Congressional Research Service
Informing the legislative debate since 1914

North Korean Cyber Capabilities: In Brief

Emma Chanlett-Avery
Specialist in Asian Affairs

Liana W. Rosen
Specialist in International Crime and Narcotics

John W. Rollins
Specialist in Terrorism and National Security

Catherine A. Theohary
Specialist in National Security Policy, Cyber and Information Operations

August 3, 2017

Congressional Research Service
7-5700
www.crs.gov
R44912

CRS REPORT
Prepared for Members and
Committees of Congress

Overview

As North Korea has accelerated its missile and nuclear programs in spite of international sanctions, Congress and the Trump Administration have elevated North Korea to a top U.S. foreign policy priority. Legislation such as the North Korea Sanctions and Policy Enhancement Act of 2016 (P.L. 114-122) and international sanctions imposed by the United Nations Security Council have focused on North Korea's WMD and ballistic missile programs and human rights abuses. According to some experts, another threat is emerging from North Korea: an ambitious and well-resourced cyber program. North Korea's cyberattacks have the potential not only to disrupt international commerce, but to direct resources to its clandestine weapons and delivery system programs, potentially enhancing its ability to evade international sanctions. As Congress addresses the multitude of threats emanating from North Korea, it may need to consider responses to the cyber aspect of North Korea's repertoire. This would likely involve multiple committees, some of which operate in a classified setting. This report will provide a brief summary of what unclassified open-source reporting has revealed about the secretive program, introduce four case studies in which North Korean operators are suspected of having perpetrated malicious operations, and provide an overview of the international finance messaging service that these hackers may be exploiting.

North Korean Cyber Operations: Scope and Capability

North Korea (officially called the Democratic People's Republic of Korea, or DPRK) has one of the smallest Internet presences in the world, and the bulk of its limited Internet access is routed through China.[1] The DPRK has a national intranet called *Kwangmyon* that offers email and websites and connects domestic institutions, but appears to be disconnected from the World Wide Web.[2] Elites and foreign visitors have access to the broader Internet, but usage is heavily monitored by the regime.[3] The North Korean government has devoted significant resources to develop its cyber operations and has grown increasingly sophisticated in its ability to attack targets. Among governments that pose cyber threats to the United States, some analysts consider the North Korean threat to be exceeded only by those posed by China, Russia, and Iran.[4] North Korea appears to be engaging in increasingly hostile cyber activities including theft, website vandalism, and denial of service attacks. Some cybersecurity analysts, however, question whether the country has developed the technical capability to conduct large-scale destructive attacks on critical infrastructure. (See "The Debate on North Korea's Perceived Cyber Capabilities" section below.)

South Korea—among the most wired countries in the world—has been the victim of suspected North Korean hacks for years, but Pyongyang's cyber activities appear to have expanded to include other countries, particularly targeting the banking sector. As in North Korea's accelerating missile program, even the failures reveal the growing capability and ambition of the Pyongyang

[1] Pagliery, Jose, "A Peek into North Korea's Internet," *CNN Tech*, December 23, 2014, http://money.cnn.com/2014/12/22/technology/security/north-korean-internet/index.html.

[2] Sparks, Matthew, "Internet in North Korea: Everything You Need to Know," *The Telegraph*, December 23, 2014, http://www.telegraph.co.uk/technology/11309882/Internet-in-North-Korea-everything-you-need-to-know.html.

[3] "How the Internet 'Works' in North Korea," Slate.com, November 26, 2016.

[4] Will Edwards, "North Korea as a Cyber Threat," *The Cypher Brief*, July 1, 2016.

regime. In early 2017, North Korean hackers reportedly attempted to break into several Polish banks. Although unsuccessful, the hackers' techniques reportedly were more advanced than many security analysts had expected. Researchers also uncovered a list of other organizations that North Korean hackers may have intended to target, including large U.S. financial institutions, the World Bank, and banks in countries from Russia to Uruguay.[5]

Organization of North Korean Cyber Operations

Open-source research findings on how the secretive Kim regime organizes its security-related operations are by definition limited and based to some degree on conjecture and guesswork.[6] However, most sources report that North Korean cyber operations are headquartered in the Reconnaissance General Bureau (RGB), specifically under Bureau 121.[7] The RGB appears to serve as the central hub for North Korea's clandestine operations and in the past has been blamed for attacks such as the 2010 sinking of the *Cheonan*, a South Korean navy corvette, killing 46 sailors.[8] The Korean People's Army (KPA) General Staff is responsible for operational planning, and its cyber units may coordinate with RGB as well.

