Electronic Journal of Social and Strategic Studies Volume 5 Issue 3
Date of publication: 31 Jan 2025 Dec 2024 – Jan 2025
DOI: https://doi.org/10.47362/EJSSS.2024.5304

North Korea's Cyber Weapons Capabilities: Impact on International Security

Siddharth Shankar[1]

Abstract

North Korea may be ranked among one of the poorest countries of the world in terms of its GDP growth but it still holds its relevance as a major power in the international world order, given the nuclear stockpile threat posed against the Western bloc led by the United States. North Korea's cyber capabilities has been characterized by opportunism. Till date, there is little evidence on North Korea having a nuclear doctrine. An analysis of the statements from the leadership suggests that North Korea has a mix of grandiose and conventional ideas on the aspect of cyber operations during military conflicts. The paper attempts to examine North Korea's cyber weapon capabilities and their potential implications for International Security through focus on three key operations – Kimsuky, Lazarus and Advanced Persistent Threat (APT) 37. These operations have targeted South Korea, parts of South Asia and the Pacific whose laggard cyber security mechanisms have borne heavy consequences. With regard to the diversification of cyber capabilities, the focus would be placed on North Korean regime's use of cyber espionage and malware applications across the Korean peninsula and in particular Japan and the United States. The application of case studies where the Korean regime – backed hackers were behind significant cyber operations, most of them fatal to the international security and order.

Keywords: North Korea, Cyber Espionage, Nuclear Doctrine, Malware Applications, Cyber Warfare, Opportunism, International Security

Introduction

North Korea may be ranked among one of the poorest countries of the world in terms of its GDP growth but it still holds its relevance as a major power in the international world order, given the nuclear stockpile threat posed against the Western bloc led by the United States.

[1] Siddharth Shankar is an Independent Researcher. He is a Postgraduate in Geopolitics and International Relations from Manipal Academy of Higher Education, Manipal, India.

DOI: https://doi.org/10.47362/EJSSS.2024.5304

North Korea's cyber capabilities has been characterized by opportunism. Till date, there is little evidence on North Korea having a nuclear doctrine. An analysis of the statements from the leadership suggests that North Korea has a mix of grandiose and conventional ideas on the aspect of cyber operations during military conflicts. The paper attempts to examine North Korea's cyber weapon capabilities and their potential implications for International Security through focus on three key operations – Kimsuky, Lazarus and Advanced Persistent Threat (APT) 37. These operations have targeted South Korea, parts of South Asia and the Pacific whose laggard cybersecurity mechanisms have borne heavy consequences.

With regard to the diversification of cyber capabilities, the focus would be placed on North Korean regime's use of cyber espionage and malware applications across the Korean peninsula and in particular Japan and the United States. The application of case studies where the Korean regime – backed hackers were behind significant cyber operations, most of them fatal to the international security and order.

Relevance for North Korea to develop Cyber Weapons Capability

The Democratic Republic of Korea under the leadership of Kim Jong-Un has been categorised as one of the poorest countries of the international world order with the least wired connectivity worldwide and highly prone to the maintenance of all forms of 'distancing' – social, economic, political as well as cultural among the global political institutions that have attempted to shape the movement as well as track the agenda of collective progress of the international order. North Korea is considered as the odd one out of the pack, with having made no attempts to interact with the international order in a diplomatic manner.

However, North Korea's cyber capability has been highly attributed in the present world order with an increasing number of cyber operations having been linked to the Kim Jong-Un regime in Pyongyang, with the level of sophistication of each operation and their concerned cyber-attack having had widespread implications across the current world order. It may be stated that the geopolitical theory of cyber power is the standard theoretical framework that may be applied to our present study. According to the Joseph Nye –

> "*Power is dependent on the context. Cyber power is the theory that depends on the resources that characterise the operational domain framed by use of electronics to*

Date of publication: 31 Jan 2025 Dec 2024 – Jan 2025
DOI: https://doi.org/10.47362/EJSSS.2024.5304

> *exploit information through interconnected systems and their associated infrastructure*" (Nye, Jr May 2010).

This has left some scholars to maintain that cyber weapon operations have continued to be North Korea's sole export of its soft power in the current age of complex interdependence and highly connected multilateral world order. Among the key reasons for the regime to continue towards the sponsor of cyber espionage operations are three-fold in their nature as well as their applicability.

