

Issue

Brief

ISSUE NO. 755
NOVEMBER 2024

North Korea's Cyber Strategy: An Initial Analysis

Abhishek Sharma

North Korea is among the states that stand out for their often defiant behaviour, divergent from typical diplomatic niceties and non-compliant with widely accepted international liberal norms and rules. This 'uniqueness' is seen, for instance, in the country's nuclear weapons development programme, which has been the object of global attention since the early 1990s. North Korea has now extended this behaviour to the cyber domain, marked by an increasing number of attacks by state-sponsored hackers against other states. Its development of cyber capabilities offers insights into the regime's views on the importance of the cyber domain in contemporary warfare. This brief examines the drivers of North Korea's cyber capabilities, gauging its successes and the risks it poses to countries, particularly the United States, South Korea, and Japan.

According to a United Nations (UN) Panel of Experts, from 2017 to 2023, the Democratic People’s Republic of Korea (DPRK or North Korea) stole virtual assets worth US\$3 billion via 58 cyberattacks on cryptocurrency platforms.¹ The finding coincided with a statement made by Anne Neuberger, US Deputy National Security Adviser (NSA) for Emerging Technology, that the money laundered by North Korea through cybercrimes is used to fund at least half of its nuclear weapons programme.² This highlights the role of cyber operations in North Korea’s statecraft, which extends beyond money heists to strategic domains such as intelligence and defence through cyber espionage and theft. To maximise its cyber potential, North Korea has invested in infrastructure and capability upgrades, strengthening its position as a formidable player in this domain.

The Lowy Institute Asia Power Index 2024 ranked North Korea 7th in cyber capabilities, above other Asian countries such as Taiwan, Japan, and India,³ while the Belfer Center’s National Cyber Power Index 2022 placed it at the 14th position, with high ratings in financial and offensive cyber capabilities.⁴ The DPRK’s strategic use of cyber capabilities is central to its goal of enhancing overall power, particularly through asymmetric warfare—a key element of its military culture. Unlike nuclear assets, cyber capabilities align well with North Korea’s offensive tactics, allowing it to operate below the escalation threshold without significant risk.

Pyongyang has expanded its asymmetric forces and cyber-hacking infrastructure to augment its conventional capabilities. According to South Korea’s National Intelligence Service (NIS), as of 2024, North Korea has 8,400 cybercrime personnel,⁵ compared to 6,800 in 2022.⁶ This growing cyber workforce is in parallel with a sharp rise in North Korean cyber operations; in 2023, the NIS reported 1.62 million hacking attempts, a 36-percent increase from the number in 2022.⁷ Emerging technologies such as Artificial Intelligence (AI) have also increased the effectiveness of DPRK cyber operations.⁸

Cybersecurity experts observe that states conduct cyber operations with a strategic rationale.⁹ For North Korea, its investments in building the state’s cyber capabilities are closely aligned with its primary objective of ensuring the regime’s security. A critical aspect of this strategy is offensive cyber capabilities, embodied by the prominent hacker group Lazarus, which is divided into small groups,¹⁰ each focusing on some sector and objectives (see Table 1).

The Reconnaissance General Bureau (RGB), which works directly under leader Kim Jong Un, oversees North Korea’s cyber operations (see Figure 1). The United States (US), South Korea, and Japan have thus far faced the brunt of the DPRK’s cyber offensive operations; in recent years, there have also been reported hacks on critical national infrastructure in India and Indonesia.¹¹ In South Korea, there has been a sharp increase in cyber intrusion attempts. A South Korean lawmaker has noted that the number of attacks targeting the Unification Ministry and other inter-Korean organisations has doubled since 2022, reaching 2,313 in 2024.¹²

Figure 1: DPRK Institutional Cyber Structure



Source: Mandiant¹³

North Korea's cyber operations have two primary objectives: generating financial resources to support Kim Jong Un's *Byungjin* policy^a initiatives, and gathering strategic intelligence. A significant portion of the stolen funds is believed to support the DPRK's nuclear and ballistic weapons programme.

The systematic development of North Korea's cyber capabilities as a political instrument—particularly in financial, intelligence, and military domains—has created a complex web of operations.

