The Democratic People's Republic of Korea

An Analysis of the DPRK's Cyber Resources and Their Threat to Global Security and Economic Stability

ISEC 1005
Cyber Crime Survey
Fall 2024

Matthew Boutilier | W0498901
Lucas Hoyles | W0276530
Liam Nolter | W0486718

Contents

Introduction

History and Context

Political History

Since 1948, the Democratic People's Republic of Korea ("DPRK" or "North Korea") has been ruled exclusively by the Kim family, creating what is essentially a dynasty. When 24-year-old Kim Il-Sung led a group of Chinese-supported communist guerrilla attacks against Japanese forces in 1937, he was praised and gained fame for being the only resistance fighter to hold territory for Korea in World War II. After the liberation of Korea in 1945, very few remaining communist soldiers were still active in the country. When the 25th Russian Army entered Korea, they were not prepared to run their half of the country. The Russian Army had very little knowledge of local Korean politics, so they decided to copy Russia and make the country pro-Soviet. Since Kim Il-Sung was well known for fighting in the war, the Russians considered him along with one other candidate to run the country. (Apple, n.d.) (Lutz T. , 2015)

Kim spoke for the first time to North Korea's residents on October 14th, 1945, at a rally that was honouring the Soviet Union for liberating Korea. Major-General Lebedev used this rally as an opportunity to present Kim as a successful military man. The residents that attended the rally were doubtful that the impressive military claims were true since Kim was only 33 at the time. When the first draft of the constitution for the DPRK was first sent to Moscow, Kim Il-Sung was not the original leader listed, instead, Kim Tu-Bong was specified to be the leader. Kim Tu-Bong was the chairman of the North Korean Workers Party at the time, but he did not show any signs of having real power since he had no military experience. (Lutz T. , 2015)

In 1949, the Worker's Party of Korea was created when the pro-communist political parties Worker's Party of North Korea and the Worker's Party of South Korea merged. Kim Il-Sung was elected as the chairman of the Worker's Party which solidified his role as leader

of the DPRK and the Worker's Party of Korea has remained in power in the region since its inception. (Lutz T. , 2015)

On July 4th, 1972, Pyongyang and Seoul both announced a joint statement. The statement called for a peaceful reunification of the country North and South Korea both made the following agreements to achieve the unification. (Ministry of Foreign Affairs of Japan, 1972) (Ministry of Unification of the Republic of Korea, 1972)

- The unification must be done independently without help or interference from foreign sources.
- They must not use force against each other to achieve the unification. It must be obtained through peaceful means.
- They will try to achieve a sense of national unity, bringing everyone together even if they have differences in beliefs, ideologies or political systems.
- They also agreed not to slander or undertake military actions against each other no matter the size of the attack.

In October 1980, Kim Il-Sung designated his son, Kim Jong-Il, as his successor. When Kim Il-Sung died from heart complications in 1994, Kim Jong-Il was bumped up to be the leader, but it was not until 1997, that Kim Jong-Il was given the chairman position of the Worker's Party of Korea. Kim Jong-Il was not elected the official president role because the president position was eliminated by the Supreme People's Assembly and Kim Il Sung was labeled the Eternal President of North Korea. According to Reuters, The Worker's

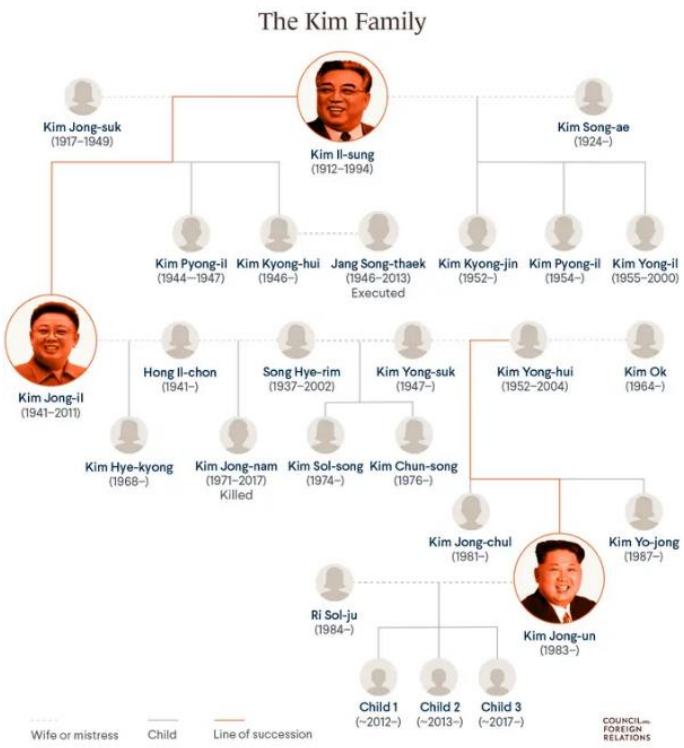

Chart 1: Kim Family Tree (Albert, 2020)

Party of Korea has been praised highly by Kim Jong-Un as being one of the longest-ruling parties in the world. He applauds the party for overcoming the hardships the country has faced and devoting all its strength in building a powerful nation. (Ha Lee & Ick Lew, n.d) (Kim, 2024) (Britannica, 2024)

Upon taking office, Kim Jong-Il appointed his son Kim Jong-Nam to a senior government position in North Korea's Ministry of Public Security and designated Kim Jong-Nam as the future leader of DPRK. This promise of leadership was later revoked in 2001 when Kim Jong-Nam was arrested in Tokyo, Japan for using a fake Dominican Republic passport for travel. Kim Jong-Nam claims he was travelling to Japan to vacation at Disneyland Tokyo. the unauthorized travel from North Korea and Kim Jong-Nam's arrest was reportedly very embarrassing for Kim Jong-Il and after the incident, Kim Jong-Il began distancing Kim Jong-Nam from DPRK leadership positions. (Ryall, 2017)

In early 2009, there was international speculation that Kim Jong-Il's son, Kim Jong-Un was now being prepped to become the new leader instead of Kim Jong-Nam. That April, these rumours were seemingly confirmed when he was given the chairman position of the National Defense Committee. When Kim Jong-Il died after suffering a heart attack in 2011, Kim Jong-Un was declared the supreme leader of North Korea, but it was not official until April 2012. The shift of power surprisingly did not disturb the regime and was able to continue without any disruption. Once he was in power, Kim brought new life back to the Korean Workers' Party. On April 15th, 2012, Kim made his first public speech as leader of North Korea and announced that the threats against his nation were never going to affect the country again. (Council on Foreign Relations, 2022) (BBC, 2023) (Murray, 2024)

History of Economic Hardship

In 1994, early stages of starvation started in North Korea, with the government keeping the information from the citizens. The media told the citizens that the country was a paradise. As the people of North Korea suffered, Kim Jong Il enjoyed pizza parties and expensive Hennessy. In September 1995, North Korea had reached out to the World Food Program for help with the famine but kept the citizens in the dark about what was happening. When the rumours of the famine spread, United Nations inspectors were taken to specific places in North Korea that were not suffering as bad. A report in 1998 showed that this was not the truth, and that all North Korea was suffering badly. Within the four years of the famine, an estimated 240,000 to 3,500,000 North Koreans perished. (Crossing Borders, n.d)

On December 1st, 2009, North Korea announced that the government would be revaluing the country's currency. This move was to cut down on private markets that were hiding away large amounts of cash. The revaluation replaced ₩1000-notes with ₩10-notes. The government also put a strict limit on the amount of cash you were allowed to exchange. The limit for the amount of won you were allowed to exchange was a hundred thousand won, which amounted to $40 dollars with the rates from the black market. After protests, the government raised the limit to a hundred and fifty thousand won in cash and three hundred thousand won in bank savings. (Harden, 2009)

In January 2020, North Korea shut their borders shortly after Beijing made an announcement regarding what is now known as COVID-19. The country had a shoot-to-kill order on their border to keep everyone out. Because of closing the border, their economy dropped 4.5% in 2020, which is the steepest decline in their economy since the famine in 1994. The country also rejected over 2 million AstraZeneca vaccines because they were concerned about the side effects that may occur. Kim Jong Un used the pandemic to take control of the markets yet again. He did this by punishing the corrupt officials and the private entrepreneurs. Along with that, he also limited the use of foreign currency in the country. (Yeo, 2021)

Military History

On December 12th, 1985, North Korea gave consent to the Nuclear Non-proliferation Treaty (NPT), which stopped the spread of nuclear weapons. This then promoted peaceful cooperation on nuclear energy. (Council on Foreign Relations, n.d)

On March 12th, 1993, North Korea tried to withdraw from the NPT. According to the International Atomic Energy Agency Chronology of Key Events, the reasons they wanted to use the escape clause was because of "The Team spirit 'nuclear war rehearsal' military exercises" and 'the IAEA demand for special inspection of two suspect sites". (IAEA, n.d.)