Firstly, to cause worldwide disruption and chaos. Cyberspace is one such domain where a majority of the 197 countries maintain their connectivity with the occurrences across the world, with the World Wide Web platform having the common reach among the global order of nations. In the 21st century world, large amounts of data on national security interests are heavily secured in encrypted formats located in the sub-critical realm known as the cyberspace. This data is often transferred among the allied countries for their analysis on the same which then may be called as 'critical information'. When the information is tempered by a third-party, rogue state it may spread international chaos and global disruption.

Secondly, to conduct espionage. Espionage is the phenomenon where an individual or a group is allocated for the purpose of long-term spying on critical infrastructures whose information may possess greater value for the beneficiaries in the areas of defence, security and their larger national interests. North Korea maintains three key methods – informational, financial as well as disruption espionage, respectively.

Lastly, to generate revenue in order to sponsor its future operations. There have been past instances where the North Korean-attributed hackers have often found to have made their operations successful in emptying the coffers of foreign national banks and their international reserves. This has been the most impacted cyber weapon application, although the least popular among the other methods of cyber weapon operations.

Examination of Cyber Weapons developed by North Korea

Cyber weapons warfare has emerged as another crucial dimension in the early 2010s where the new North Korean regime under Kim Jong-Un (2011) had spearheaded the idea and approach in the state-sponsorship to homegrown cyber hacker groups. This method had found to be

DOI: https://doi.org/10.47362/EJSSS.2024.5304

adopted given the large influx of data on the Korean peninsula, especially information that may pertain to the national security interests on the military modernisation at the 38th Parallel ceasefire zone. These groups are often identified to operate at foreign locations diffused across the wide world but are observed to have a commonality to utilise the attributed North Korean IP-addresses in order to complete their cyber espionage operations.

Cyber campaigns have the capability to easily confuse the potential targets and have the tendency to create a sense of vulnerability in the receiver systems, thereafter the disruption caused is the resultant from an immediate consequence from the concerned operations. North Korea's cyber weapons capabilities have continued to be a major security threat in the cyber-physical space; a convergent area that connects the real and the virtual world.

Among the three key cyber weapons capability which includes malware, ransomware and denial of service (DoS) attacks. The present study attempts to identify and keenly learn and produce an analysis on North Korea's cyber weaponisation with the use of Denial of Service (DoS) attacks (m.-h. Kim February 2022). Denial of Service attack is a phenomenon in which a malicious actor attempts to render a computer or other device unavailable to its intended users through the aspect of interruption of the device's normal functioning capabilities (Suh, North Korea's Cyber Capabilities and Strategy 2022).

North Korea's Cyber Weapons Capability: Denial-of-Service Attacks as a Case in point

With having set the background behind Norh Korea's nature, relevance as well as the categories of cyber weapons which have been deployed till date, this section of the paper would arrive at North Korea's utilisation of one such cyber weapon capability – the Denial-of -Service attacks. This has found prominence in secondary sources that have traced the country's recent past replete with examples that showcase the weapon as a go-to tool for the top leadership in order to demonstrate their technological might to create minor, yet selected distractions.

Yet, these distractions may be categorised as North Korea's soft power in the international order. Denial-of-Service has been one such cyber weapon that the state leadership has found to indirectly implement through state-sponsored hackers that target the hit-list given by the regime. Since 2012, the data on Denial-of-Service attacks have been found consistent ever since Kim Jong-Un has risen to power.

Date of publication: 31 Jan 2025 Dec 2024 – Jan 2025
DOI: https://doi.org/10.47362/EJSSS.2024.5304

Among the key Denial-of-Service attacks, the paper would attempt to concentrate on three key operations sponsored by the North Korean regime – Operation Kimsuky, Lazarus and APT 37. Each of the enlisted operations would be analysed in detail to derive the geopolitical implications for the world order.

Operation Kimsuky

The morning hours of March 13, 2013 had been considered dreadful for Seoul and Beijing with the extensive ruckus created by their respective information technology and the foreign affairs ministries in their initial attempts towards the clarification and condition their external, public environment on the knowledge of the grave issue placed at their table. The operation was termed so given the mail accounts identified as *kimsukyang* and *kim asdfa* respectively had been successful in their conducts of cyber espionage to target 11 South Korean and 2 Chinese organisations, respectively.

A study revealed that the supposedly North Korean funded espionage group were to be targeted for the attack given the varied reasons to be justified in the subsequent paragraphs. This allegation had been proved to be true with the case having been studied and proved appropriate by a variety of leading cyberspace scholars across the globe.