The size of North Korea's cyber force has been estimated to be between 3,000 and 6,000 hackers trained in cyber operations, with most of these "warriors" belonging to the RGB and the KPA's General Staff.[9] North Korea identifies talented students and trains them at domestic universities such as Kim-Il-Sung University, Kim Chaek University of Technology, and the Command Automation University.[10] Some research suggests that some students train internationally in Russia and China.[11] North Korean hackers often live overseas—a freedom only afforded to a few elite citizens—to take advantage of other countries' more advanced infrastructure.[12]

North Korean Motivations

Since the beginning of the decade, security experts and U.S. officials have voiced increasing concern about North Korea's improving cyberattack capabilities. Analysts of North Korean affairs identify a range of motivations for North Korea to conduct cyber operations, including retaliation, coercion, espionage, and financial gain. The hacking of Sony Pictures Entertainment in 2014, which the Federal Bureau of Investigation (FBI) publicly attributed[13] to the North Korean government, apparently was motivated by Pyongyang's displeasure with a movie's depiction of the fictional assassination of leader Kim Jong-un. Since 2009, serial cyberattacks on South Korean institutions and media outlets have demonstrated North Korean goals of disrupting and disturbing, as well as of conducting espionage.

[5] "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*. March 25, 2017.

[6] All information in this product is drawn from unclassified open-source material.

[7] "North Korea's Cyber Operations," Center for Strategic and International Studies Korea Chair, December 2015.

[8] Joseph Bermudez, "A New Emphasis on Operations Against South Korea?" *38 North Special Report*, June 2010.

[9] Ken Gause, "North Korea's Provocation and Escalation Calculus: Dealing with the Kim Jong-un Regime," Center for Naval Analyses, August 2015.

[10] "N. Korea Bolsters Cyberwarfare Capabilities," *The Korea Herald*, July 27, 2014.

[11] Donghui Park, "North Korea Cyber /Attacks: A New Asymmetrical Military Strategy," Henry M. Jackson School for International Studies post, June 28, 2016.

[12] "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*. March 25, 2017.

[13] "FBI Head Details Evidence That North Korea Was Behind Sony Hack," *Los Angeles Times*, January 7, 2015.

In recent years, it has appeared that North Korea may increasingly be seeking financial gain from its cyber operations. In response to North Korea's two nuclear tests in 2016 (its fourth and fifth overall) and accelerating pace of missile testing, United Nations Security Council resolutions have imposed progressively stringent sanctions on the country. Even China, North Korea's primary patron and source of more than 80% of its trade, appears willing to further pressure the Kim regime. In need of resources to maintain its two-track policy (the so-called *byungjin* line) of economic development and nuclear weapons development, the Kim regime may be demanding more income from its cyber program.

The use of cyber operations fits into North Korea's national strategy of employing asymmetric tactics to disrupt its adversaries. Because the difficulty of attributing any particular attack to a specific party potentially enhances deniability, North Korea's use of cyber activities may help it mitigate the risk of retaliation and provide its traditional defenders—most often China—cover to resist punishing the regime. The precarious security situation on the Korean peninsula contributes to this calculus: a direct military attack by North Korea on South Korea or another party would most likely result in a counter-strike on North Korea, which could escalate into a broader military conflict that could bring down the North Korean regime. An attack in cyberspace, however, could disrupt the status quo with less risk of retaliation. Military analysts who follow North Korea note that the Kim regime is attracted to the use of irregular provocations to keep its adversaries off balance, and often prefers low-intensity strikes. The relatively low cost of cyber operations, together with the mitigated risk of retaliation, may make them more appealing to the North Korean regime.[14]

The Debate on North Korea's Perceived Cyber Capabilities

In recent years numerous cyberattacks around the world have been attributed to North Korea. Observers suggest North Korea has a sophisticated and ever-growing offensive cyber capability. Others assess North Korea as not possessing the infrastructure or technical skill necessary to undertake global cyberattacks. Still others note that some of the attacks ascribed to North Korea appear relatively unsophisticated and could have been completed with limited access to advanced technologies or a high degree of technical capability. The debate largely centers around whether North Korea has the capability to go beyond mere nuisance to more destructive cyberattacks on critical infrastructure.