On October 9th, 2006, the Democratic People's Republic of Korea announced that they had conducted a nuclear test and that countries globally expressed their worry about the test in defiance of the international warnings they had received. The test was successful without any radiation leaks. A Korean news organization described the test as a historic event that brought happiness to the North Korean military and people and that it would help maintain peace and stability within the region. (CTBTO, 2006)

On September 3rd, 2017, a significant in size nuclear test was conducted. This test indicated that the bomb that they had made was significantly more powerful than the others tested before. The seismic activity estimated that the explosion exceeded 200 kilotons. This size of an explosion backs up the claims that North Korea may have developed a hydrogen bomb. (Council on Foreign Relations, 2022)

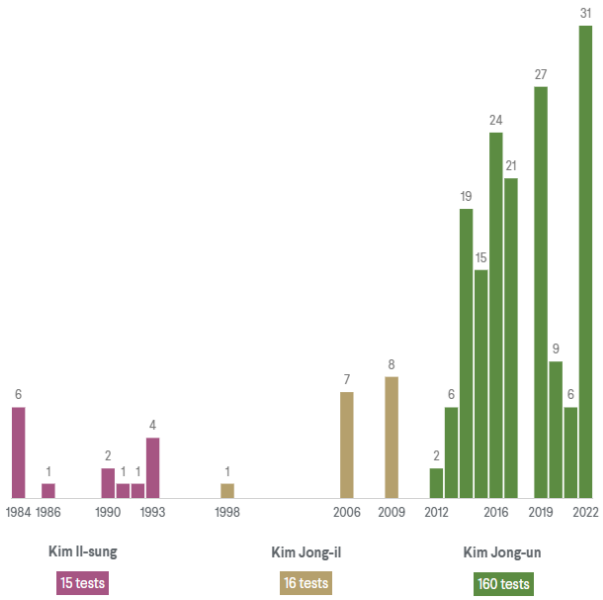

Chart 2: North Korea Missile launches (Council on Foreign Relations, 2022)

Adoption of Cyber

In 1996, Kim Jong Il told soldiers that "all wars in the future will be computer wars.", and this has proven to largely be true. Kim Jong Il saw the importance of technological warfare and the need for a training scheme that would produce highly skilled cyber-operatives for the nation. Despite less than 0.01% of citizens having access to the internet, the government has created an intranet system known as *Kwangmyong* or *Bright*, which contains an estimated 5,500 websites. However, access to the intranet is greatly restricted to foreigners, even contractors for the government who are not citizens. Starting in elementary school, children who are proficient in math and/or science are given access to general IT/Computer courses, if they excel, they can then move on to specialized secondary schools that focus on general computing and software development. Many graduates of these schools end up studying a variety of software-based courses at Kim Il Sung University or Kim Chaek University. However, the government recruits many of its cyber operators from Moranbong University or Mirim College, schools reserved for the top programmers. South Korea's Nation Intelligence Service has claimed that as of 2024 North Korea cyber-force of over 8,000 personnel dedicated to conducting cybercrime on behalf of the North Korean regime. (Statista, 2024) (Talmadge, 2014) (Harrison, 2017) (Sharma, 2024)

Since the late 2000s, North Korea has gravitated to cyberattacks as their preferred method to gain international intelligence and defence information on nation-states they view as hostile to the DPRK. First targeting both South Korea and the United States in 2009 and 2013 with DDoS attacks. North Korea quickly realized the large payout potential that cybercrime provides and has since focused a significant portion of its attacks on international financial institutes and cryptocurrency-based organizations. It was reported by a United Nations Panel of Experts that from 2017-2023 North Korea cryptocurrency-focused cyberattacks have stolen roughly $3 billion. In 2023, A US Diplomat claimed that 50% of North Korea's income is coming from cyberattacks and it is believed that North Korea is utilizing this money to fund the country's development of nuclear weapons. (Weaver, 2009) (Sharma, 2024) (Muncaster, 2023)

Contemporary Government

In 1945, at the end of WWII, Japan surrendered the land that was known at the time as *Japanese Korea*, which was then divided into the Democratic People's Republic of Korea and South Korea along the 38th parallel, North being controlled by the Soviet Union and South being independently controlled with US backing; this arrangement was meant to be temporary in order to remove Japanese forces from the peninsula, however when US forces left South Korea, Kim Il Sung seized the opportunity and in June 1950 started a Soviet-backed invasion When South Korea was nearly annexed, the US, along with seventeen UN members intervened The war lasted until July 1953, when the Korean Armistice Agreement was signed by the US (on behalf of the UN), North Korea, and China. The Armistice Agreement defined the new borders and resulted in North Korea gaining the city of Kaesong, however, they lost a total of 3,900 km^2, including the city of Sokcho, to South Korea. (Britannica, 2024) (Department of State, n.d.)

In contemporary times, North Korea has become a recluse in global relations, empowering its leader to consolidate power and create the dictatorship it currently is. Although the DPRK has a constitution that guarantees rights such as freedom of speech, assembly, and demonstration, along with guaranteeing free activity relating to political parties, under *Article 67*. However, their criminal code *Section 62 (Chapter III, Section I)* says:

- A person who has spread incitement or propaganda with a purpose against the nation shall be sentenced to a term of reform through labour of less than 5 years.
- In particularly grave cases, he or she shall be sentenced to a term of reform through labour of more than 5 years and less than 10 years. (Democratic People's Republic of Korea, 2015)

The combination of these conflicting laws has created a loophole where the government can ignore the freedoms defined in their constitutional document by interpreting someone's speech or actions as going against the ruling party/government.

Natural Resources

The DPRK has a unique economic structure known as a Command Economy, the only other Command Economy in existence currently is Cuba, the system was formerly used in the Soviet Union and China as a method to maintain control over resources and production. In a Command Economy, the government/controlling entity dictates the production amounts and pricing of goods, and a majority of industries are publicly owned. This economic style allows the government to set production quotas and regulate resource usage to align with their current needs, which are not necessarily the needs of citizens. The country's GDP and economic growth are unknown to the World Bank, however, it is generally thought to have a rather low GDP per capita. (Clarke, 2024) (World Bank Group, n.d.)

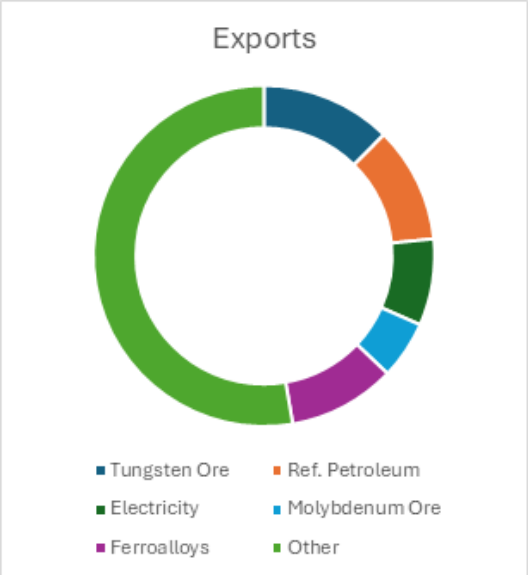

Chart 3: Pie Chart displaying North Korea's Export (World Bank Group, n.d.)s

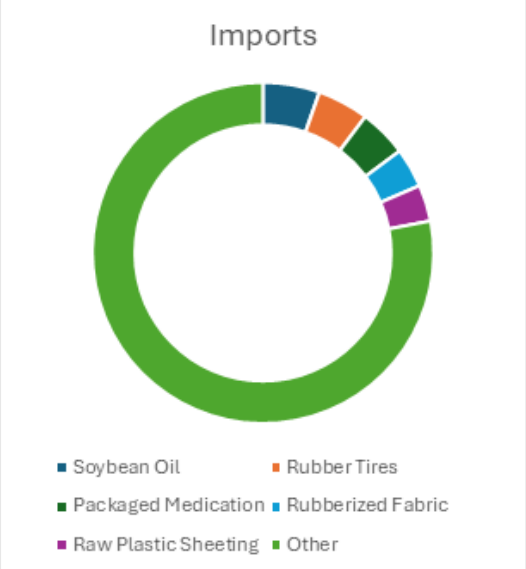

Chart 4: Pie Chart displaying North Korea Imports (World Bank Group, n.d.)

As a whole, North Korea has a diverse economy in terms of imports and exports, despite being ranked 182nd in per capita export value, and 219th in per capita import value. The country's top exports include Tungsten Ore, Refined Petroleum, and Ferroalloys, with China purchasing a total of $131M, and Senegal purchasing $26.9M from North Korea in 2022. When looking at North Korea's imports, there is a trend of finished products as opposed to raw materials, in 2022 their top imports were Soybean Oil, Rubber Tires, and Pre-Packaged Medications, with a majority being purchased from China ($894M) (OEC, n.d.)