The allegation framed by the victims were that the North Korean regime involved in an unsophisticated, yet a highly targeted campaign against the South Korean military as well as its subsidiary think tanks. In specific context, the targets included the Korea Institute for Defence Analysis, the Sejong Institute and the South Korean Ministry of Unification which goes to imply the respected domain specialisation being directly proportional to the North Korean national interests that would be reflected and subsequently affected in both the short as well as the long term (North Korean Advanced Persistent Threat Focus: Kimsuky 2020).

Another report by Kaspersky Labs, a Russia-based multinational cybersecurity and anti-virus firm, supports the South Korean allegation with their key findings. Among the findings came the choice of the targets – the Korea Institute for Defence Analysis and the Sejong Institute, both South Korean set of institutions that provide for primary research on national security, defence upgradation and stability as well as key regional security issues that may have a direct or indirect consequences for North Korean border security and their larger national interests. With the 38th Parallel also known as the Korean Demilitarized Zone (DMZ) having been a

DOI: https://doi.org/10.47362/EJSSS.2024.5304

contested issue for both the Koreas in close to 73 years, the larger North Korean mindset turned national interest has been to claim to discard the standstill agreement and proceed with the idea of a unified Korean peninsula.

This policy has been well reflected in Kim Jong-Un's regime with technology used as their instrument to create a Korean soft power of disruption that leads to chaos and instability with their southern neighbours and what better than targeting the 'new oil' of the 21st century, which is, data. The two think-tanks whose network clouds had stored enormous information processed by eminent research scholars had proved wholly resourceful for the Kim regime up North.

The Internet Protocol (IP) addresses were identified to be traced to the location of the Jilin Province as well as the Liaoning Province Network, both located in the Eastern Chinese division. Given the impact of the cyberattack extended to the Chinese as also the victims, it was very easy to link the program with North Korea, given the geographical proximity with the stated regions as a territorial boundary. There have been claims that the internet service providers that extend Internet accessibility in both the above stated Chinese provinces are believed to maintain lines across the North Korean territory, thereafter the strategic location of the regions may have played to the North Korean regime advantage.

The South Korean economy had recorded a damage of 800 billion won equivalent to US$750 million with the March 2013 North Korean DoS attack on the military institutions. This had contributed to a phase of tension within the South with the potential for reputational damage with their allies and trading partners being at risk, especially in matters of critical data sharing and storage of military data cloud. This aspect may be found adopted by their allied partners when observed the consistent inability of South Korean government in making efforts to tackle the threat in an aggressive manner.

Operation Lazarus

As mentioned in the previous section, North Korea has the capability towards pursuing three strategic objectives with its cyber operations which includes informational espionage, informational disruption and generation of finance. Operation Lazarus or commonly called as the Lazarus Group is another North Korean-state funded hacker group that had made its name in cyber warfare and cybersecurity concepts.

DOI: https://doi.org/10.47362/EJSSS.2024.5304

Among the major cyber operations that have been conducted to date, two have gained international significance and recorded widespread shockwaves in the international order. The two operations of the Group being the Bangladesh Bank Heist (2016) and the global WannaCry cyberattack (2017). Both these case points of cyber weapon operations would be analysed with details in the subsequent sections.

The Lazarus Group's cyber operations history may be traced to 2009 where they had targeted both the South Korean as well as the United States administration websites in attempt towards sparking informational espionage that leads to scenes that may leads to large-scale informational disruption and chaos among the domestic economy and political environment of the two countries. However, the Bangladesh Bank Heist was marked as the darkest moment in the history of cybersecurity as a model for country-wise adaptation against data theft protection. In February 2016, the Bangladesh Central Bank's morning hours were noted to be regular, with machine errors were projected to be 'normal' in function across the country's central bank whose primary responsibility lies in minting and circulation of Bangladesh's currencies (Park 2021).

The early working hours of the Bangladesh Bank were usually considered to be busy with diffused sounds of enormous paperwork that deals with tallying bank, money and currency receipts. The malfunction triggered by the Lazarus was therefore, considered to be a technical glitch in the bank's central computer command network given the mass utilisation of the software for the bank's daily chores. It was when a signal was alarmed through the release of a US Central Intelligence Agency report where it specified the root-cause of the malfunction was an innocuous mail with the attached malfunction that the Bangladesh Bank authorities were notified and made to cautiously act towards securing their financial stability network.