Table 1: DPRK Threat Actors

DPRK Threat Actor	Sub-Divisions	Target Areas	Objectives	Attempted Cyber Intrusion Incidents	Tactics, Techniques, and Procedures
Lazarus ¹⁴		Government, military, financial, manufacturing, publishing, media, entertainment, and international shipping companies, as well as critical infrastructure		Operation Troy, WannaCry 2.0, Sony Pictures Entertainment Ltd, Cryptocurrency attacks	
	BlueNoroff (APT38, Sapphire Sleet, Alluring Pisces)	Financial institutions, blockchain, cryptocurrency businesses, ATMs	Collect revenue	Bangladesh Central Bank Heist	Phishing and backdoor intrusion, spear phishing operations, watering hole attacks, crypto jacking operations
	Andraneil (APT45, Stonefly group, Silent Chollima, Onyx Fleet)	Defence, aerospace, space, nuclear facilities, engineering, medical, and energy sectors ¹⁵	Steal classified information, intellectual property theft, and ransomware attacks ¹⁶	Maui Ransomware	Exploiting software vulnerabilities
	Kimsuky (TEMP, Firework, Emerald Sleet, Velvet Chollima) ¹⁷	Critical infrastructure, think tanks, South Korean government entities, Korean experts	Intelligence-gathering missions (South Korea, Japan, and the US)	2014 Korea Hydro and Nuclear Power	Spear phishing

Source: Author's own, using various open sources.

^a Kim Jong Un's *Byungjin* policy aims to further two parallel goals: nuclearisation and economic development.

Cyber as a Strategic Asset

While cyber heist remains a key component of the DPRK's cyber calculus, its broader application of cyber power—targeting adversarial networks for intelligence collection and espionage—plays a role in analysing enemy actions. North Korea has carefully managed global perception, leading observers to focus on its financial cybercrimes as if they solely fund strategic initiatives. This narrative, however, obscures Pyongyang's extensive espionage operations, which have proven essential for the Kim Jong Un regime's strategic decision-making.^b

^b Although there is no direct evidence to show that cyber espionage operations had led to specific decisions made by the regime, it is hard to ignore the thread that connects the two. One of the important incidents often overlooked is the 2016 North Korea targeted actions to penetrate the US-South Korea operations command to collect intelligence and its later decision to alter the Nuclear Doctrine, specifying the condition under which nuclear weapons will likely be used. The 2016 cyber theft led to North Korea stealing US-South Korea Op command plans, which included plans to assassinate the North Korean leader Kim Jong Un. Just some years later, the revised version of North Korean nuclear doctrine stated that any attempt to assassinate the supreme leader will cause North Korea to use its nuclear weapons. Although the threat of the assassination was already there, even before, but these specific changes were made only in the 2022 declaration. See: https://csrc.nist.gov/glossary/term/Cyber_Attack

DPRK's Cyber Operations in Three Phases

Over the past 15 years, North Korea's cyber campaigns have evolved with each operation, such as Distributed Denial-of-Service (DDoS) attacks, Sony, WannaCry, and cryptocurrency theft such as Axie Infinity. This trajectory has shifted in both sophistication and objectives. Accordingly, the DPRK's cyber journey can be divided into three phases: Experimentation (2009-2014), Normalisation (2015-2017), and Weaponisation (2018-2024).

Experimentation (2009-2014)

During these years, North Korea conducted a series of cyber operations for the first time, against strong adversaries like South Korea and the US. The DPRK made mistakes while undertaking these cyber operations. For example, DPRK hackers reused the same virus code for multiple attacks, including the Bangladesh Bank heist in 2016 and the Sony hack in 2014,^c even using the same IP addresses—an oversight in masking digital footprints.¹⁸ Such mistakes, though undetected at that time, would be easily traceable today, when states and private-sector stakeholders are more cognisant.

This phase of North Korean cyber activity was characterised by tactical operations with limited strategic impact—an approach that evolved in the next phase as the DPRK became more proactive and adaptable.

Normalisation (2015-2017)

In this period, DPRK cyber operations were targeted towards collecting financial resources—a shift that coincided with the stringent United Nations Security Council (UNSC) sanctions regime¹⁹ after the DPRK conducted nuclear tests in January 2016.²⁰ In just two years, North Korea had launched cyber operations against banks in 18 countries.²¹ The most notorious incident was the 2016 attack on the Central Bank of Bangladesh, where North Korea attempted to steal US\$1 billion.²² Regular attacks allowed North Korean hackers to refine their techniques for infiltrating banking IT infrastructure.

Another incident during this phase occurred in India, involving the Cosmos Co-operative Bank in Pune, which lost US\$11 million via what is called 'jackpotting', an illegal method of withdrawing cash from an ATM by using

^c The cyber attack against Sony in 2014 was the first time that North Korea truly captured the world's attention. A year earlier, the Dark Seoul attack showed the seriousness of North Korea as a cyber threat, even if the operation was limited to just South Korea. The attack targeted critical national infrastructures in South Korea, including the electricity grid, media organisations, and banks, resulting in the breakdown of services and impacting people's daily lives.