Technical Infrastructure

North Korea's overall connectivity is low, with approximately 19% of households owning computers in 2017, however only 1% of households have access to Kwangmyong, and approximately 19% of citizens owning smartphones in 2018. Typically, the main access points for the federal intranet are located in schools, although even the schools without access now teach students about the internet and intranet. (Miles, 2018) (Insikt Group, 2024)

A defector told People for Successful Corean Reunification, *Pscore*, a South Korean human rights organization:

> *"I was taught about the World Wide Web, and even had to memorize it for an exam, but I only knew about the internet in theory... I knew it was a sort of network where you can search but didn't actually know what it was. "*

Reports have shown that a few dozen families connected to the Kim regime have unfettered access to the internet, while some government officials, researchers, and IT students have heavily supervised access, overall, this amounts to approximately three thousand people. While a large majority of connections are made through LAN networks, access for businesses and schools is done through Asymmetrical Digital Subscriber Line and Fiber-Optic connections, while many households still rely on Point-to-Point Protocol for their connection. (Burgess, 2023) (Park S., 2017)

Their internet infrastructure is limited to four Class-C IP ranges, through a connection from China. There is also a fifth Class-C range available should the need arise; this range is on loan from China Unicom Telecommunications Company and was the original access point before North Korea installed proper infrastructure. According to Trend Micro, satellite connections are also available in the DPRK, however, the legality of owning a dish is unknown and they may be restricted to certain groups. (Kropotov, Lin, Fyodor, & Hacquebord, 2017)

North Korean Threat Actors

Lazarus

The name “Lazarus” is often used as an umbrella term in public reporting for North Korean cyber threat actors operating North Korea’s Reconnaissance General Bureau. They are considered the be the most predominant cyber threat actors operating out of North Korea. Lazarus is believed to have been established in July 2009 when a series of coordinated distributed denial-of-service attacks directed at websites for major government agencies, news media companies and financial institutes were launched against the United States of America and South Korea. Originally believed to be a cybercriminal group acting independently, Lazarus has since been designated as a national threat actor, working in support of the North Korean Government. (Reuters, 2009) (MITRE, 2024)

Figure 1: APT Logo used for Lazarus (Vectra, n.d.)

Lazarus Motivations

In the beginning of their hacking campaigns, Lazarus primarily focused their attacks on South Korea and their government agencies. Due to this, it is believed their original motivation was their desire to disrupt communications and commit cyber espionage within South Korea. After their public breach of Sony Pictures in 2014, Lazarus’ motives became much more overt in their support for North Korea. Since then, the majority of the group's hacking operations have been targeting the financial sectors of various organizations around the world, with a particular focus on the cryptocurrency industry. These events are clear indications that the group's financial motives are increasing. (Behnke, 2023)

Sub-Groups Within Lazarus

There are believed to be at least 5 different sub-groups within Lazarus that help support the DPRK in espionage, financial gain and geopolitical disruption. These sub-groups are:

BlueNorOff	Focuses attacks on financial institutes. Involved in the creation of malware utilized in Lazarus' cyberattack on the Bangladesh Central Bank. (Kaspersky Labs, 2018)
Citrine Sleet	Focuses attacks on the cryptocurrency industry utilizing fake crypto-currency platforms and uploading malicious Python packages to GitHub posed as simple programs that would install Trojan malware on a user's machine. (Nelson, 2024)
AndAriel	Originally focusing on espionage and DDoS attacks, has recently moved to focusing on the creation and distribution of the Maui ransomware used to target healthcare institutes in May 2021. US DOJ has issued an indictment for North Korean national Rim Jong Hyok for his involvement in AndAriel's cyber operations. (Department of Justice, 2024)
TEMP.Hermit	A small sub-group of Lazarus is believed to be mainly focused on providing DPRK with espionage and destructive cyber attacks mainly targeting South Korea. Believed to share significant resources with BlueNorOff (Department of Health & Human Services, 2021)
Kimsuky	Focused on intelligence gathering on enemy nation states for DPRK through social engineering and waterhole attacks. Kimsuky is considered to be the Lazarus sub-group responsible for the creation of remote backdoor malware utilized in North Korea's cyber operations (Department of Health & Human Services, 2021)

Key Figures Within Lazarus

Operating under the safety of the North Korean government, there is little known about specific figures within Lazarus. In February 2021 the United States Department of Justice (DOJ) indicted 3 members of North Korea's intelligence agency, The Reconnaissance General Bureau, as key members who participated in Lazarus' hacking operations. (Cimpanu, 2021)

Park Jin Hyok – Born in the 1980's (Reported dates of birth in 1984 and 1981), North Korean state-sponsored computer programmer who was indicted in connection to his role in multiple Lazarus operations. Park is believed to be one of the programmers who created malware that Lazarus would utilize in their attacks. US DOJ has charged Park with conspiracy to commit wire fraud, bank fraud and computer fraud. Since Park's indictment, North Korea has denied his existence. (FBI, 2021)

Image 1: Park Jin Hoyk (FBI, 2021)

Jon Chang Hyok – Reported to be born in 1989, a North Korean state-sponsored hacker who was indicted in connection to his role in multiple Lazarus operations. Jon is believed to have been directly involved in the creation and distribution of the ransomware malware that Lazarus utilized to target numerous cryptocurrency exchanges. US DOJ has charged Park with conspiracy to commit wire fraud, bank fraud and computer fraud. (FBI, 2021)

Image 2: Jon Chang Hyok (FBI, 2021)

Kim Il - Reported to be born in 1994, a North Korean state-sponsor hacker who was indicted in connection to his role in multiple Lazarus operations. Kim is believed to have been directly involved in the creation and distribution of ransomware malware that Lazarus utilized in their cyber-heist on international financial institutions. Kim is considered to have led Lazarus' development and marketing of the "Marine Chain Token" cryptocurrency offering that DPRK used to control interest in marine shipping vessels and evade US sanctions. (FBI, 2021)

Image 3: Kim Il (FBI, 2021)

Rim Jong Hyok – North Korean military intelligence officer and believed member of Lazarus sub-group AndAriel. An indictment for Rim's arrest was issued in July 2024 for conspiracy to computer hacking, and money laundering in connection to AndAriel's creation and use of the "Maui" ransomware. Which was used to gain unauthorized network access and extort ransoms on US healthcare facilities and companies as early as May 2021. (FBI, 2024)

Image 4: Rim Jong Hyok (FBI, 2024)

Common Attack Techniques

Spear-Phishing & Social Engineering

A large number of North Korean attacks stem from spear-phishing attacks on desirable companies' employees, typically in the form of emails regarding investments, job postings, or payroll errors; and social media posts that would attract their target. (CTIIC, 2023)

Insider Attacks

North Korea will send IT-trained workers abroad to get jobs as contractors with notable companies that may hold classified data, such as government agencies, IT companies, architectural and engineering firms, and law firms. Once they gain access to the data it is exfiltrated to North Korea. Another facet of these operations is if the operative gains access to the accounting department of a company, it may be used to aid money laundering and cryptocurrency transfer in and out of the country. (CTIIC, 2023)

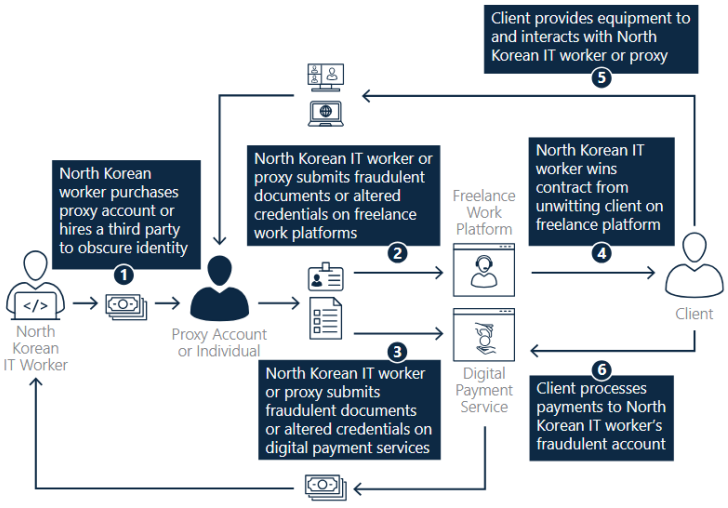

Figure 2: Demonstration on North Korea Threat Actor Insider Attack (CTIIC, 2023)

Use of Vulnerabilities & Exploits

In order to facilitate many of these operations, the North Korean government will develop their own or purchase malware and exploits from brokers such as the Shadow Brokers, a brokerage that's believed to have ties to Russia, to gain access or establish persistence in the victim's systems. North Korean threat actors are well known for using zero-day vulnerabilities in their attacks, as well as the entire suite of stolen NSA exploits that were leaked by Shadow Brokers. (CTIIC, 2023)

Notable Hacking Operations

2009 and 2013 DDoS Attacks

Believed to be the first major operation conducted by North Korea-backed threat actors. Over the span of 5 days in July 2009, there were three waves of Distributed Denial of Service (DDoS) attacks on websites that were owned by government agencies and financial institutions in both the USA and South Korea. Websites that were attacked include ones owned by the White House, the Pentagon, the New York Stock Exchange and the NASDAQ in the United States and the Blue House, the Ministry of Defence, the National Intelligence Service and the National Assembly in South Korea. (Zetter, 2009)

During the second wave of DDoS attacks, cybersecurity researchers reported that the attackers were utilizing a newly created Trojan, titled "Dozer", to compromise various machines around the world. Attackers were then able to remotely take control of multiple compromised computers as a botnet to conduct the DDoS attacks. Director of Malware Research, Joe Stewart, at cybersecurity firm SecureWorks reported that his review of the code used to create the Dozer trojan indicated that it was created just the day before attacks began, it appeared to have been written based on a Korean-language browser and it reused code from the previously know worm "Mydoom". (Zetter, 2009)

By October 2009, the South Korean National Intelligence Service (NIS) announced they had confirmed North Korea as responsible for the DDoS attacks. NIS was able to link attacks to North Korea through a Chinese IP address that was used in the attack that was also rented by the North Korean Ministry of Post and Telecommunications. (Reuters, 2009)