In April 2014, General Curtis M. Scaparrotti, then-Commander, United Nations Command and the Republic of Korea Combined Forces, offered the following assessment:

> North Korea employs computer hackers capable of conducting open-source intelligence collection, cyber-espionage, and disruptive cyber-attacks. Several attacks on South Korea's banking institutions over the past few years have been attributed to North Korea. Cyber warfare is an important asymmetric dimension of conflict that North Korea will probably continue to emphasize—in part because of its deniability and low relative costs.[15]

Other observers support the contention that North Korea has developed, and is expanding, its offensive cyber capabilities, noting increases in personnel and testimony from defectors. In May

[14] "North Korea's Cyber Operations," Center for Strategic and International Studies Korea Chair, December 2015.

[15] U.S. Congress, House Committee on Armed Services, Statement of General Curtis M. Scaparrotti, Commander, United Nations Command; Commander, United States -Republic of Korea Combined Forces Command, United States Forces Korea, 113th Cong., 2nd sess., April 2, 2014, http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf.

2015 a North Korean defector, Professor Kim Heung-Kwang, who taught computer science at North Korea's Hamheung Computer Technology University, told BBC News that he estimated "between 10% to 20% of the regime's military budget is being spent on online operations" and that "harassing other countries is to demonstrate that North Korea has cyber war capacity" that could eventually result in "military attacks, killing people and destroying cities."[16] Relying on Korean and English resources, the Center for Strategic and International Studies concluded in a 2015 report:

> Left unchecked and barring any unpredictable power shift, North Korea is likely to continue to place strategic value in its cyber capabilities. Future North Korean cyberattacks are likely to fall along a spectrum, with one end being continued low intensity attacks and the other end characterized by high intensity attacks from an emboldened North Korea. Concurrently, the DPRK will likely deepen the integration of its cyber elements into its conventional military forces.[17]

Some observers suggest that, because there is little visibility into North Korea's activities, the possible threats from North Korean cyber activities are often inflated. An assessment released by the Korea Economic Institute found that the international community's "fears of the unknown increase the risk of threat inflation dramatically."[18] These analysts contend that while North Korea may have the capability to undertake global cyber nuisance or theft-motivated activities, the nation lacks the ability to undertake operations that are "complex or as devastating as the Stuxnet attack, a computer virus that disrupted Iran's nuclear program."[19]

Selected Case Studies of Suspected North Korean Cyberattacks

This section provides brief overviews of four instances of suspected North Korean cyberattacks. The cases have been selected to illustrate a range of possible North Korean motivations: the first discusses possible North Korean responsibility for a globally disruptive attack, the second involves the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging service, the third is a U.S. case in which the goal appeared to be nonfinancial, and the last is an attack on banks in South Korea, the regime's most frequent target.

WannaCry

On May 12, 2017, organizations across the world reported ransomware infections affecting their computer systems. The infections, caused by a ransomware strain referred to as WannaCry, restrict users' access to a computer until a ransom is paid to unlock it. Reportedly, 300,000 users

[16] Dave Lee and Nick Kwek, "North Korean Hackers 'Could Kill,' Warns Key Defector," *BBC News*, May 29, 2015, pp. http://www.bbc.com/news/technology-32925495.

[17] James Lewis, Victor Cha, and Jun, LaFoy, Sohn, "North Korea's Cyber Operations: Strategy and Responses," *Center for Strategic and International Studies, Office of the Korea Chair*, November 23, 2015, https://www.csis.org/analysis/executive-summary-north-koreas-cyber-operations-strategy-and-responses.

[18] Dr. Alexandre Mansourov, "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance," *Korea Economic Institute of America -ACADEMIC PAPER SERIES*, December 2, 2014. http://keia.org/sites/default/files/publications/kei_aps_mansourov_final.pdf.

[19] Will Edwards, "North Korea as a Cyber Threat," *The Cipher Brief*, July 1, 2016. https://www.thecipherbrief.com/article/asia/north-korea-cyber-threat-1092.

in at least 150 countries were affected by the ransomware.[20] The WannaCry worm was initially delivered through phishing attacks, but was able to spread more quickly than normal ransomware, as it exploited security vulnerabilities to move remotely between unpatched computers.