DPRK's Cyber Operations in Three Phases

or manipulating banking softwares. The attack was linked to the Lazarus Group, which hacked the bank's system and altered its software. They also recruited people via dark-web networks to execute the jackpotting.²³ Although the Federal Bureau of Investigation (FBI) had issued a warning to Indian authorities, the timing during the weekend rush led to delayed response. This incident was replicated in over two dozen countries worldwide, showcasing the extent, scope, and scale of planning by North Korean hackers.

It was during these years that the DPRK's cyber actors became more comfortable with undertaking complex operations and executing cyberattacks in coordination with their networks based in North Korea and in other parts of the world. These attacks targeted critical national infrastructure, posing serious national security risks to the affected countries. Although North Korea's focus remained on limited objectives, this phase enabled it to access vast amounts of money, effectively bypassing UNSC sanctions with ease.

Weaponisation (2018-Present)

This phase has been marked by two characteristics: adopting new technologies to enhance the effectiveness and efficiency of cyberattacks, and implementing a wide spectrum of cyber operations to achieve diverse objectives. During these years, the DPRK has intensified both the frequency of cyberattacks and its use of new social-engineering techniques, targeting financial resources and intelligence purposes. While efforts to fund its nuclear and ballistic missile programmes are continuing, there is an increased emphasis on cyber espionage, IP theft, and surveillance.²⁴ This phase coincides with a rise in cyber espionage campaigns globally, especially in sectors with dual-use technologies, such as defence industries, aerospace, space, and shipbuilding. DPRK hackers has also begun targeting high-profile individuals in military, foreign policy, and think tank circles, primarily in South Korea and the US, but with a broader reach extending to India, Japan,²⁵ Spain,²⁶ and the United Kingdom (UK). Cases of industrial theft targeting Russian defence companies further reveal Pyongyang's drive to acquire critical military technology.

In addition to targeting cryptocurrency platforms, North Korea has used ransomware to fund operations against US military and defence contractors.^{d,27} Hackers would encrypt medical testing and electronic record files, and demand

d *Maui ransomware* is an example where North Korean hackers targeted 'U.S. hospitals and healthcare companies, to extort ransome, and then use that money' to 'purchase internet servers to commit computer intrusions against the U.S., South Korean and PRC government. See: https://www.justice.gov/d9/2024-07/hyok_filed_indictment.pdf

DPRK's Cyber Operations in Three Phases

a ransom in exchange for giving access to the files.²⁸ After receiving the money through Bitcoin, the ransom was transferred to two intermediaries in Hong Kong, converted to tether, and ultimately converted to Chinese yuan, accessed in the Dandong province, adjacent to the North Korean city of Sinuiju.

Indeed, North Korean hackers have become more innovative, integrating new technologies such as AI for greater effectiveness and exploring alternative ways to bypass security systems and generate additional funds. This includes collaborating with foreign citizens by masking their North Korean identities and adopting tactics like cryptojacking and exploiting mixing services.²⁹ Hackers have expanded their technical reach by developing malware for 32-bit and 64-bit Windows platforms³⁰ as well as targeting the Apple macOS platform, which is widely used by high-end companies, particularly in the fintech sector.³¹

The evolution of the DPRK's cyber operations through experimentation, normalisation, and weaponisation highlights two critical points: the systematic institutionalisation of its domestic cyber infrastructure, marked by increased investment in cyber capabilities, and a growing strategic convergence between the regime's stated goals and cyber statecraft.

Table 2: Espionage Victimology

Industry	Information Targeted
Defence	<ul style="list-style-type: none"> • Heavy and light tanks and self-propelled howitzers • Light strike vehicles and ammunition supply vehicles • Littoral combat ships and combatant craft • Submarines, torpedoes, unmanned underwater vehicles (UUVs), and autonomous underwater vehicles (AUVs) • Modeling and simulation services

DPRK's Cyber Operations in Three Phases

Industry	Information Targeted
Aerospace	<ul style="list-style-type: none"> • Fighter aircraft and unmanned aerial vehicles (UAVs) • Missiles and missile defence systems • Satellites, satellite communications, and nano-satellite technology • Surveillance radar, phased-array radar, and other radar systems
Nuclear	<ul style="list-style-type: none"> • Uranium processing and enrichment • Material waste and storage • Nuclear power plants • Government nuclear facilities and research institutes
Engineering	<ul style="list-style-type: none"> • Shipbuilding and marine engineering • Robot machinery and mechanical arms • Additive manufacturing and 3D printing components and technology • Casting, fabrication, high-heat metal moulding, and rubber and plastic moulding • Machining processes and technology

Source: Nation Cyber Security Centre, UK³²

Current Cyber Threats from DPRK

The DPRK's cyber operations have escalated to serious national security threats across three main areas: IT worker-related operations, cryptocurrency theft, and cyber espionage. These activities, primarily targeting countries such as South Korea, Japan, and the US, have also impacted other countries like India, Indonesia, and Bangladesh, which do not have adversarial relations with North Korea.