The Blue House in South Korea was targeted by North Korean threat actors again in June 2013. Hackers utilized the trojan/wiper malware known as "DarkSeoul" to target The Blue House's website with a DDoS attack. Taking down the agency's website and replacing it with a pro-DPRK defacement page. While the website was hacked, attackers were able to collect information on any site users, which led to the release of personal information on

roughly 220 thousand people, 100 thousand of whom were ordinary South Korean citizens. (Hyeon-Seop & Yeo-Bin, 2018)

Similar to the DDoS attacks that occurred in 2009, South Korea's NIS was able to link this attack to an IP address associated with the attacker that had been previously utilized in previous cyber operations by North Korean threat actors. Both attacks from 2009 and 2013 were later attributed to Lazarus as the group's cyber operations became more understood. (BBC, 2013)

Sony Pictures Breach

Lazarus operating under the alias "Guardians of Peace" (GOP) utilized a variant of the "Shamoon" wiper malware to compromise the network of Sony Pictures Entertainment (SPE). SPE was made aware of the breach on November 24th, 2021, when the malware used by Lazarus took down numerous computers used by SPE's employees and the GOP deface page was uploaded to their network. Lazarus' breach of SPE was done in response to the movie studio's decision to release the comedy movie "The Interview". In which a fictional talk show host is invited to North Korea to interview the country's leader, Kim Jong Un, while the talk show host is also approached by CIA agents requesting his help in an assassination attempt on Kim Jong Un during his trip. (Zetter, 2014)

The hackers claimed to have had access to the SPE network for over a year and have stolen over 100TB. In the days following the breach, Lazarus began leaking the stolen data online, releasing roughly 200GBs of stolen data over the span of 9 "data dumps". This data included personal information on roughly 4,000 SPE employees, executive's emails, screenplay and information regarding future movie plans, along with full videos of unreleased movies. Lazarus's breach SPE is considered the 4th most costly data breach in history. (Zetter, 2014) (Firmex, n.d.)

Bangladesh Central Bank Cyber-Heist

In February 2016, Lazarus was reportedly behind a series of cyberattacks on multiple international banks. By using malware, they were able to exploit a vulnerability in the network of the Bangladesh Central Bank. Lazarus was able to gain control of the bank's SWIFT Alliance Access (SAA) software, the main communication software utilized by numerous international banks to initialize financial transfers. Once the hackers had access to this internal tool, they used it to send fund transfer requests through SAA to other banks utilizing that software. Those banks, under the impression the SAA fund request was legitimate, would then send the funds to bank accounts controlled by Lazarus. Compared to typical data breaches that often include customer information, this method of attack has the potential to be much more destructive by allowing the hackers to take control of entire bank payment channels. (Riley & Mullen, 2016)

The cyber heist occurred between February 4th and 5th in 2016 Using compromised SAA credentials, Lazarus initiated thirty-five different fund transfer requests totalling $951 million from the Bangladesh Bank's account with the Federal Reserve Bank of New York. The funds were requested to be deposited into bank accounts located in the Philippines and Sri Lanka. Thirty of the thirty-five requests, totaling $851 million were flagged for bank staff review but the remaining five requests went through. A $20 million transfer to a Sri Lankan bank account was able to be recovered after the request by Deutsche Bank due to the misspelling of a false non-governing organization "Shalika Foundation". Hackers having misspelled "foundation" as "fundation". The four remaining Philippine transfers were completed, with a total of $81 million being deposited into personal bank accounts in the Philippines. (Aneez, 2016)

The United States National Security Agency (NSA) reported that the malware and hacking methods utilized by Lazarus in their 2014 Sony Breach were similar to those utilized to conduct the cyber heist on the Bangladesh Central Bank and attributed the attack to the North Korean state actor. This is considered the first time a nation-state threat actor utilizing their cyber attacks to steal funds. (Groll, 2017) (Reuters, 2017)

WannaCry Ransomware Attack

In May 2017, Lazarus conducted one of the largest ransomware attacks in history using a ransomware crypto-worm malware named “WannaCry”. This malware utilized an exploit for Windows known as “EternalBlue” that used a vulnerability in Windows Server Message Block protocol to remotely execute code on a target computer. Once a target computer is compromised, WannaCry installs the backdoor tool known as “DoublePulsar” to provide the attackers access to the compromised machines. After the backdoor was installed, WannaCry checks if the machine is already part of the host domain name. If the name is not found, WannaCry encrypts all data on the computer, modifies security configurations to hide its nefarious activity, and then deletes shadow copies of data. When a victim tried to use a compromised machine, they would be met with a payload message informing them of the attack and demanding payment of roughly $300-$600 in Bitcoin. WannaCry had three hardcoded bitcoin addresses included in its payload message, meaning the same three bitcoin wallets were used in all WannaCry attacks. (Goodin, 2017) (Brenner, 2017)

Since WannaCry utilized the EternalBlue SMBv1 exploit it was able to spread at a rapid rate, infecting over 300,000 computers around the world in the span of seven hours. Many of its victims are large corporations and government agencies. A total of three-hundred-twenty-seven payments were paid to the hard-coded bitcoin wallets from WannaCry’s ransom note, totaling over $130 million. It’s reported by cyber-risk analyst firm, Cyence, that damages from the hack potentially cost its victims $4 billion. WannaCry’s spread was ended when cybersecurity researcher Marcus Hutchins discovered the domain the crypto-worm used to determine if a machine had been affected or not was unregistered. Hutchins registered the domain which in turn caused the worm to stop spreading. The next day Microsoft issued a security update for many of its operating systems that patched the SMBv1 vulnerability WannaCry exploited to conduct its attack, to protect against WannaCry and other similar ransomware attacks. (Collins, 2017) (Berr, 2017) (ABC News, 2017) (Warren, 2017)

Multiple cybersecurity firms quickly found similarities in the code of WannaCry and the that of malware utilized by Lazarus in the previous hacking operations. By December 2017, The White House publicly acknowledged North Korea's involvement in the cyber-attack following the result of both an NSA and a CIA-led investigation linking the attack to Lazarus. At the time of the press release Homeland Security Advisor, Thomas Bossert, claimed the US government had gathered evidence that indicated Kim Jong Un authorized the release of WannaCry. (Solon, 2017) (Uchill, 2017)

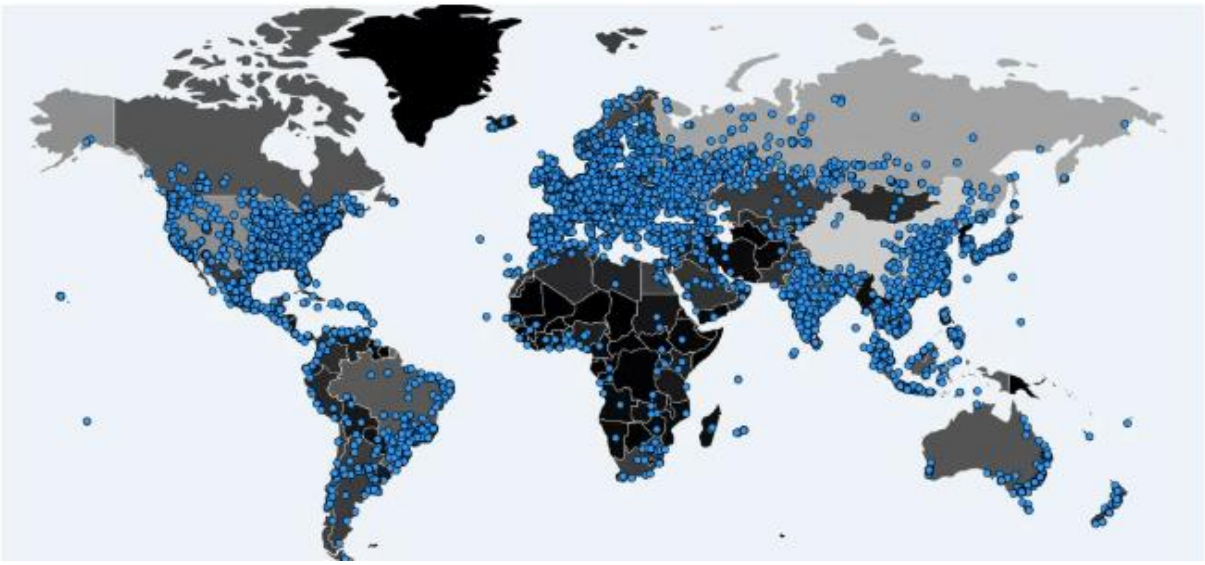

Figure 3: World map showcases where computers affected by WannaCry were located (Chappell, 2017)

2020-2021 Spear-Phishing Attacks

In November 2020, it was reported that members of Lazarus attempted a spear-phishing attack on a number of employees at the British pharmaceutical company AstraZeneca. While posing as job recruiters, the attackers would reach out to notable employees under the guise of providing a job offer. They would send their target documents that appeared as job descriptions but would also contain malware designed to install a backdoor to allow the attackers unauthorized access to the machine. Lazarus's spear-phishing operation on AstraZeneca targeted staff that were currently working on COVID-19 vaccine research but has been reported to have been unsuccessful. (Stubbs, 2020)