In April 2017, an anonymous online group known as the Shadow Brokers released what it alleged was a series of surveillance-enabling tools stolen from the National Security Agency (NSA) that, among other things, exploited a Microsoft Windows security vulnerability known as EternalBlue.[21] It was then reported that Microsoft had patched the vulnerabilities that these tools exploited the previous month, prompting speculation that NSA had alerted Microsoft to the theft.[22] Included in the March 2017 security update was a patch to protect against the propagation of WannaCry ransomware. Subsequently, only unpatched systems were susceptible to WannaCry, including outdated versions of Windows. Its proliferation was further inhibited after the implementation of a "kill switch" on May 12, 2017.[23]

North Korea is suspected to be the architect of WannaCry, which experts say was written after the Shadow Brokers release.[24] According to news reports, the NSA issued an internal assessment that linked the ransomware to North Korea's RGB.[25] The assessment attributes WannaCry to North Korea with "moderate confidence," and includes as evidence IP addresses in China that are known to have been used by the RBG. The WannaCry hackers are said to be part of the "Lazarus Group" that was also behind February 2016 SWIFT hacks (see below). In both cases, the cyberattacks may have been used as an attempt to raise revenue for the regime. However, some security researches believe that flaws in the WannaCry code and its demands for payment in digital currency suggest that the hackers may have used WannaCry to accumulate personal wealth.[26] The hackers raised $140,000 in the digital currency bitcoin through WannaCry but have yet to convert it to hard cash, reportedly most likely due to an operational error that has made the transactions trackable by law enforcement entities.[27]

Bangladesh Bank

In February 2016, a series of cyberattacks on banks in Bangladesh and Southeast Asia resulted in the theft of approximately $81 million.[28] Some researchers have linked these attacks to North Korea, citing similarity between the code used in this incident and that used in previous attacks in

[20] Initial reports placed the number of affected computers at 200,000. See Goldman, Russell. "What We Know and Don't Know About the International Cyberattack," *New York Times*, May 12, 2017.

[21] Schneier, Bruce, "Who Are the Shadow Brokers?" *The Atlantic*, May 23, 2017, https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

[22] Dellinger, AJ, "WannaCry Ransomware Attack: NSA Disclosed Vulnerability to Microsoft After Learning It Was Stolen by Shadow Brokers," *International Business Times*, May 17, 2017.

[23] Newman, Lily Hay. "How An Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack," *Wired*, May 13, 2017.

[24] Schneier, Bruce, "Who Are the Shadow Brokers?" *The Atlantic*, May 23, 2017, https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

[25] Nakashima, Ellen, "The NSA Has Linked the WannaCry Computer Worm to North Korea," *Washington Post*, June 14, 2017.

[26] Reuters, "Symantec Says 'Highly Likely' North Korea Group Behind Ransomware Attacks," May 23, 2017, http://www.cnbc.com/2017/05/23/symantec-says-highly-likely-north-korea-group-behind-ransomware-attacks.html.

[27] Ibid.

[28] Viswanatha, Aruna and Hong, Nicole, "U.S. Preparing Cases Linking North Korea to Theft at N.Y. Fed," *Wall Street Journal*, March 22, 2017, https://www.wsj.com/articles/u-s-preparing-cases-linking-north-korea-to-theft-at-n-y-fed-1490215094.

which North Korea was implicated. In this theft, hackers used the Society for Worldwide Interbank Financial Telecommunication (SWIFT) global messaging service to the Federal Reserve Bank of New York to transfer money from the Bangladesh Central Bank to accounts in the Philippines. (See **Appendix** below for further background on the SWIFT system.) This reportedly was achieved by network intruders inserting malware into a SWIFT terminal used by Bangladesh's central bank. Bangladesh's network may have been particularly vulnerable, as it reportedly lacked a firewall to protect against outside intrusion. The hackers sent fraudulent SWIFT messages between the banks in New York and Bangladesh, and altered the printed confirmation of transactions in order to obscure the activity. The hackers had requested nearly $1 billion from one bank to the other, but the U.S. central bank rejected most of the requests. On March 21, 2017, Deputy Director of the National Security Agency Richard Ledgett noted research that "forensically" tied this incident to the cyberattacks on Sony, and said that if North Korea's role in the bank robbery was confirmed, it would represent a troubling new capability.[29] Reportedly, some investigators believe that Chinese intermediaries aided North Korea in conducting the theft, while others have outright accused Chinese hackers of being the perpetrators.[30]

In addition to the Bangladesh Bank, hackers reportedly attacked other banks using SWIFT. According to one report,[31] North Korea is now being linked to similar attacks on banks in as many as 18 countries.[32] The SWIFT system is used by some 11,000 banks and companies to transfer money from one country to another and is considered the backbone of global finance. Yet cyberattacks on banks have not been limited to the use of SWIFT; other bank attacks were said to have employed a "watering hole" technique in which hackers lurk around a highly trafficked website in order to redirect the website's visitors to a page containing malicious software. Security researchers at Symantec believe that the same hackers were behind both of these attack methods.[33]

Sony Pictures Entertainment

In the run-up to the scheduled Christmas Day 2014 release of *The Interview*, a film depicting the fictional assassination of North Korean leader Kim Jong-un, North Korea's Foreign Ministry called the film "the most blatant act of terrorism and war" and threatened a "merciless countermeasure."[34] On November 24, Sony Pictures Entertainment experienced a cyberattack that disabled its information technology systems, destroyed data, and accessed internal emails and other documents that were then leaked to the public. North Korea denied involvement in the attack, but praised hackers, who called themselves the "Guardians of Peace," for having done a

[29] Spicer, Jonathan and Menn, Joseph, "U.S. May Accuse North Korea in Bangladesh Cyber Heist: WSJ," March 22, 2017, Reuters, http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN16T2Z3.