Cryptocurrency Theft

Cryptocurrency platforms have become a prime target for North Korean hackers, offering an efficient avenue for money laundering. The attacks began in 2017,³³ targeting South Korean exchanges like Bithumb³⁴ and Yobit,³⁵ and escalated after 2018³⁶ as cryptocurrencies started becoming more widely accepted and traditional bank intrusions became more difficult to execute.^c Between 2017 and 2018 alone, hackers stole US\$571 million from exchanges.³⁷ North Korea seized the opportunity to exploit the crypto market; a 2024 UN Panel of Experts report estimated that, between 2017 and 2023, North Korean hackers stole US\$3 billion through crypto heists (see Table 2), accounting for nearly 44 percent of the total crypto hack.³⁸ Hackers employ many tactics, including spear phishing, which deploys malware and steals cryptocurrencies. The FBI has noted the increasing sophistication and persistence of these cyber operations targeting crypto assets and products.³⁹

Despite better law enforcement, strict regulatory guidelines, and a sanctioning regime in the US cryptocurrency ecosystem, North Korean hackers continue with their sophisticated and persistent attacks. While these constraints have reduced the volume of illicit cryptocurrency (see Figure 3), hackers have adapted and refined their techniques. In addition to mixers, cross-chain bridges have emerged as an attractive option for money laundering. Hackers also target cryptocurrency users via fake job offers on LinkedIn,⁴⁰ fake applications,⁴¹ job scams,⁴² and coding assessments.^{f,43}

e It took North Korean hackers longer, in some cases months and years to break into the banking system and get into its SWIFT system. Cryptocurrency money laundering was an easy process that took less effort with greater return and less attention from the law enforcement agencies.

f Coding assessments are part of a tactic employed by North Korea, wherein hackers use job interviews to approach developers on social media sites such as LinkedIn, where they are asked to download rogue packages to show their coding skills (e.g., building a Python project).

Current Cyber Threats from DPRK

Figure 2: Illicit Money Stolen by DPRK



Source: Chainalysis 2024 Crypto Crime Report⁴⁴

To counter increasing constraints, North Korean hackers have started using new software tools and are shifting their focus to markets with less regulations and more flexible financial environments.⁴⁵

Table 3: Major Cyber Thefts (Crypto Platforms, 2022-2024)

Company Name	Attack Date	Amount (in US\$ million)
Terraport Finance	10 April 2023	4
Merlin DEX	26 April 2023	1.8
Atomic Wallet	2 June 2023	120
Alphapo	22 July 2023	110
Alex Infinity	14 April 2022	615
Poloneix	10 November 2023	114
Orbit Chain	31 December 2023	81
Wazir	18 July 2024	235
Indodax	11 September 2024	20

Source: Recorded Future⁴⁶

Current Cyber Threats from DPRK

DPRK Information Technology Workers

DPRK IT workers have emerged as a serious threat as they manage to bypass the 2017 United Nation Security Council Resolution (UNSCR) 2397 that banned work authorisations for North Korean workers.⁴⁷ These hackers employ methods to evade the ban, such as adopting fake identities and using false emails, social media accounts, payment platforms, as well as false websites and proxy computers.^{g,48}

The objective of DPRK IT workers appears to be twofold: to earn finances for North Korean strategic programmes^h and to invade big US companies and steal critical data and information.ⁱ

Cyber Espionage

Espionage plays a crucial yet often overlooked role in North Korea's cyber operations, serving as a strategic tool for maintaining North Korea's strategic calculations, keeping itself updated with the plans linked to the regime's survival. According to the Recorded Future report, espionage was the primary objective behind 72 percent of the 273 mapped North Korean cyberattacks, underscoring its role in the country's cyber strategy (see Figure 4).⁴⁹ Two key actors involved in these operations are the Onyx Fleet (also known as Andraneil) and Kimsuky, both of which have focused on gathering sensitive data through cyber intrusion.⁵⁰ In recent years, Symantec has observed, North Korean cyber actors are increasingly targeting entities with classified or highly sensitive information or intellectual property.⁵¹ With more high-value targets, hackers have also improved their Tactics, Techniques and Procedures (TTPs), upgrading from DDoS attacks to disk-wiping and now using ransomware.⁵²

