Internal Security Review
2025, no. 33, pp. 391–417

https://doi.org/10.4467/20801335PBW.25.036.22653

ARTICLE

Cybercrime as an adaptation method of the Democratic People's Republic of Korea to the sanctions regime

SEBASTIAN JEŻ

University of Warsaw

https://orcid.org/0009-0001-3605-3054

Abstract

Offensive activities of the Democratic People's Republic of Korea in cyberspace constitute one of the more serious threats to global cybersecurity. Despite international sanctions, the DPRK regime effectively employs cybercriminal operations to generate state revenues amounting to billions of dollars. The aim of the article is to assess the scale, nature and significance of financial cybercrime within North Korea's economic and operational strategy under the sanctions regime. North Korean cyber groups, the largest profit-driven cyber attacks attributed to the DPRK, were discussed, and mechanisms implemented by governments and international organisations to counter state-sponsored cybercrime were presented. The results of the analysis indicate that North Korea's offensive cyber activities serve as a strategic tool enabling the regime not only to effectively obtain financial resources, but also to achieve political objectives and project power in cyberspace. These conclusions highlight the need to re-evaluate existing strategies for combating this type of cybercrime, particularly considering isolated regimes.

Keywords

North Korea, cybersecurity, cybercrime, cyber espionage, cyber warfare, public attribution, Lazarus group

Introduction

Cyber operations conducted by hackers sponsored by state (state-sponsored cyber threat), whose main goal is to obtain direct financial benefits, are one of the latest trends in the activities of such actors. In the early stages of development, state operations in cyberspace were dominated by espionage, cyberterrorism and warfare. Since around 2013, there has been a noticeable intensification of cybercriminal activities aimed at carrying out operations with high financial potential. One of the first examples of this phenomenon were operations carried out by states with limited resources, which operating under international sanctions, gradually integrated cybercrime as a tool for generating income[1].

Particular attention is drawn by the Democratic People's Republic of Korea (DPRK), which in recent years has carried out some of the most severe attacks in terms of financial losses incurred by victims. The key aspect of these activities is that the entities responsible for them do not operate as independent, loosely connected criminal groups, but are an integral operational part of the regime. Direct management and control directly by state structures qualify these operations as state-sponsored cyber threat[2].

The aim of the article is the analysis of the scale, nature and significance of financial cybercrime in North Korea's economic and operational strategy under the sanctions regime. The hypothesis adopted in this paper assumes that financial cybercrime is an important and systematic element of North Korea's operational strategy, enabling to effectively circumvent international sanctions as well as finance political and military regime objectives. In order to achieve the research objectives, a case study was used, which is considered an appropriate method in situations where the researcher has limited control over the phenomenon being analysed and the subject of the analysis is not only historical but also contemporary processes[3]. This method allowed for an in-depth analysis of the problem under study, which is particularly relevant given the limited access to primary data and the high level of complexity of the analysed phenomenon. The case study was supplemented with a comparative method in order to compare cases of cybercrime in different operational contexts. Moreover, the technique of analysing existing sources was

[1] J. DiMaggio, *Sztuka wojny cyfrowej. Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej* (Eng. The art of cyberwarfare: an investigator's guide to espionage, ransomware and organised cybercrime), Warszawa 2023, p. 57.

[2] K. Chung, K. Lee, *Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicle*, Seoul 2017, pp. 23–26.

[3] R.K. Yin, *Studium przypadku w badaniach naukowych. Projektowanie i metody*, Kraków 2015, pp. 47–87.

used, including a critical review of the literature on the subject, reports from international organisations as well as available quantitative data.

Understanding financial cybercrime in the DPRK requires placing it in the broader strategic context. In recent decades, the North Korea's adaptation of asymmetric strategies has been a conscious response to complex challenges related to military security and the economic situation. The turn of the 20th and 21st centuries brought about a shift in the balance of power on the Korean Peninsula, partly resulting from the dynamic development of the Republic of South Korea and the simultaneous economic stagnation of the DPRK[4].