While the attempted breach of AstraZeneca was unsuccessful. Lazarus's focused attack on a healthcare/pharmaceutical-related target matched similar cybercrime trends seen during the COVID-19 pandemic. When both state-backed threat actors and cybercriminals targeted these industries at much higher rates than in previous years. These attackers hope to either demand high ransoms for any stolen public data or cause destructive damage to the healthcare systems of those they deem hostile nations. (Stubbs, 2020)

Lazarus began conducting a similar spear-phishing attack, focused on cybersecurity researchers at both Microsoft and Google in January 2021. Posing as software developers looking for insight or help with possible software vulnerabilities, members of Lazarus would target employees at both companies looking for help or offering to collaborate. The attackers would try to get the victim to download an attachment or visit a blog owned by the attacker that would compromise these employees' machines. (Newman, 2021)

Google did release a statement that confirmed researchers at their organization were compromised, but they did not specify an exact number. After reviewing the malware utilized in the attack Kaspersky Lab researcher, Costin Raiu, noted its similarity in that of the malware known to be utilized by Lazarus in their previous hacking operations. (Newman, 2021)

Cryptocurrency-Focused Attacks

In recent years, Lazarus' hacking operations have often targeted organizations operating within the cryptocurrency industry. By utilizing the lack of industry regulations, along with the anonymity provided under cryptocurrency transactions. It was reported by blockchain security firm Immunefi that crypto theft contributed by Lazarus from 2021-2023 totalled roughly $1.9 billion, with $308.6 million of that total coming from five successful attacks in 2023. Immunefli reported that Lazarus' crypto-theft operations contributed to over 16% of all reported cryptocurrency thefts that occurred in 2023. (Immunefi, 2023)

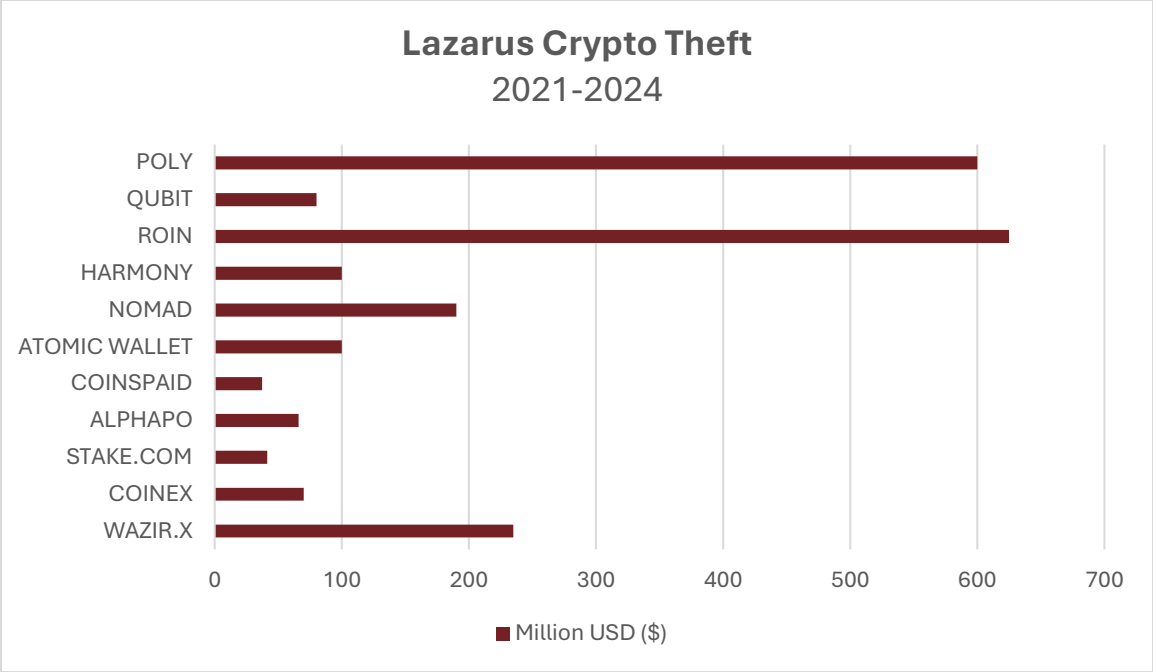

Chart 5: Lazarus crypto theft from 2021-2024 and their victims (Immunefi, 2023)

Poly Network

In August 2021, the decentralized cryptocurrency exchange Poly Network reported that an unauthorized user had gained access to their networks and had transferred roughly $610 million in cryptocurrency to three external wallet addresses. Attackers had utilized a vulnerability in the Ethereum cross-chain manager service Poly Network to conduct a brute-force attack that allowed them to reassign themselves as owners of specific crypto-wallets. Attackers could then funnel funds from the compromised wallets into their own

accounts. A review of this incident notes similarities between how this attack was conducted and previous attacks attributed to Lazarus, linking the North Korean threat actors to this hack. (Gagliardoni, 2021)

Qubit Blockchain Bridge

In January 2022, Lazarus discovered a vulnerability in the South Korean-based Qubit protocol on the cross-bridge blockchain protocol associated with Ethereum. Attackers used an exploit that allowed them to mint qXETH, the assent used to represent Ether that is bridged with Ethereum blockchain without limits. The attackers then used the unbacked qXETH to transfer roughly $80 million in cryptocurrency to the crypto mixer known as Tornado Cash to help with laundering the stolen funds back to accounts owned by the attacker. The utilization of Tornado Cash has been largely attributed to North Korean threat actors, linking the attack on the Qubit Blockchain Bridge to Lazarus. (Chainalysis, 2023)

Axie Infinity (Ronin Network)

In March 2022, hackers stole over $615 million worth of cryptocurrency from the online NFT-based game Axie Infinity. The hack was later linked to the North Korean nation-state actors operating for Lazarus. Similar to previous Lazarus' contributed breaches like AstraZeneca, Lazarus was able to compromise an engineer working with the developer of Axie Infinity, Sky Mavis, by posing as job recruiters. the attackers sent a PDF presented as a job description that was laced with malicious code. Once the engineer opened the PDF on his work computer, the attack chain started that was able to penetrate the Ronin system, the Ethereum-linked sidechain that was used to support the minting of NFTs within Axie Infinity. Sky Mavis had to raise additional venture capital in order to reimburse any users affected by the hack. (Toulas, 2022) (Kharif, 2022)

Harmony Horizon Blockchain Bridge

In June 2022, Lazarus utilizing an exploit similar to the one they used to hack the Qubit cross-bridge blockchain, compromised the Horizon cross-bridge protocol that connected the cryptocurrency exchange Harmony with the blockchain of Ethereum, Binance Chain and Bitcoin. Through this hack, Lazarus was able to steal roughly $100

million worth of cryptocurrency, which was laundered back to the DPRK government through Tornado Cash. (Lutz S. , 2022)

Nomad Blockchain Bridge

Lazarus continued their attack on major cryptocurrency bridge protocols in August 2022. Hackers exploited the Nomad Bridge protocol, that connects the cryptocurrency exchange Moonbeam to the Ethereum blockchain, stealing roughly $190 million in cryptocurrency. These funds were then laundered by Lazarus utilizing Tornado Cash. Shortly after this attack, the US Office of Foreign Assets Control (OFAC) blacklisted the use of Tornado Cash, resulting in the software's web domain being taken down and one of the software developers being arrested. (Bignell, 2022) (Calburn, 2022)

Atomic Wallet

In June 2023, members of Lazarus targeted the Estonia-based crypto wall server, Atomic Wallet. Hackers were able to compromise roughly 5,500 user-owned digital wallets, stealing roughly $100 million in cryptocurrency. Lazarus began laundering this money utilizing the crypto mixer Sinbad.io but once reports were released stating that attacks were being tracked, Lazarus switched to using the Russia-based crypto mixer Garantex in an attempt to disguise their identity. (Satter, 2023) (Immunefi, 2023)

CoinsPaid

In early July 2023, CoinsPaid, one of the largest cryptocurrency payment processing companies in the world, announced it experienced a cyber attack that resulted in the theft of over $37 million in cryptocurrency. CoinsPaid worked in collaboration with cybersecurity firm Match Systems to review the incident. Through this review, CoinsPaid was able to link the attack to Lazarus. Hackers reportedly spent roughly six months trying to compromise their corporate network through numerous methods including DDoS and brute-force attacks. It was determined that a spear-phishing attack on CoinsPaid employees by attackers posing as job recruiters is what resulted in the CoinsPaid security breach. (Kuzin & Krupyshev, 2024)

Alphapo

Alphapo is a large cryptocurrency payment processor that focuses its services on crypto-based gambling websites. In late July 2023, Alphapo became the victim of a cryptocurrency-focused attack conducted by Lazarus that resulted in the theft of roughly $60 million in cryptocurrency from “hot wallets”. Hot wallets are crypto wallets that are always connected to the internet, this allows the wallet owners to withdraw and deposit funds quicker than a more traditional “cold wallet”. Hot wallets are commonly used by crypto-based gambling websites to allow users to place bets at a rapid pace similar to how a customer would in a traditional brick-and-mortar casino. Unfortunately, due to them being permanently connected to the internet hot wallets are not as secure as cold wallets. Alphapo did not state how Lazarus was able to compromise these wallets, but it is believed that it was done through the use of leaked private keys that Alphapo used to manage user’s hot wallets. (Solimano, 2023)