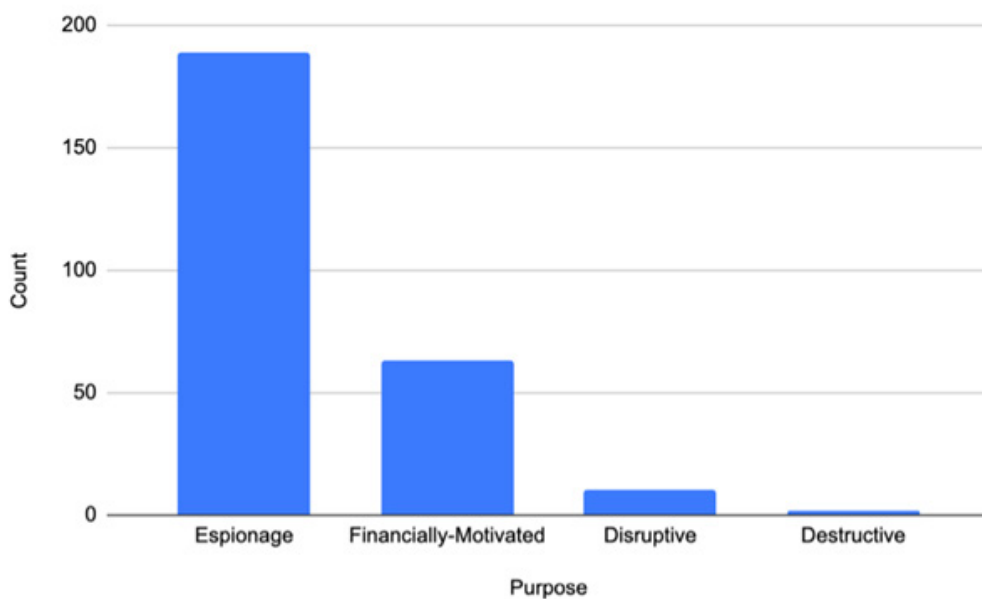
g In 2024, the US Department of Justice convicted a US Tennessee national for assisting DPRK workers get IT jobs. The US national was running a laptop farm for North Korean IT workers, helping them generate an amount of US\$250,000 dollars per year. As per the US Department of Justice, the US national allegedly assisted them [DPRK IT workers] in using a stolen identity to pose as a US citizen; hosted company laptops at his residences; downloaded and installed software without authorisation on such laptops to facilitate access and perpetuate the deception; and conspired to launder payments for the remote IT work, including to accounts tied to North Korean and Chinese actors See: <https://www.darkreading.com/remote-workforce/tennessee-man-helped-dprk-workers-get-jobs-at-us-orgs-fund-wmds>; <https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and#:~:text=The%20IT%20workers%2C%20who%20were,the%20usands%20of%20dollars%20in%20damages>

h These are referred to as event-based operations that are tactical operations with immediate and near-immediate impact.

i These are presence-based operations which are strategic and aimed at a lengthy intrusion phase, focused on clandestine sabotage operations oriented at gathering intelligence and strategic information.

Current Cyber Threats from DPRK

Figure 3: Objectives of North Korean Cyber Attacks



Source: Recorded Future⁵³


Evaluating the Threat of DPRK Cyber Operations

While it is critical to highlight the cybersecurity threat from North Korea, particularly its increased cyber activities, the extent of this cyber threat should not be exaggerated. Much of the cyber rhetoric surrounding it, such as “cyberwar” and “Cyber Pearl Harbour”, stems from myths that complicate the cyber discourse regarding perceptions towards the cyber domain. These exaggerations overstate the cybersecurity risks that states can impose on adversaries in either peacetime or conflict. To clarify, it is essential to differentiate between Offensive Cyber Operations (OCOs) based on two criteria: objectives and the types of operations. Separating the OCOs provides clarity and puts North Korea’s strategic motivations and intent in context. These two criteria can be further divided into tactical or strategic objectives, and event-based or presence-based operations.