According to the post-heist studies on the case, there have been substantial claims that have clarified the aspect that in January 2015; exactly a year prior to the heist, a reference by the pen name "Rasel Ahlem" enclosed within an anonymous mail was directed to the Bangladesh Bank authorities, posing as a job seeker within the esteemed institution. The mail had directed the concerned authorities to download his so-called "CV template" enclosed along with a cover letter which had been identified as the initial point of entry for the virus into the computer network, disrupting their collective function altogether. In February 2016, the Lazarus were steadfast to act their mission with a year of observation into the key security regulations and

DOI: https://doi.org/10.47362/EJSSS.2024.5304

mechanism operated by the authorities that were considered paramount for the transfer of billions of dollars from the Bank's foreign accounts to various large beneficiaries.

The malfunction was enough to crack open the digitally (heavy) protected vaults, giving way for the transfer of $80 million out of the $1 billion scheduled transfer into multiple shell accounts. So, it had been traced that the hack was conducted at 20:00 hrs Bangladesh time and its reserves of close to 1 billion were placed with the US-Federal Reserve account. The study maintains that on February 4, 2016 when the Bangladesh central bank had closed for the night, the Lazarus had portrayed themselves as imposters of the central bank when they had directed instructions to the Federal Reserve to drain out $1bn to networks that lead to their control of the money inflow (The Lazarus heist: How North Korea almost pulled off a billion-dollar hack 2021).

When the Federal Reserve had attempted to contact the Central Bank channel, the Lazarus were successful in intercept the network of communication with the Bangladeshis being asleep and Friday and Saturday (the two subsequent days) reflected their version of 'weekend' (Park 2021). While the shocking news of confirmation mail was accounted on Saturday, the Feds were on weekend holidays until Monday. So it wasn't until Monday, the 8th of February 2016 that the Bangladesh Bank office was able to confirm the imposter threat notice with the Federal Reserve (M. Kim 2016).

With close to $101mn had crossed the network and into the untraceable imposter accounts. However, a single mistake had cost the Lazarus a remainder of $20mn in their efforts to accumulate the entirety of $1bn, with the $20mn having traced to have been directed to a charity mis-spelled "*Shalika Fundation*" to the original Shalika Foundation (Park 2021).

The Federal Reserve's eagle-eyed employees were able to reverse the request for transaction and thereafter the Bangladesh Central Bank's Fed account was credited with a mere reserve of $20mn aside from the original amount of $1bn in the Federal Reserve account.

Operation Advanced Persistent Threat 37

The North Korean cyber group, also widely known by the acronym APT37 have been described in the reports of security research scholars as uniquely distinctive and a far more obscure group in the aspect of a different techniques of hacking stored in their arsenal. The cyber-group also

DOI: https://doi.org/10.47362/EJSSS.2024.5304

going by the names of *ScarCruft* and *Group 123*, is a North Korean hacker group distinguished by its unique techniques and relatively obscure operations. According to security research reports, the group has built an extensive arsenal of hacking tools and methods, making it a prominent player in cyber warfare. Since its activities were first identified in 2014, APT37 has primarily focused in directing its cyber-attacks on South Korea, targeting military, governmental, and private entities.

Among its key operations is **Operation Golden Time** that occurred between August 2016 and March 2017. This campaign involved the use of decoy documents to exploit vulnerabilities during the download process and execute shell codes from compromised websites. These sophisticated techniques were directed at South Korean military administration entities, enabling the hackers to infiltrate systems and exfiltrate critical data (FireEye Incorporation, 2018).

The prominent North Korean cyber-group have been known for deploying custom malware to gain initial access and facilitate information espionage. The group has demonstrated a high degree of sophistication in its operations, employing tools such as **wiper malware** and leveraging vulnerabilities in commonly used software like **Flash Player** and **Microsoft Internet Explorer**. Additionally, APT37 has been identified as capable of stealing credentials and sensitive data directly from web browsers.

Operating in secrecy, APT37 continues to pose a significant threat in the cyber domain. Its advanced toolset and innovative techniques reflect its focus on maintaining operational stealth while executing highly targeted attacks, cementing its role as a formidable actor in North Korea's cyber warfare strategy against the central, regional as well as the sidelines players of the International Security order.