[30] Lema, Karen and Mogato, Manuel, "Bangladesh Bank Hackers 'Possibly Chinese,' Says Philippines Senator," Reuters, April 5, 2016, http://www.reuters.com/article/us-usa-fed-bangladesh-philippines-idUSKCN0X2190.

[31] Kaspersky Lab, "Lazarus Under the Hood," accessed at https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf.

[32] Pagliery, Jose, "North Korea-linked hackers are attacking banks worldwide," *CNN*, April 4, 2017, http://www.cnn.com/2017/04/03/world/north-korea-hackers-banks/.

[33] Mozer, Paul and Sang-Hun, Choe, "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*, March 25, 2017, https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html?_r=0.

[34] "Hackers' Threats Prompt Sony Pictures to Shelve Christmas Release of 'The Interview,'" *Washington Post*. December 17, 2014.

"righteous deed."[35] Hackers then sent emails, threatening "9/11-style" terrorist attacks on theaters scheduled to show the film, leading some theaters to cancel screenings and for Sony to cancel its widespread release; U.S. officials claimed to have "no specific, credible intelligence" of such a plot.[36]

The FBI and the Director of National Intelligence (DNI) attributed the cyberattacks to the North Korean government.[37] During a December 19, 2014, press conference, President Obama pledged to "respond proportionally" to North Korea's alleged cyber assault, "in a place, time and manner of our choosing" and called the incident an act of "cyber-vandalism."[38] On December 20, cyber analysts and news media reported that the North Korean network providing access to the Internet went offline for approximately 10 hours. Many cyber analysts said the disruption pointed to a network attack, although they could not rule out either an overload or a preventive shutdown by North Korea.[39] U.S. officials would not comment on whether this constituted the "proportional response," saying only that some elements of the response would be seen while others would not. Although elements of the U.S. intelligence community publicly claimed to have compelling proof of North Korean involvement in the attacks on Sony, some information security experts questioned whether North Korea had the capability to conduct destructive attacks and whether the malware involved contained markers that would definitively indicate North Korean origin.[40]

The Sony incident differs from other cyberattacks in that it had a destructive element; in this incident, many of the work stations targeted were damaged beyond repair and had to be replaced. Previously, much of the cyber activity that stemmed from North Korea had been limited to being disruptive, such as denial of service or website defacement. For example, the South Korean government accused North Korea of a December 2014 cyberattack on the computer systems of the Korea Hydro and Nuclear Power Ltd (KHNP), which runs South Korea's nuclear power plants.[41] In December 2014 and again in March 2015, hackers published designs, manuals, and other information that had been obtained through a phishing attack on employee email accounts, prompting heightened cybersecurity measures. Investigators said that the hackers intended to cause a malfunction at atomic reactors, but failed to break into their control system, which is not connected to the Internet.[42]

[35] "North Korea: Sony Hack a Righteous Deed But We Didn't Do It," *The Guardian*, December 7, 2014.

[36] "U.S. Weighs Options to Respond to Sony Hack, Homeland Security Chief Says," *Wall Street Journal*, December 18, 2014.

[37] FBI National Press Office, "Update on Sony Investigation," December 19, 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[38] Grossman, Andrew, "U.S. Weighs Options to Respond to Sony Hack, Homeland Security Chief Says," *Wall Street Journal*, December 18, 2014, https://www.wsj.com/articles/u-s-weighs-options-to-respond-to-sony-hack-homeland-security-chief-says-1418926834.

[39] Bennett, Cory, "Did the US Take Down North Korea's Internet?" *The Hill*, December 23, 2014, http://thehill.com/policy/cybersecurity/227944-was-the-us-behind-north-koreas-internet-outage.

[40] See FBI National Press Office, "Update on Sony Investigation," December 19, 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation, and Szoldra, Paul, "A Hacker Explains Why You Shouldn't Believe North Korea Was Behind the Massive Sony Attack," *Business Insider*, June 10, 2016, http://www.businessinsider.com/north-korea-sony-hack-2016-6.