This framework clarifies the types of cyberattacks it engages in and helps eliminate unnecessary cyberwar rhetoric. According to Offensive Cyber-theorist Daniel Moore, for a cyber incident to qualify as a cyberwar, it must satisfy five parameters: targets, impact, attackers, goals, and relationships.⁵⁴ This framework also distinguishes serious incidents from what he calls “peacetime offensive operations”, such as cyber espionage and cybercrimes, including cyber theft.⁵⁵ For example, the Sony attack would not be considered cyberwarfare as Sony is a private corporation. In contrast, the US-Israel cyber campaign against Iran’s Natanz facility, also popularly known as Stuxnet, would be considered a cyberwar.

Whether North Korean cyberattacks can qualify as cyberwarfare would require deeper analysis, which requires a separate, more detailed study. At this point, it is important to recognise that applying this framework to North Korea’s cyber operations may not always be correct, as the cyber domain is complex. For example, long-term intelligence gathering or cybercrimes could help the regime strengthen its defences by allowing it to make an “informed decision”, thus constituting a “strategic breach of national security”.⁵⁶ Therefore, for a country like North Korea, applying a deductive approach to offensive cyber operations would not stand scrutiny due to loopholes.

As North Korea enters a new phase of strategic relevance in Northeast Asia, marked by its renewed political and military partnership with Russia, the regime is expected to further invest in military modernisation, particularly in emerging domains such as space and cyberspace. Cyberspace is particularly attractive for activities such as cyber sabotage, cyber espionage, cyber heist, intelligence gathering, and IT theft. Therefore, the world is likely to see an increasing number of cyberattacks against DPRK adversaries like South Korea, the US, and Japan. As North Korea strengthens its conventional and covert military capabilities, the cyber domain will become vital, alongside areas like space, drones, and shipbuilding. The regime's targets will also thereby expand, driven by its aspiration to fund the country's nuclear and ballistic programmes and to steal secrets for building its conventional military and new warfare domain.

To counter North Korean cyberattacks, it is necessary for like-minded states to view these actions as violations of appropriate state behaviour in cyberspace, not as isolated incidents targeting specific countries. As geopolitics intersect with cyber activities, coordination among countries sharing revisionist agendas is likely to grow, turning cyber into a contested domain rather than one of cooperation. It is crucial to strengthen cyber cooperation with allies⁵⁷ and partners through law enforcement, enhanced cyber resilience, capacity building, and shared critical cyber intelligence and information to keep the cyberspace safe and secure. 

Abhishek Sharma is Research Assistant, Strategic Studies Programme, ORF.

- 1 “UN Documents on DPRK,” March 7, 2024, https://www.securitycouncilreport.org/un_documents_type/sanctions-committee-documents/?ctype=DPRK%20%28North%20Korea%29&ctype=dprk-north-korea
- 2 Sean Lyngaas, “Half of North Korean Missile Program Funded by Cyberattacks and Crypto theft, White House says,” *CNN*, May 10, 2023, <https://edition.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html>
- 3 “Lowy Institute Asia Power Index 2024,” <https://power.lowyinstitute.org/data/military-capability/signature-capabilities/cyber-capabilities/>
- 4 “National Cyber Power Index 2022,” <https://www.belfercenter.org/publication/national-cyber-power-index-2022>
- 5 Ministry of National Defence, Republic of Korea, “2020 Defence White Paper,” https://www.mnd.go.kr/user/mndEN/upload/pblictN/PBLICTNEBOOK_202307280406019810.pdf
- 6 Ministry of National Defence, Republic of Korea, “2020 Defence White Paper”
- 7 Kim Na-young, “N. Korea Attempts to Use Generative AI for Hacking Attacks: Spy Agency,” *Yonhap News Agency*, January 24, 2024, <https://en.yna.co.kr/view/AEN20240124003300320?input=tw>
- 8 Abhishek Sharma, “Emerging Technologies Will Strengthen North Korean Cyber threat,” *Binding Hook*, February 13, 2024, <https://bindinghook.com/articles-hooked-on-trends/emerging-technologies-will-intensify-the-north-korean-cyber-threat/>
- 9 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Oxford University Press, 2022), 74.
- 10 Michael Barnhart et al., “Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations,” *Google Cloud Blog*, March 23, 2022, <https://cloud.google.com/blog/topics/threat-intelligence/mapping-dprk-groups-to-government/>
- 11 Shreyas Reddy, “North Korean Cybercriminals Steals \$22M from Indonesian Crypto Exchange,” *NK NEWS*, September 17, 2024, <https://www.nknews.org/2024/09/north-korean-cybercriminals-steal-22m-from-indonesian-crypto-exchange/>
- 12 Shreyas Reddy and Joon Ha Park, “North Korea Cyberattacks on Seoul’s Unification Ministry Double Since 2022,” *NK News*, September 25, 2022, <https://www.nknews.org/2024/09/north-korean-cyberattacks-on-seouls-unification-ministry-double-since-2022/>
- 13 Taylor Long et al., “APT45: North Korea’s Digital Military Machine,” *Google Cloud Blog*, July 26, 2024, <https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine>