Assessment of North Korea's Cyber Weapons Capabilities on International Security

With having discussed North Korea's key cyber operations in the previous sections, the paper would now attempt to provide the geopolitical implications of these operations on international security of North Korea's immediate neighbourhood region, Northeast Asia and beyond. The assessment would, thereafter, cover the implications of these stated cyber operations on South Korea, China, Japan, Russia and the United States of America with efforts of the respective countries to tackle with the implications of these cyber operations against having severe consequences on their domestic economic interests.

DOI: https://doi.org/10.47362/EJSSS.2024.5304

South Korea

Given the series of cyber weapon operations deployed under the North Korean regime, it may be clarified that the first target for a large variety of such operations have been South Korea itself. With the geographical proximity of both the Koreas located within the Korean peninsula and separated by a ceasefire line known as the 38th Parallel, South Korea's ruthless Northern neighbour has found to have utilised its incognito appearance in the cyber-physical domain in order to project its one and only application of its soft power to the international order. Among the three cyber operations – Kimsuky, Lazarus as well as APT37 and their respective cases discussed alongside, our analysis attempts to provide an overview assessment of the implications to the South Korean economy.

Kimsuky group's major stint in projection of North Korea's funding to anonymous cyber hackers had been prevalent in the March 2013 Denial of Service attack on the Korean Institute of Defence Analysis as well as the Ministry of Unification had accumulated a total of US$700 million worth of financial damage with the campaign of informational espionage of critical military information on the border development strategies in the areas of quantity of additional troops deployment in the ceasefire line as well as the broader national security information that has been found to hacked and potentially traded with the North Korean regime (Greenberg February 2010).

The involvement of Kimsuky group in the December 2014 South Korean Hydro and Nuclear Power Co. Ltd had been considered the largest scale of cyber hack operations managed by the North Korean group. The hack on the Korea Hydro and Nuclear Power company had meant the North Korean-funded Kimsuky had the operational control over 24 civil program-aimed nuclear reactors that contribute close to 29% of their energy requirements (Mansourov 2014). There have been reports that have called out the vulnerability of South Korea's nuclear facility control systems having been considered too flawed for such a critical program and have been blamed for its compromise.

China

With the North Korean cyber infrastructure having been largely disconnected from the global network platforms such as the World Wide Web, it ought to be keenly noted that its internet and potential cyber activities and the resultant data traffic usually passes through two key

DOI: https://doi.org/10.47362/EJSSS.2024.5304

network providers – China's Unicom and Russia's Trans Telecom, respectively. Sources have revealed that close to 60% of its internet traffic are observed to pass through the Russian telecom provider, Trans Telecomm Co. Ltd. This figure reveals that North Korea's vulnerabilities to the any foreign retaliatory cyber counteractions are considered to be relatively low because of the inability of complete identification on the North Korean hacking network.

China has played the role in provision of covert, indirect support to selective North Korean cyber warfare operations. Operation Kimsuky's informational espionage on acquiring South Korean military secrets had reported to have utilised the Chinese IP addresses which were traced to the Jilin and Liaoning Provinces of Eastern China to have contributed to their hacking operations.

In matters of Northeast Asian security, China may not have been the direct recipients of Kimsuky or the larger North Korean-hacker community's cyber weapons operations. But the sheer geographical proximity with Pyongyang and the Eastern Chinese valleys have raised international actors' suspicions on China's role of providing occasional shelters to these overseas hacker groups that have been traced to have North Korean identity and broader proofs of the Kim-regime connections since 2013.

Russia

In the context of cyber space operations, North Korean hackers have been accused by the United States of conducting a majority of their operations under the auspices of the Russian internet provider platform operations. Much of Russia's cyber space ties with Kim's North Korea date to November 2017 when it had been reported that a Russian telecommunication company had begun to provide North Korea with a second internet connection and there have also been scholarly observations which reported and verified the lack in tracing the IP addresses of the cyber-attacks when the hackers are found to borrow the Russian-IP address channel.

There have been reports from South Korean and American institutions that have claimed the Lazarus group hackers to have maintained trusted relationships with the top-tier Russian cybercriminals. This idea has also proved to be supported across the Western hemisphere with the technical capability of North Korean hacker groups to consider the Russian version of cybercriminals as their 'beneficial partners' in the former's continued efforts of conducting cyberattacks aimed at either Western institutions or their proxies in Northeast Asian region.