[41] "S.Korea Accuses North of Cyber-Attacks on Nuclear Plants," *Phys.org*, March 17, 2015.

[42] "South Korea Says Nuclear Reactors Safe After Cyber-Attacks," *Security Week*, December 25, 2014.

South Korean Banks

In March 2013, several South Korean banks and news broadcasters experienced network disruption at a time when American and South Korean military forces were conducting major exercises. In this attack, malware previously identified as "DarkSeoul" evaded South Korean cybersecurity software and rendered computers unusable.[43] The Korea Communications Commission said that the disruption originated at an Internet Protocol address in China but that it was not known who was responsible. Some observers suspected North Korean involvement, particularly as the attacks reportedly were less sophisticated than those that have been linked to China.[44] Previous attacks that had been linked to North Korea mostly involved a less sophisticated method of attack known as a denial of service, in which Internet traffic targets and overwhelms a particular site, causing it to become temporarily unusable. A denial of service attack on the National Agricultural Co-operative Federation bank in 2011 caused a three-day outage that left customers unable to access their accounts, and also deleted some credit card records.[45] A wave of denial of service cyberattacks beginning on July 4, 2009, temporarily slowed or disabled targets in both the United States and South Korea. The South Korean National Intelligence Service said that the attacks appeared to have been carried out by a hostile group or government, and a Korean news service reported that the agency had implicated North Korea or pro-North Korean groups.[46] Similar malware code reportedly was used in these latter two attacks, and some of the Internet Protocol addresses were traced to computers in North Korea. South Korean officials claim that North Korea has conducted more than 6,000 cyberattacks since 2010, costing nearly $650 billion in repairs and economic losses.[47]

Issues for Congress

As North Korea improves its ability to conduct more aggressive cyber operations, the executive branch and Congress face pressure to counter such attacks. Response in the cyber arena is mostly classified, heightening the need for relevant congressional committees to engage with the intelligence and defense communities. Classified briefings could broaden congressional understanding of cyber threats to critical infrastructure sectors and how effectively U.S. cyber capabilities can respond to North Korean cyberattacks. How secure is the U.S. financial system? Should Congress develop legislation to regulate the network security of the financial sector? Are more regulations needed to prevent traders from unwittingly exposing their systems to infiltrators? Should the United States direct resources toward securing weak links in international finance systems? What are federal agencies' roles and responsibilities in responding to a cyber incident on private networks? What offensive capabilities is the United States employing to respond to North Korean hackers? What is the Administration's strategy to deter cyberattacks from North Korea? What pressure can the United States put on countries that host North Korean

[43] Sang-Hun, Choe, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *New York Times*, March 20, 2013.

[44] "Cyberattack Shakes South Korea: Could North Korea Have Pulled it Off?" *Christian Science Monitor*, March 20, 2013.

[45] Nicole Perlroth and Michael Corkery, "North Korea Linked to Digital Attacks on Global Banks," *New York Times*, May 26, 2016.

[46] "North Korea 'Behind South Korean Bank Cyber Hack,'" *BBC News*, May 3, 2011, http://www.bbc.com/news/world-asia-pacific-13263888.

[47] Hern, Alex, "North Korean 'Cyberwarfare' Said to Have Cost South Korea £500m," *The Guardian*, October 16, 2013.

overseas hackers? How should the United States weigh North Korean cyber intrusions against other more conventional threats emanating from the regime? How should the sanctions regime address North Korean cyber operations?

The global nature of cyber operations requires multiple committees with varying jurisdictions to share information, oversight, and authority. International finance, foreign affairs, homeland security, armed services, law enforcement, and information technology infrastructure committees may all have equities in this area. Developing legislation may require disparate Members and committees to adequately address the complex nature of the challenge.

Appendix. SWIFT and Cyber-Facilitated Bank Robbery Schemes

Cybersecurity experts and, more recently, U.S. government officials, have suspected North Korean involvement in multiple cyber intrusions designed to exploit a bank's access to the SWIFT network. Based in Belgium, SWIFT is an international financial messaging service that connects more than 11,000 customers in more than 200 countries. Today, SWIFT is the most widely used cross-border financial messaging service, and its messaging platform, SWIFTNet, has long held a reputation for being able to provide secure, reliable, standardized, and quick financial messaging.