- 14 “Lazarus Group (APT38): North Korean Threat Actor,” Radware, <https://www.radware.com/cyberpedia/ddos-attacks/the-lazarus-group-apt38-north-korean-threat-actor/#:~:text=The%20Lazarus%20Group%2C%20also%20known,linked%20to%20North%20Korean%20hackers.>
- 15 National Cyber Security Centre, “NCSC and Partners Issue Warning Over North Korean State-Sponsored Cyber Campaign to Steal Military and Nuclear Secrets,” <https://www.ncsc.gov.uk/news/ncsc-partners-vigilant-dprk-sponsored-cyber-campaign>
- 16 National Cyber Security Centre, “NCSC and Partners Issue Warning Over North Korean State-Sponsored Cyber Campaign to Steal Military and Nuclear Secrets”
- 17 “National Coordinator for Critical Infrastructure Security and Resilience,” <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a>
- 18 Geoff White, *The Lazarus Heist: From Hollywood to High Finance: Inside North Korea’s Global Cyber War* (National Geographic Books, 2022), 119
- 19 Richard Roth, Holly Yan, and Ralph Ellis, “U.N. Security Council Approves Tough Sanctions on North Korea,” *CNN*, March 3, 2016, <https://edition.cnn.com/2016/03/02/world/un-north-korea-sanctions-vote/>
- 20 Katie Hunt, K.J. Kwon, and Jason Hanna, “North Korea Claims Successful Test of Nuclear Warhead,” *CNN*, September 2016, <https://edition.cnn.com/2016/09/08/asia/north-korea-seismic-activity/index.html>
- 21 Jose Pagliery, “North Korea-Linked Hackers are Attacking Banks Worldwide,” *CNN*, April 4, 2017, <https://edition.cnn.com/2017/04/03/world/north-korea-hackers-banks/index.html>
- 22 Kim Zetter, “That Insane, \$81M Bangladesh Bank Heist? Here’s What We Know,” *Wired*, May 16, 2016, <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>
- 23 White, *The Lazarus Heist: From Hollywood to High Finance: Inside North Korea’s Global Cyber War*
- 24 “Stonefly: Extortion Attacks Continues Against the U.S. Targets,” *Symantec*, October 2, 2024, <https://symantec-enterpse-blogs.security.com/threat-intelligence/stonefly-north-korea-extortion>
- 25 John Leyden, “Japan Blames North Korea for PyPI Supply Chain Cyberattack,” *Dark Reading*, March 11, 2024, <https://www.darkreading.com/application-security/japan-blames-north-korea-for-pypi-supply-chain-cyberattack>
- 26 Jonathan Greig, “North Korean Gov’t Hackers Targeted Aerospace Company in Spain,” *Recorded Future*, September 30, 2023, <https://therecord.media/north-korean-govt-hackers-spain>
- 27 Elias Groll, “North Korean Hacker Used Hospital Ransomware Attacks to Fund Espionage,” *Cyberscoop*, July 24, 2024, <https://cyberscoop.com/north-korea-hacking->