Stake.com

In September 2023, the Lazarus group hacked the Stake.com casino platform and was able to steal over $41 million worth of cryptocurrency. The hackers were able to steal $15.7 million in Ethereum and $25.6 million in Binance Smart Chain and Polygon. The hackers used social engineering and malware to target employees of Stake.com. The co-founder of Stake.com, Edward Craven, said that the hack did not happen because of the hackers gaining access to the private keys. The hack targeted user’s cryptocurrency wallets through the platform. The hackers were able to gain access to the hot wallets through a combination of phishing scams to download malware, and the private key leak. (Toulas, 2023) (Avan-Nomayo, 2023)

CoinEx

Hong Kong-based cryptocurrency exchange, CoinEx, announced the crypto hot wallets used to store the entire exchange’s crypto assets had been compromised resulting in the theft of roughly $70 million of the exchange's total assets. Blockchain research firm,

Elliptic, stated after their review of the incident that a number of factors indicate that Lazarus is responsible for the attack. (Howcroft & Satter, 2023)

WazirX

In July 2024, the Indian cryptocurrency exchange and trading company, WazirX, had a major hack against their company. The hack was worth $235 million of WazirX's assets. The figure above shows how much cryptocurrency was lost in the attack. The hackers were able to take 59 thousand Ethereum. The attackers used Tornado Cash to switch the cryptocurrency over to cash. The North Korean hackers were able to use an exploit through Liminal which is the software that deals with digital assets and crypto. This exploit allowed them to transfer the funds out of the WazirX wallet. (Elliptic, 2024) (The Hindu Bureau, 2024) (Innowave, 2024)

North Korea's Allied Nation States

China

Dating back to 1961, North Korea had signed a treaty of friendship, cooperation, and mutual assistance with China. This treaty is still in effect and was renewed for another twenty years back in 2021. However, the treaty may not survive through the extension as North Korea continued the development of their nuclear weapons program against the wishes of China. (Vu, 2021)

Image 5: DPRK Leader Kim Jong Un meets with President of China, Xi Jinping (Rauhala & Fifield, 2018)

China's support for North Korea started during the Korean War from 1950-1953. China has helped North Korea with political and economic backing since Kim Il Sung was in office. In 2015, China opened a container shipping route along the border to boost the exports of Coal from North Korea to China. A 1961 treaty says that Beijing is forced to come to Pyongyang's defence if there is unprovoked aggression. The Chinese government tried to get this revoked, and they decided to stay neutral instead of abiding by the treaty. (Fong, 2024)

The relationship between China and North Korea has deteriorated as North Korea keeps testing ballistics under the control of Kim Jong Un. North Korea has launched ballistic missile tests while China was having high-profile events like the BRICS Summit. North Korea has been heavily dependent on China for its economy. The trade value from China takes up 90% of North Korea's total food and energy imports. China had a 2.3-billion-dollar trade with North Korea that accounted for nearly all North Korea's trade in 2023. (Chivvis & Keating, 2024) (Park, Swaine, & Russel, 2018)

Beijing also allowed North Korea to have some of the income from North Korean workers being sent over to China, even though the United Nations banned the practice.

Through this practice, North Korea would receive around five hundred million dollars annually. North Korea would then take this money and put it towards the ballistics and nuclear testing they did. China also exports millions of barrels of oil to North Korea illegally through ship transfers. When North Korea tested their ballistics in 2022, they aimed close to Japan to show China that they could be of use to them with their weapons because of the capacity to go long ranges (Chivvis & Keating, 2024)

Russia

North Korea and Russia are also allies. Their relationship was rocky, but because of the war in Ukraine, Pyongyang supplied Moscow with military equipment and ammunition in exchange for cash, the possibility of advanced military equipment and a rekindled security agreement. Russia has been dependent on North Korea for both supplies and soldiers to use against their war with Ukraine. Since September 2023, North Korea has reportedly sent Russia as many as five million artillery shells. This is a significant number considering estimates that Russia only has the capacity to make 2–3 million shells a year. Russia has used North Korean Kn-23/24 ballistic missiles in Ukraine, although the failure rate for these missiles is reportedly quite high. (Chivvis & Keating, 2024)

On April 25th, 2019, Kim Jong Un made a trip over to Russia for a summit with Vladimir Putin. This meeting took place on Russky Island in Vladivostok. This is the first time that Kim has travelled to Russia since Kim assumed office in 2011. At this summit, Putin mentioned how North Korea and Russia were talking about multilateral projects that would help the economies of both countries. Russia, like China, had North Korean labour workers, but they did not have the same abundance of workers in Russia that China did. Between 2017 and 2019, the amount of North Korean workers in Russia dropped from thirty thousand to ten thousand. Although Russia is the second most important

Image 6: DPRK Leader Kim Jong Un meeting with President of Russia Vladimir Putin (Associated Press, 2024)

economic partner to North Korea, it only amounts for 1 percent of the foreign trade. The main resource that Russia supplies to North Korea is refined petroleum products. (Kireeva & Zakharova, 2019)

Syria

Syria and North Korea have also had an allyship that originated during the Cold War. When North Korean pilots started fighting alongside the Syrian Air Force during the wars with Israel, starting the partnership between North Korea and Syria. Syria also used North Korea's reactor at the Yongbyon Nuclear Center as a template for their nuclear reactor that was located outside of Deir ez-Zor. When Israel struck the Al-Kibar nuclear site, it resulted in the death of ten North Korean scientists who were assisting in the construction of the reactor. Between 2012 and 2017, North Korea shipped forty batches of supplies that were used for chemical warfare and were also acid-resistant. Throughout the Syrian Civil War, Pyongyang had also supplied the capital of Syria with missile technology. (Ramani, 2021)

Cuba

On May 24th, 2016, North Korea's government and the Communist Party of Cuba had talks of strengthening the relationship between Pyongyang and Havana. The alliance between Pyongyang and Havana has stopped Cuba from diplomatically acknowledging South Korea even though Cuba has economic cooperation with Seoul. The reason that North Korea and Cuba had become allies was because of Kim Il Sung and Fidel Castro's ideological beliefs. Ernesto Guevara, who was one of Fidel Castro's closest followers, was very impressed by the industrial input of North Korea, and how the country had rebuilt itself after the American Invasion. Kim Il Sung had admired "Cuba's independent streak within the communist bloc." (Ramani, 2016) (Young, 2016).

Image 7: Former DPRK Leader Kim Il Sung with Former President of Cuba, Fidel Castro (Reddit, n.d.)

References

ABC News. (2017, May 10). *Ransomware cyberattack: Computer expert who blocked WannaCry virus says he's no hero.* Retrieved from ABC News: https://web.archive.org/web/20170517060218/http://www.abc.net.au/news/2017-05-16/ransomware-cyberattack-marcus-hutchins-gives-interview/8530574

Albert, E. (2020, June 17). *North Korea's Power Structure*. Retrieved from Council on Foreign Relations: https://www.cfr.org/backgrounder/north-koreas-power-structure

Aneez, S. (2016, March 31). *Sri Lankan in Bangladesh cyber heist says she was set up by friend*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-fed-bangladesh-sri-lanka-idUSKCN0WX1UI/

Apple, C. (n.d.). *All in the Family*. Retrieved from The Spokesman-Review: https://www.spokesman.com/stories/2020/apr/30/history-north-koreas-kim-dynasty/

Associated Press. (2024, June 17). *Putin to visit North Korea starting Tuesday for talks with Kim Jong Un*. Retrieved from NBC News: https://www.nbcnews.com/news/world/putin-visit-north-korea-kim-jong-un-rcna157463

Avan-Nomayo, O. (2023, September 5). *Stake co-founder says wallet keys 'not compromised' in crypto casino's $41m hack*. Retrieved from DL News: https://www.dlnews.com/articles/defi/stake-co-founder-says-hacker-did-not-compromise-private-keys/

BBC. (2013, July 16). *North Korea 'behind cyber attack' on South websites.* Retrieved from BBC News: https://www.bbc.com/news/world-asia-23324172

BBC. (2019, April 26). *North Korea profile - Timeline*. Retrieved from BBC News: https://www.bbc.com/news/world-asia-pacific-15278612

BBC. (2023, September 11). *Profile: North Korean leader Kim jong Un*. Retrieved from BBC News: https://www.bbc.com/news/world-asia-pacific-11388628

Behnke, R. (2023, October 16). *A History of the Lazarus Group, North Korea's Notorious Cyber Actors*. Retrieved from Halborn: https://www.halborn.com/blog/post/a-history-of-the-lazarus-group-north-korea-s-notorious-cyber-actors

Berr, J. (2017, May 16). *"WannaCry" ransomware attack losses could reach $4 billion*. Retrieved from CBS News: https://web.archive.org/web/20170614105447/http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Bignell, F. (2022, August 4). *Crypto Hackers Strike Again, Adding Solana and Nomad to the List of Victims*. Retrieved from The Fintech Times: https://thefintechtimes.com/crypto-hackers-strike-again-adding-solana-and-nomad-to-the-list-of-victims/

Brenner, B. (2017, May 17). *WannaCry: the ransomware worm that didn't arrive on a phishing hook*. Retrieved from Naked Security by Sophos: https://web.archive.org/web/20170711015125/https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/