Cybercriminals have long targeted financial institutions and their customers through a variety of methods. One such method appears to involve the exploitation of weak security measures at the targeted bank to access the SWIFT messaging service and, in turn, carry out fraudulent financial transactions. The Bangladesh incident described above involved this method. Some observers initially presumed that the Bangladesh Central Bank attack was an isolated incident. Since the Bangladesh Central Bank revelations, however, additional incidents involving similar methods have been reported by the media.[48]

The growing number of such reported incidents has raised several questions among banking and cyber experts regarding the perpetrators, the evolving nature of their capabilities to exploit SWIFT's services, the full extent of the number of compromised banks (including any financial losses that may have resulted), and the effectiveness of existing countermeasures to protect financial institutions from future cyber intrusions. In May 2016, SWIFT's chief executive officer called the Bangladesh case and ensuing revelations at other banks a "watershed event for the industry" and "a big deal ... [that] gets to the heart of banking."[49]

North Korea Access to SWIFT

SWIFT has contributed to international pressure to cut North Korea off from the global financial system by excluding it from its financial messaging services network. On February 27, 2017, a United Nations (U.N.) Panel of Experts report indicated that SWIFT included seven North Korean banks in its network—three of which are subject to U.N. sanctions.[50] By March 8, SWIFT removed the three U.N.-sanctioned banks from their network.[51] By March 16, SWIFT removed the remaining four North Korean banks identified by the U.N. Panel of Experts report.[52] In explaining its termination of services, SWIFT stated that the banks no longer complied with SWIFT membership criteria. According to *The Economist*, reasons for their exclusion included

[48] Michael Corkery, "Once Again, Thieves Enter SWIFT Financial Network and Steal," *New York Times*, May 12, 2016, https://www.nytimes.com/2016/05/13/business/dealbook/swift-global-bank-network-attack.html.

[49] SWIFT, "Gottfried Liebbrandt on Cyber Security and Innovation," keynote address, as prepared for delivery, at the 14th Annual European Financial Services Conference, Brussels, May 24, 2016, https://www.swift.com/insights/press-releases/gottfried-leibbrandt-on-cyber-security-and-innovation.

[50] United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, S/2017/150, February 27, 2017, http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150.

[51] Jeremy Wagstaff and Tom Bergin, "SWIFT Messaging System Bans North Korean Banks Blacklisted by U.N.," Reuters, March 8, 2017, http://www.reuters.com/article/us-northkorea-banks-swift-idUSKBN16F0NI.

[52] Tom Bergin, "SWIFT Messaging System Cuts Off Remaining North Korean Banks," Reuters, March 16, 2017, http://www.reuters.com/article/us-northkorea-banks-idUSKBN16N2SZ.

participation in activities that are illegal, endanger security, or adversely affect SWIFT's reputation.[53]

Other SWIFT-Related Cyber Incidents

The Bangladesh Central Bank case described above gained widespread attention in part due to the sheer amount of stolen funds, the role of the U.S. Federal Reserve in authorizing 5 of the 35 fraudulent payment requests, and the clever exploitation of bank holidays, manipulation of bank-specific operating procedures (including the printer used to confirm SWIFT messages), and transnational transfer of funds to a jurisdiction (the Philippines) known for its bank secrecy laws and a gambling industry that is not subject to anti-money laundering regulations. Since the incident was first reported in March 2016, several other alleged cases have been reported in the media, including attempted intrusions into banks in Vietnam, Ecuador, Ukraine, Turkey, and India. In light of multiple recent cases involving cyber intrusions that target bank access to the SWIFT network, there remains ongoing uncertainty regarding whether any of these attacks can be attributed to North Korea.[54]

Background on SWIFT

SWIFT is organized as a cooperative society under Belgian law and is owned and controlled by its shareholders. Customers include banks, investment institutions, central banks, market infrastructures, and corporate clients. SWIFT, however, is not a bank, does not hold accounts or funds for customers, and is not authorized as a financial clearing and settlement institution. SWIFT began its messaging service in 1977, replacing the Telex technology on which banks previously relied to communicate cross-border financial transfer instructions.[55] In 2016, SWIFT processed more than 6.5 billion financial messages. The volume of financial messages through

[53] "The Investigation into the Bangladesh Heist Continues," *The Economist*, March 23, 2017.