- indictment-fbi-apt-45/
- 28 Groll, “North Korean Hacker Used Hospital Ransomware Attacks to Fund Espionage”
- 29 White, *The Lazarus Heist: From Hollywood to High Finance: Inside North Korea’s Global Cyber War*
- 30 “Cryptocurrency Businesses Still Being Targeted by Lazarus,” Securelist, March 26, 2019, <https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/>
- 31 “Cryptocurrency Businesses Still Being Targeted by Lazarus”
- 32 National Cyber Security Centre, “North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime’s Military and Nuclear Programs,” <https://www.ic3.gov/Media/News/2024/240725.pdf>
- 33 “Lazarus Group Pulled Off 2020’s Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options,” Chainalysis, February 9, 2021, <https://www.chainalysis.com/blog/lazarus-group-kucoin-exchange-hack/>
- 34 Catalin Cimpanu, “Bithumb Cryptocurrency Exchange Hacked Third Time in Two Years,” ZDNet, March 30, 2019, <https://www.zdnet.com/article/bithumb-cryptocurrency-exchange-hacked-a-third-time-in-two-years/>
- 35 Daniel Shane, “Bitcoin Exchange Goes Bust After Hack,” *CNN*, December 20, 2017, <https://money.cnn.com/2017/12/20/technology/south-korea-bitcoin-exchange-closes/index.html>
- 36 “North Korean Hackers Have Prolific Year as their Unlaundered Cryptocurrency Holdings Reach All-time High,” Chainalysis, January 13, 2022, <https://www.chainalysis.com/blog/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/>
- 37 Geoff White, *Crime Dot Com: From Viruses to Vote Rigging, How Hacking Went Global* (Reaktion Books, 2020), 124.
- 38 Kelly Ng, “Crypto Theft: North Korea-Linked Hacker Stole \$1.7b in 2022,” *BBC*, February 2, 2023, <https://www.bbc.com/news/world-asia-64494094#>
- 39 FBI, “North Korea Aggressively Targeting Crypto Industry with Well-Disguised Social Engineering Attacks,” <https://www.ic3.gov/Media/Y2024/PSA240903>
- 40 Ravie Lakshmanana, “North Korean Hackers Target Cryptocurrency Users on LinkedIn with RustDoor Malware,” *The Hacker News*, September 16, 2024, <https://thehackernews.com/2024/09/north-korean-hackers-target.html>
- 41 Ravie Lakshmanana, “North Korean Hackers Targets Job Seekers with Fake FreeConference App,” *The Hacker News*, September 4, 2024, <https://thehackernews.com/2024/09/north-korean-hackers-targets-job.html>
- 42 Ravie Lakshmanana, “North Korean Threat Actors Deploy COVERTCATCH Malware via LinkedIn Job Scams,” *The Hacker News*, September 7, 2024, <https://thehackernews.com/2024/09/north-korean-threat-actors-deploy-covertcatch-malware-via-linkedin-job-scams.html>

- com/2024/09/north-korean-threat-actors-deploy.html
- 43 Ravie Lakshmanana, “Developers Beware: Lazarus Group Uses Fake Coding Tests to Spread Malware,” *The Hacker News*, September 11, 2024, <https://thehackernews.com/2024/09/developers-beware-lazarus-group-uses.html>
- 44 “2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fail, But Ransomware and Darknet Markets See Growth,” Chainalysis, January 18, 2024, <https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/>
- 45 Anton Sokolin, “North Korea Linked Hackers Steals Millions from India’s Largest Crypto Exchange,” *NK News*, July 19, 2024, <https://www.nknews.org/pro/north-korea-linked-hackers-steal-millions-from-indias-largest-crypto-exchange/>
- 46 Jonathan Greig, “UN Probing 58 Alleged Crypto Heists by North Korea Worth \$3 billion,” *Recorded Future*, March 23, 2024, <https://therecord.media/north-korea-cryptocurrency-hacks-un-experts>
- 47 United Nations Security Council, “S/RES/2397 (2017),” <https://main.un.org/securitycouncil/en/s/res/2397-%282017%29>
- 48 Office of Public Affairs, U.S. Department of Justice, <https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and#:~:text=The%20IT%20workers%2C%20who%20were,thousands%20of%20dollars%20in%20damages.>
- 49 “North Korea’s Cyber Strategy,” *Recorded Future*, June 2023, <https://go.recordedfuture.com/hubfs/reports/cta-nk-2023-0622.pdf>
- 50 “Onyx Sleet Uses Array of Malware to Gather Intelligence for North Korea,” *Microsoft Threat Intelligence*, July 25, 2024, <https://www.microsoft.com/en-us/security/blog/2024/07/25/onyx-sleet-uses-array-of-malware-to-gather-intelligence-for-north-korea/>
- 51 “Stonefly: Extortion Attacks Continue Against U.S. Targets,” *Symantec*, October 2, 2024, <https://symantec-enterprise-blogs.security.com/threat-intelligence/stonefly-north-korea-extortion>
- 52 “Stonefly: Extortion Attacks Continue Against U.S. Targets”
- 53 “North Korea’s Cyber Strategy”
- 54 Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, 16.
- 55 Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, 19.
- 56 Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, 24.
- 57 Abhishek Sharma, “Why Seoul Needs to Do More to Spotlight North Korea’s Defiance of Cyber Norms,” *NK PRO*, September 30, 2024, <https://www.nknews.org/pro/why-seoul-needs-to-do-more-to-spotlight-north-koreas-defiance-of-cyber-norms/>



Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA

Ph. : +91-11-35332000. Fax : +91-11-35332005

E-mail: contactus@orfonline.org

Website: www.orfonline.org