DOI: https://doi.org/10.47362/EJSSS.2024.5304

United States of America

The United States are the significant recipients of increased North Korean cyber warfare operations when considered from the perspective of International Security, with having classified an entirety of North Korean cyber-hacker groups categorized under the name of 'Hidden Cobra'. The US official reports are often found to have over-exaggerated on the extent of North Korean cyber operations, however, the top US officials have found to rank North Korea among the top four cyber threats that may have the capability to launch disastrous cyber warfare attacks against the United States.

There have been CIA reports post the 2013 Kimsuky and Lazarus cyberattacks that have claimed that Pyongyang's advanced cyberwarfare prowess had surpassed a few, selected nations that have extensive informational database of key US algorithms and their national security interest policy reports that have concentrated on North Korean-related policy developments and subsequent data-secured encoded transfers that are stored in South Korean military think-tanks, whose later vulnerability for cyber-hack breach had been questioned post the 2014 Kimsuky operation.

Conclusion

The paper has focused the study entirely on North Korea's experimentation and subsequent exploitation of its cyber weapons capabilities given the extent of increased interconnectedness of the global order on multilateralism, complex interdependence as well as world-wide-web dominated cyber-physical environment. The theory of cyber power helps in explaining the emergent need for norms that regulate cyberspace protection against breach by false IP-addresses operated by hacker groups.

The world of cyberspace may be close to three decades since its global adoption, however, the 21st century global order is dominated by risks emanating from non-traditional domains of warfare; cyberspace having identified to be the preferred facilitator with wide-scale impacts and least costs of investment. Although, there have been debates whether cyberattacks ought to be classified as acts of terrorism.

Yet, state-sponsored cyber warfare may have potential yet drastic implications for global security given that data-security is the heart of the present-day critical information

Date of publication: 31 Jan 2025 Dec 2024 – Jan 2025
DOI: https://doi.org/10.47362/EJSSS.2024.5304

infrastructure. Thereafter, there ought to have been a regulatory framework common to the South Korea, United States and its larger allies to prevent the breach by an un-identified virus or malware supported hacker entity.

References

FireEye Incorporation. 2018. *APT37 (Reaper): The Overlooked North Korean Actor.* California: FireEye.

Greenberg, Andy. February 2010. "The Toolset of an Elite North Korean Hacker Group on the Rise." *Wired.*

Jun, J, S LaFoy, and E Sohn. 2015. *North Korea's Cyber Operations: Strategies and Responses.* Lanham, USA: Rowman & Littlefield.

Kim, C W, and C Polito. 2019. "The Evolution of North Korean Cyber Threats." *The Asan Institute for Policy Studies* 1-12.

Kim, M. 2016. "Why Provoke? The Sino-US Competition in East Asia and North Korea's Strategic Choice." *Journal of Strategic Studies, Vol. 39* 979-998.

Kim, min-hyung. February 2022. "North Korea's Cyber Capabilities and their Implications for International Security." *Sustainability 14(3): 1744.*

Klingner, Bruce. September 2023. *North Korea's Cybercrimes Pay for Weapons Programs and Undermine Sanctions.* Washington DC: The Heritage Foundation.

Lee , Y, H Kwon, J Lee, and D Shin. 2018. "The Countermeasure Strategy Based on Big Data Against North Korean Cyber-attacks." *Korean Journal of Defense and Analysis; Vol. 30* 437-454.

Mansourov, A. 2014. *North Korea's Cyber Warfare and Challenges for the US-ROK Alliance.* Washington D.C: Korea Economic Institute of America.

2020. *North Korean Advanced Persistent Threat Focus: Kimsuky.* 27 October. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a.

Nye, Jr, Joseph S. May 2010. *Cyber Power.* Cambridge: Harvard Kennedy School.

Park, Joshua. 2021. "THE LAZARUS GROUP: THE CYBERCRIME SYNDICATE FINANCING THE NORTH KOREA STATE." *Harvard International Review*, Spring: 34-39.

Suh, Elisabeth. January 2022. "North Korea's cyber capabilities and strategy." *German Council of Foreign Relations.*

—. 2022. "North Korea's Cyber Capabilities and Strategy." *DGAP.* January 07. https://dgap.org/en/research/publications/north-koreas-cyber-capabilities-and-strategy-0.

2021. *The Lazarus heist: How North Korea almost pulled off a billion-dollar hack.* 21 June. https://www.bbc.com/news/stories-57520169.