Britannica. (2024, July 4). *Kim Il-Sung; president of North Korea*. Retrieved from Britannica: https://www.britannica.com/biography/Kim-Il-Sung

Britannica. (2024, October 25). *Kim Jong Il: North Korean Political Leader*. Retrieved from Britannica: https://www.britannica.com/biography/Kim-Jong-Il

Burgess, M. (2023, June 8). *The Bizarre Reality of Getting Online in North Korea*. Retrieved from WIRED: https://www.wired.com/story/internet-reality-north-korea/

Calburn, T. (2022, August 10). *GitHub courts controversy by suspending Tornado Cash developers and reneging on cookie commitments*. Retrieved from The Register: https://www.theregister.com/2022/08/10/github_tornado_cookies/

Chainalysis. (2023, May 3). *The $80 Million Qubit Hack Likely the Work of North Korea-linked Cybercriminals*. Retrieved from Chainalysis: https://www.chainalysis.com/blog/qubit-hack-north-korea/

Chappell, B. (2017, May 15). *WannaCry Ransomware: What We Know Monday*. Retrieved from NPR: https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday

Chivvis, C. S., & Keating, J. (2024, October 8). *Cooperation Between China, Iran, North Korea, and Russia: Current and Potential Future Threats to America*. Retrieved from Carnegie Endowment of International Peace: https://carnegieendowment.org/research/2024/10/cooperation-between-china-iran-north-korea-and-russia-current-and-potential-future-threats-to-america?lang=en

Cimpanu, C. (2021, February 17). *US charges two more members of the 'Lazarus' North Korean hacking group*. Retrieved from ZD NET: https://www.zdnet.com/article/us-charges-two-more-members-of-the-lazarus-north-korean-hacking-group/

Clarke, C. (2024). *Command Economy: Definition, How It Works, and Characteristics*. Retrieved from Investopedia: https://www.investopedia.com/terms/c/command-economy.asp

Collins, K. (2017, May 12). *Watch as these bitcoin wallets receive ransomware payments from the ongoing global cyberattack.* Retrieved from Quartz: https://qz.com/982993/watch-as-these-bitcoin-wallets-receive-ransomware-payments-from-the-ongoing-cyberattack

Council on Foreign Relations. (2022, June 28). *North Korea's Military Capabilities*. Retrieved from Council on Foreign Relations: https://www.cfr.org/backgrounder/north-korea-nuclear-weapons-missile-tests-military-capabilities

Council on Foreign Relations. (n.d). *North Korean Nuclear Negotiations*. Retrieved from Council on Foreign Relations.

Crossing Borders. (n.d). *The North Korean Famine*. Retrieved from Crossing Borders: https://www.crossingbordersnk.org/the-north-korean-famine

CTBTO. (2006). *2006 DPRK Announced Nuclear Test*. Retrieved from Comprehensive Nuclear-Test-Ban Treaty Organization: https://www.ctbto.org/our-work/detecting-nuclear-tests/2006-dprk-nuclear-test

Democratic People's Republic of Korea. (2015). *Criminal Law of DPRK.* Democratic People's Republic of Korea.

Department of Health & Human Services. (2021, March 25). *North Korean Cyber Activity*. Retrieved from HHS Cybersecurity Program: https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf

Department of Justice. (2024, July 25). *North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers*. Retrieved from Office for Publuc Affairs: https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals

Department of State. (n.d.). *Korean War and Japan's Recovery*. Retrieved from Milestones in the History of U.S. Foreign Relations - Office of the Historian: https://history.state.gov/milestones/1945-1952/korean-war

Elliptic. (2024, July 18). *$235 million lost by WazirX in North Korea-linked breach*. Retrieved from Elliptic: https://www.elliptic.co/blog/235-million-lost-by-wazirx-in-north-korea-linked-breach

FBI. (2021, February 17). *Most Wanted: Jon Chang Hyok*. Retrieved from Federal Bureau of Investigation: Most Wanted: https://www.fbi.gov/wanted/cyber/jon-chang-hyok

FBI. (2021, February 17). *Most Wanted: Kim Il*. Retrieved from Federal Bureau of Investigation: Most Wanted: https://www.fbi.gov/wanted/cyber/kim-il

FBI. (2021, February 17). *Most Wanted: Park Jin Hyok*. Retrieved from Federal Bureau of Investigation: Most Wanted: https://www.fbi.gov/wanted/cyber/park-jin-hyok

FBI. (2024, July 24). *Most Wanted: Rim Jong Hyok*. Retrieved from Federal Bureau of Investigation: Most Wanted: https://www.fbi.gov/wanted/cyber/rim-jong-hyok

Firmex. (n.d.). *The 10 Most Expensive Data Breaches in Corporate History*. Retrieved from Touch Point by Firmex: https://www.firmex.com/resources/blog/the-10-most-expensive-data-breaches-in-corporate-history/#:~:text=1.,Buy%2C%20JPMorgan%20Chase%20and%20Target.

Fong, C. (2024, March 7). *The China-North Korea Relationship*. Retrieved from Council on Foreign Relations: https://www.cfr.org/backgrounder/china-north-korea-relationship

Gagliardoni, T. (2021, August 12). *The Poly Network Hacker Explained*. Retrieved from Kudelski Security Research: https://research.kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained/

Goodin, D. (2017, May 12). *An NSA-derived ransomware worm is shutting down computers worldwide.* Retrieved from ARS Technica: https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/

Groll, E. (2017, March 21). *NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist*. Retrieved from Foreign Policy: https://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/

Ha Lee, J., & Ick Lew, Y. (n.d). *History of North Korea* . Retrieved from Britannica: https://www.britannica.com/topic/history-of-North-Korea

Harden, B. (2009, December 2009). *North Korea revalues currency, destroying personal savings*. Retrieved from Washington Post: https://www.washingtonpost.com/wp-dyn/content/article/2009/12/01/AR2009120101841.html?hpid=moreheadlines

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

Horschig, D. (2024, July 31). *How Are Cyberattacks Fueling North Korea's Nuclear Ambitions?* Retrieved from Center for Strategic & Internation Studies: https://www.csis.org/analysis/how-are-cyberattacks-fueling-north-koreas-nuclear-ambitions

Howcroft, E., & Satter, R. (2023, September 15). *Blockchain analysts suspect North Korea-linked hackers behind $70 million crypto theft*. Retrieved from Reuters: https://www.reuters.com/technology/blockchain-analysts-suspect-n-korea-linked-hackers-behind-70m-crypto-theft-2023-09-15/

Hyeon-Seop, H., & Yeo-Bin, L. (2018, March 24). *North Korea's Cyber Attacks and Our Cyber Security Situation.* Retrieved from Ministry of Unification of The Republic of Korea: https://blog.naver.com/gounikorea/221236005588

IAEA. (n.d.). *Fact Sheet on DPRK Nuclear Safeguards*. Retrieved from Internation Atomic Energy Agency: https://www.iaea.org/newscenter/focus/dprk/fact-sheet-on-dprk-nuclear-safeguards

Immunefi. (2023, December). *Lazarus Group Report*. Retrieved from Immunefi: https://downloads.ctfassets.net/t3wqy70tc3bv/EhGU8jztu6R938dcMfI9Q/b8e6bf8f6bdba576e547875abd916414/Immunefi_Lazarus_Group_Report.pdf?utm_source=immunefi

Innowave. (2024, July 31). *North Korea behind $230M WazirX Hack*. Retrieved from Innowave: https://innowave.tech/north-korea-behind-230m-wazirx-hack/

Insikt Group. (2024, July 18). *Despite Sanctions, North Koreans Continue to Use Foreign Technology.* Retrieved from Recorded Future: https://www.recordedfuture.com/research/north-koreans-continue-to-use-foreign-technology

Kaspersky Labs. (2018). *Lazarus Under The Hood.* Russia: Kaspersky Labs.

Kharif, O. (2022, June 23). *Axie-Infinity Developer to Reimburse Hack Victims, Restart Ronin*. Retrieved from Bloomberg: https://web.archive.org/web/20221206052254/https://www.bloomberg.com/news/articles/2022-06-23/axie-infinity-developer-to-reimburse-hack-victims-restart-ronin

Kim, J. (2024, October 10). *North Korea's Kim lauds 'longest ruling party' on anniversary with Russian guests*. Retrieved from Reuters: https://www.reuters.com/world/asia-pacific/north-koreas-kim-lauds-longest-ruling-party-anniversary-with-russian-guests-2024-10-10/

Kireeva, A., & Zakharova, L. (2019, April 26). *Takeaways From the Long-Awaited Russia-North Korea Summit*. Retrieved from The Diplomat: https://thediplomat.com/2019/04/takeaways-from-the-long-awaited-russia-north-korea-summit/

Kropotov, V., Lin, P., Fyodor, Y., & Hacquebord, F. (2017, October 17). *A Closer Look at North Korea's Internet*. Retrieved from Trend Micro: https://www.trendmicro.com/en_ca/research/17/j/a-closer-look-at-north-koreas-internet.html

Kuzin, E., & Krupyshev, M. (2024, February 7). *The CoinsPaid Hack Explained: We Know Exactly How Attackers Stole and Laundered $37M USD*. Retrieved from CoinsPaid.