[54] See Allison Grande, "Ecuadorean Bank Is 3rd Caught Up in Hack of SWIFT Users," *Law 360*, May 20, 2016, https://www.law360.com/articles/798829; Michael Riley and Alan Katz, "SWIFT Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh," *Bloomberg News*, May 26, 2016, https://www.bloomberg.com/news/articles/2016-05-26/swift-hack-probe-expands-to-up-to-dozen-banks-beyond-bangladesh; Symantec, "SWIFT Attackers' Malware Linked to More Financial Attacks," *Security Response Blog*, May 26, 2016, https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks; SWIFT, "Gottfried Liebbrandt on Cyber Security and Innovation," keynote address, as prepared for delivery, at the 14th Annual European Financial Services Conference, Brussels, May 24, 2016, https://www.swift.com/insights/press-releases/gottfried-leibbrandt-on-cyber-security-and-innovation; Krishna N. Das and Ruma Paul, "Exclusive: Bangladesh Probes 2013 Hack for Links to Central Bank Heist," Reuters, May 25, 2106, http://www.reuters.com/article/us-cyber-heist-bangladesh-idUSKCN0YG2UT; Josh Kovensky, "Hackers Reportedly Steal $10 Million from a Ukrainian Bank Through SWIFT Loophole," *Kyiv Post*, June 25, 2016, https://www.kyivpost.com/article/content/ukraine-politics/hackers-steal-10-million-from-a-ukrainian-bank-through-swift-loophole-417202.html; Can Sezer and Birsen Altayli, "Turkey's Akbank Faces $4 Million Hit from Attempted Cyber Heist," Reuters, December 16, 2016, http://www.reuters.com/article/us-akbank-cyber-idUSKBN1450MC; Julie Steinberg and Gabriele Parussini, "Was North Korea Behind the Hacking of a Bank in India? *Wall Street Journal*, April 10, 2017, https://www.wsj.com/articles/cybertheft-attempt-on-indian-bank-resembles-bangladesh-heist-1491816614; Jim Finkle, "Exclusive: SWIFT Discloses More Cyber Thefts, Pressures Banks on Security," Reuters, August 31, 2016, http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C.

[55] SWIFT was founded in 1973 as a member-owned cooperative. SWIFT shareholders elect a 25-member board of directors who govern the company and oversee its management. The current CEO is Gottfried Liebbrandt (previously of McKinsey and Company). The chairman of the board of directors is Yawar Shah (also the managing director of franchise risk and strategy at Citigroup). One other current SWIFT board member represents a U.S. financial institution: Emma Loftus, who is managing director and head of global payments, foreign exchange, and channels at J.P. Morgan Treasury Services, USA.

SWIFTNet has grown in recent years.[56] In April 2017, SWIFT reported an average of 28.4 million FIN messages, the most common form of messaging service provided by SWIFT, per day. In the first quarter of CY2017, SWIFT reported a total of 1.71 billion FIN messages (up from 1.56 billion in the first quarter of CY2016).

Messages sent by SWIFT customers are authenticated and encrypted with specialized SWIFT security and identification technology.[57] Customers may access the SWIFT messaging environment through a variety of means, including via permanent leased lines, the Internet, SWIFT's cloud service, and appointed partners. One common way to access the SWIFT environment is through the SWIFT Alliance Access (SAA); this was the interface that the Bangladesh Central Bank used in 2016. Access to the SWIFT environment is also subject to a variety of security protocols designed to protect customer data from unauthorized disclosure or modification during transmission. Security protocols include physical measures to protect the premises where access points are located, SWIFT-specific digital keys, certificates, and signatures. Banks, for example, are identified by a set of assigned codes and SWIFT verifies the authenticity of such credentials before messages can be transmitted.

In May 2016, following widespread media attention to the Bangladesh Central Bank case, SWIFT announced the beginning of a new "Customer Security Programme" designed to improve information sharing on cyber threats and offer additional tools to protect the SWIFT platform and customer-managed entry points into the system.[58] SWIFT also now maintains a cybersecurity "roadmap" that identifies security priority areas on a rolling three-year period.

Author Contact Information

Emma Chanlett-Avery
Specialist in Asian Affairs
echanlettavery@crs.loc.gov, 7-7748

Liana W. Rosen
Specialist in International Crime and Narcotics
lrosen@crs.loc.gov, 7-6177

John W. Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

Catherine A. Theohary
Specialist in National Security Policy, Cyber and Information Operations
ctheohary@crs.loc.gov, 7-0844

[56] See https://www.swift.com/about-us/swift-fin-traffic-figures#topic-tabs-menu.

[57] See https://www.swift.com/about-us/discover-swift/information-security.

[58] SWIFT, "Gottfried Liebbrandt on Cyber Security and Innovation," keynote address, as prepared for delivery, at the 14th Annual European Financial Services Conference, Brussels, May 24, 2016, https://www.swift.com/insights/press-releases/gottfried-leibbrandt-on-cyber-security-and-innovation.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu