conventional military capabilities, and cyber aggression.[178]

Neither the April 27 Panmunjom Declaration nor the joint statement following the June 12 Singapore summit explicitly addressed cyber. Some will argue

[175] "North Korea's Ruling Elite Are Not Isolated," *Recorded Future*, July 25, 2017. (https://www.recordedfuture.com/north-korea-internet-activity/)

[176] U.S. Department of Justice, Press Release, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," September 6, 2018. (https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and)

[177] "(LEAD) U.S. to end aid to countries helping N. Korea's cyberattacks," *Yonhap News Agency* (South Korea), March 27, 2018. (http://m.yna.co.kr/mob2/en/contents_en.jsp?cid=AEN20180327009400315&domain=3&ctype=A&site=0100000000)

[178] Anthony Ruggiero, "Hold the Nobel Prize: Kim Is Setting a Trap for Trump," *Politico*, May 10, 2018. (https://www.politico.com/magazine/story/2018/05/10/trump-north-korea-kim-jong-un-nobel-prize-218357)

against including cyber activities on the same grounds that they argue against addressing human rights, namely that it would be a distraction from the nuclear negotiations. Yet the U.S. has avoided human rights discussions in nuclear negotiations for some 25 years without securing an effective nuclear agreement or improvements to North Korean human rights.

The failure to address North Korean cyber activities allows the regime to believe these are permissible provocations. All future security discussions and negotiations must include a cyber component, and the regime must know the consequences for employment of hostile cyber activities to include cyber-enabled economic warfare.

Incentivize publication of information about cryptocurrency hacks

Cryptocurrency exchanges have become a target of choice for cyber criminals. While North Korea has been blamed for some of the attacks, others remain unattributed or are the work of other cyber criminals. Because exchanges often do not publicize details about these hacks, it is difficult for outside researchers to analyze transactions and uncover the methodologies used in each attack.

No matter the level of threat, the United States and South Korea should issue breach notification rules and work with relevant authorities in other jurisdictions to require exchanges to release specific information about attackers, including the wallets where they deposit stolen funds. While taking steps to ensure the protection of clients' identity, publicizing attack information would warn third parties against engaging in transactions with those wallets, and it would enable researchers to uncover illicit networks and patterns of transactions. Researchers could determine any connections between cryptocurrency hackers and those involved in ransomware or other malicious cyber exploitations. This greater visibility would enable law enforcement to better prosecute crimes and decision makers to better develop policies to combat these attacks.

Conclusion

Cyber is just one weapon in North Korea's arsenal, yet it has given new leverage to Pyongyang. In particular, North Korea has demonstrated its capability and intention to target the economic livelihood of its adversaries through cyber-enabled means.

While North Korea has yet to unleash a large-scale crippling attack on Washington or Seoul, its persistent offensive cyber campaigns demonstrate that Pyongyang's cyber capabilities improve day by day. North Korea has shown it can penetrate network defenses and even destroy compromised computers. And while North Korea's cyber army is still a long way from posing an existential threat to the U.S. and its allies, treating cyber as an afterthought could be something Washington and Seoul may later regret.

Acknowledgments

The authors would like to thank Samantha Ravich, Annie Fixler, Jonathan Schanzer, David Adesnik, Nicole Salter, Cliff May, Mark Dubowitz, Erin Blumenthal, Trevor Logan, Boris Zilberman, and Daniel Ackerman. In addition we are grateful for the expert external reviews critical comments from Jung Pak, Bruce Klingner, and Richard Andres. Any errors are the authors' sole responsibility.

This report is part of a series of studies on adversarial strategies from FDD's project on cyber-enabled economic warfare. The project aims to promote a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities that the new environment poses and assist as policymakers develop and implement a winning strategy for the United States within this domain.

Cover Illustration by Daniel Ackerman

About The Authors

Mathew Ha is a research associate at FDD focusing on North Korea. He studies North Korea's illicit financing, human rights, the U.S.-Korea alliance, and inter-Korean relations. He brings experience working with the Korea Chair at the Center for Strategic and International Studies and the Committee for Human Rights in North Korea. He completed an MA in Asian Studies at Georgetown University with a concentration in Politics and Security and the Korean peninsula. He holds a BA in World Politics from Hamilton College.

David Maxwell is a senior fellow at FDD. He is a 30-year veteran of the United States Army, retiring in 2011 as a Special Forces Colonel with his final assignment serving on the military faculty teaching national security strategy at the National War College. He has served in various command and staff assignments in the Infantry in Germany and Korea as well as in Special Forces at Ft. Lewis, Washington; Seoul, Korea; Okinawa, Japan; and the Philippines, with total service in Asia of more than 20 years. He served on the United Nations Command / Combined Forces Command / United States Forces Korea CJ3 staff where he was a planner for UNC/CFC OPLAN 5027-98 and co-author of the original ROK JCS – UNC/CFC CONPLAN 5029-99 (North Korean Instability and Collapse) and later served as the Director of Plans, Policy, and Strategy (J5) and the Chief of Staff for Special Operations Command Korea (SOCKOR). From 2000 to 2002 he commanded 1st Battalion, 1st Special Forces Group (Airborne) in Okinawa, Japan. He has been the G3 and Chief of Staff of the US Army Special Operations Command. He commanded the Joint Special Operations Task Force-Philippines in 2006-2007.

About the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance

The Center on Sanctions and Illicit Finance (CSIF) at the Foundation for Defense of Democracies (FDD) works to expand the understanding of economic warfare in the 21st century to develop further the doctrines and strategies of American financial and economic suasion. Launched in 2014, CSIF builds upon FDD's success as a leading policy institute on the use of financial measures in foreign policy. Our mission is to strengthen and preserve the ability of America and its allies to deploy economic tools to promote national security, develop strategies to isolate rogue actors, and identify and guard against economic threats and vulnerabilities.

For more information, please visit www.defenddemocracy.org.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.defenddemocracy.org