Lee, T. B., & James, E. S. (2015, June 3). *The 2014 Sony hacks, explained*. Retrieved from VOX: https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

Lutz, S. (2022, June 29). *North Korean Attackers Behind $100M Harmony Hack: Report*. Retrieved from Decrypt: https://decrypt.co/104138/north-korean-attackers-behind-100m-harmony-hack-report

Lutz, T. (2015). *Cult of Personality: North Korea under Kim Il-Sung*. Retrieved from Senior Capstone Theses: https://scholarworks.arcadia.edu/cgi/viewcontent.cgi?article=1011&context=senior_theses

Miles, T. (2018, June 20). *Tackling North Korea's chronically poor sewage 'not rocket science' - U.N.* Retrieved from Reuters: https://www.reuters.com/article/world/tackling-north-koreas-chronically-poor-sewage-not-rocket-science-un-idUSKBN1JG2RH/

Ministry of Foreign Affairs of Japan. (1972). *Situation in the Korean Peninsula*. Ministry of Foreign Affairs of Japan.

Ministry of Unification of the Republic of Korea. (1972). *The July 4 South-North Joint Communiqué*. Peacemaker.

MITRE. (2024, April 11). *Lazarus Group*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/groups/G0032/

Muncaster, P. (2023, June 5). *North Korea Makes 50% of Income from Cyber-Attacks: Report*. Retrieved from Infosecurity Magazine: https://www.infosecurity-magazine.com/news/north-korea-makes-50-income/

Murray, L. (2024, Novemeber 22). *Kim Jong-Un: North Korean Political Official*. Retrieved from Britannica: https://www.britannica.com/biography/Kim-Jong-Eun

Nelson, N. (2024, September 20). *Citrine Sleet Poisons PyPI Packages With Mac & Linux Malware*. Retrieved from Dark Reading: https://www.darkreading.com/threat-intelligence/citrine-sleet-poisons-pypi-packages-mac-linux-malware

Newman, L. H. (2021, January 26). *North Korea Targets—and Dupes—a Slew of Cybersecurity Pros*. Retrieved from WIRED: https://www.wired.com/story/north-korea-hackers-target-cybersecurity-researchers/

OEC. (n.d.). *North Korea*. Retrieved from Observatory of Economic Complexity (OEC): https://oec.world/en/profile/country/prk

Park, J., Swaine, M., & Russel, D. (2018, January 25). *Bitter Allies: China and North Korea*. Retrieved from Asia Society: https://asiasociety.org/new-york/events/bitter-allies-china-and-north-korea

Park, S. (2017, October 6). *North Korea (Korea, Democratic People's Republic of)*. Retrieved from Asia Internet History Projects: https://sites.google.com/site/internethistoryasia/country-region-information/north-korea-korea-democratic-peoples-republic-of

Ramani, S. (2016, June 7). *The North Korea-Cuba Connection*. Retrieved from The Diplomat: https://thediplomat.com/2016/06/the-north-korea-cuba-connection/

Ramani, S. (2021, March 23). *The North Korean-Syrian Partnership: Bright Prospects Ahead*. Retrieved from 38 North: https://www.38north.org/2021/03/the-north-korean-syrian-partnership-bright-prospects-ahead/

Rauhala, E., & Fifield, A. (2018, March 28). *Kim-Xi meeting presents a new challenge for Trump on North Korea*. Retrieved from The Washington Post: https://www.washingtonpost.com/world/asia_pacific/kim-xi-meeting-presents-a-new-challenge-for-trump-on-north-korea/2018/03/28/55e7e8a6-31f9-11e8-b6bd-0084a1666987_story.html

Reddit. (n.d.). *Kim Il-Sung & Fidel Castro*. Retrieved from Reddit: https://www.reddit.com/r/communism/comments/1btm94/kim_ilsung_fidel_castro/?rdt=37315

Reuters. (2009, October 30). *North Korea behind cyber attacks-South's spy chief*. Retrieved from Reuters: https://www.reuters.com/article/economy/north-korea-behind-cyber-attacks-souths-spy-chief-idUSSEO249027/

Reuters. (2017, March 23). *U.S. may accuse N. Korea in Bangladesh cyber heist - WSJ*. Retrieved from Reuters: https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN16T2Z3/

Riley, C., & Mullen, J. (2016, August 31). *Banks urged to tighten security as hacks continue*. Retrieved from CNN: https://money.cnn.com/2016/08/31/technology/swift-bank-hacks/index.html

Ryall, J. (2017, February 14). *Profile: Who was Kim Jong-nam, the exiled half-brother of North Korean dictator Kim Jong-un?* Retrieved from The Telegraph: https://web.archive.org/web/20170214164214/http://www.telegraph.co.uk/news/2017/02/14/profile-kim-jong-nam-exiled-half-brother-north-korean-dictator/

Satter, R. (2023, June 13). *North Korean hackers stole $100 million in recent cryptocurrency heist, analysts say*. Retrieved from Reuters: https://www.reuters.com/world/north-korean-hackers-stole-100-million-recent-cryptocurrency-heist-analysts-2023-06-13/

Sharma, A. (2024, November 21). *North Korea's Cyber Strategy: An Initial Analysis*. Retrieved from Observer Research Foundation: https://www.orfonline.org/research/north-korea-s-cyber-strategy-an-initial-analysis#:~:text=Unlike%20nuclear%20assets%2C%20cyber%20capabilities,to%20augment%20its%20conventional%20capabilities.

Solimano, P. (2023, July 27). *North Korean Hacker Cell Lazarus Allegedly Behind $60M Alphapo Hack*. Retrieved from Decrypt: https://decrypt.co/150282/north-korean-hacker-cell-lazarus-allegedly-behind-60m-alphapo-hack

Solon, O. (2017, May 15). *WannaCry ransomware has links to North Korea, cybersecurity experts say.* Retrieved from The Garudian: https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group

Statista. (2024, October). *Countries with the lowest internet penetration rate as of October 2024*. Retrieved from Statista: https://www.statista.com/statistics/725778/countries-with-the-lowest-internet-penetration-rate/

Stubbs, J. (2020, November 27). *Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca - sources.* Retrieved from Reuters: https://www.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no/exclusive-suspected-north-korean-hackers-targeted-covid-vaccine-maker-astrazeneca-sources-idUSKBN2871A2/

Talmadge, E. (2014, February 23). *North Korea: Where the Internet has just 5,500 sites*. Retrieved from Toronto Star: https://www.thestar.com/news/world/north-korea-where-the-internet-has-just-5-500-sites/article_c2a2f09a-eb09-539a-8d98-1d9f509eb088.html

The Hindu Bureau. (2024, September 4). *Stolen crypto from WazirX mostly converted to Ether and moved with Tornado Cash: Report*. Retrieved from The Hindu: https://www.thehindu.com/sci-tech/technology/stolen-crypto-from-wazirx-mostly-converted-to-ether-report/article68603898.ece

Toulas, B. (2022, July 12). *Hackers stole $620 million from Axie Infinity via fake job interviews*. Retrieved from Bleeping Computer: https://www.bleepingcomputer.com/news/security/hackers-stole-620-million-from-axie-infinity-via-fake-job-interviews/

Toulas, B. (2023, September 5). *Crypto casino Stake.com loses $41 million to hot wallet hackers*. Retrieved from Bleeping Computer: https://www.bleepingcomputer.com/news/security/crypto-casino-stakecom-loses-41-million-to-hot-wallet-hackers/

Uchill, J. (2017, December 2017). *WH: Kim Jong Un behind massive WannaCry malware attack.* Retrieved from The Hill: https://web.archive.org/web/20171222003927/http://thehill.com/policy/cybersecurity/365580-wh-kim-jong-un-ordered-release-of-disastrous-wannacry-malware

Vectra. (n.d.). *Lazarus Group*. Retrieved from Vectra: https://www.vectra.ai/threat-actors/lazarus

Vu, K. (2021, July 30). *Why China and North Korea decided to renew a 60-year-old treaty*. Retrieved from The Interpreter: https://www.lowyinstitute.org/the-interpreter/why-china-north-korea-decided-renew-60-year-old-treaty

Warren, T. (2017, May 13). *Microsoft issues 'highly unusual' Windows XP patch to prevent massive ransomware attack*. Retrieved from The Verge: https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack

Weaver, M. (2009, July 8). *Cyber attackers target South Korea and US*. Retrieved from The Guardian: https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack

World Bank Group. (n.d.). *Korea, Dem. People's Rep.* Retrieved from World Bank Group: https://data.worldbank.org/country/KP

Yeo, A. (2021, November 22). *North Korea is addressing the pandemic in its 'style.' That means leaving a lot of people hungry.* Retrieved from Brookings: https://www.brookings.edu/articles/north-korea-is-addressing-the-pandemic-in-its-style-that-means-leaving-a-lot-of-people-hungry/

Young, B. R. (2016, November 28). *Revolutionary Solidarity: Castro's cozy relationship with North Korea*. Retrieved from NK News: https://www.nknews.org/2016/11/revolutionary-solidarity-castros-cozy-relationship-with-north-korea/

Zetter, K. (2009, July 8). *Lazy Hacker and Little Worm Set Off Cyberwar Frenzy.* Retrieved from WIRED: https://web.archive.org/web/20090710221733/http://www.wired.com/threatlevel/2009/07/mydoom/

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