Pyongyang's unification aspirations, which have determined its foreign policy for years, have begun to encounter new obstacles. Despite significant investment in the defence sector, the DPRK gradually recognised the limitations of its conventional military capabilities, especially in the context of changing global dynamics of the balance of power after the end of the Cold War. The reduction in external support, mainly from Russia and China, as well as the US's continued strong military presence in South Korea have prompted the regime to re-evaluate its strategic priorities and intensify its asymmetric activities[5].

Despite its isolation on the international stage, North Korea is consistently developing sophisticated strategies aimed at undermining the position of its main rivals: the United States and the Republic of Korea. Pyongyang intensifies activities aimed at strengthening operational capabilities and focuses on developing capabilities in asymmetric operations, both conventional and cybernetic. The development of technology and operational methods in cyberspace is a key element of this strategy and enables the DPRK to carry out intelligence and sabotage activities, as well as activities aimed at obtaining financial resources[6].

The specific nature of cyber attacks carried out by states stems primarily from the difficulties in attributing them quickly and accurately – identifying the perpetrator can be a lengthy and ambiguous process, which limits the possibility of immediate response. Attackers often use intermediaries, such as private hacker groups, mercenary companies or informal organisations that deliberately operate in a manner that makes it difficult to clearly link their activities to the commissioning state. This complexity requires the use of advanced analytical methods that enable the entire chain of evidence to be traced – from tactics, techniques and procedures, through specific individuals, to institutional sponsors. This process is further

[4] J. Jun, S. LaFoy, E. Sohn, *North Korea's Cyber Operations: Strategy and Responses*, Center for Strategic & International Studies, 2023, pp. 11–15.

[5] Ibid.

[6] Ibid., pp. 24–25.

complicated by the fact that some countries use public attribution in a manner that lacks transparency, which means that the final assignment of political responsibility is often based on evidence of varying quality[7].

The attribution of attacks is an extremely broad issue and would require a separate study. However, it is worth noting that several types of attribution are distinguished in the literature on the subject[8]. The first is technical attribution, which aims to identify the specific end device, server or other form of infrastructure used to carry out the attack. It serves as a starting point for further analysis. On this basis, it becomes possible to move on to organisational or personal attribution, which focuses on establishing the identity of the persons or groups behind the offensive activities. It attempts to answer the question of who is directly responsible for the attack and what environment – organisation or criminal group – may be behind it, if any is involved. The results of both these processes form the basis for political attribution, which is the most complex and sensitive stage of assigning responsibility. It involves linking the collected technical, intelligence and organisational data with the interests and activities of a specific country that may have commissioned the attack[9].

Each type of attribution poses unique challenges – from technical ones[10] that hinder investigations, to the lack of clear regulations in international law[11], to the risk of arbitrary decisions resulting from political conditions[12]. The multidimensional nature of the attribution process, especially in the context of assigning responsibility to a specific country, makes it particularly vulnerable to challenge. This problem manifests itself both on the international stage, especially in relations between antagonistic regimes, and in expert discourse, where differences in methodological approaches and limited availability of evidence further complicate the achievement of consensus.

---

7 M. Mueller et al., *Cyber Attribution: Can a New Institution Achieve Transnational Credibility?*, "The Cyber Defense Review" 2019, vol. 4, no. 1, pp. 107–122; H. Lin, *Attribution of Malicious Cyber Incidents*, "Aegis Paper Series" 2016, 1607, pp. 30–42; W. Banks, *Cyber Attribution and State Responsibility*, "International Law Studies" 2021, vol. 97, pp. 1058–1072.

8 T. Rid, B. Buchanan, *Attributing Cyber Attacks*, "Journal of Strategic Studies" 2015, vol. 38, no. 1–2, pp. 4–37. http://dx.doi.org/10.1080/01402390.2014.977382.

9 H. Lin, *Attribution of Malicious Cyber Incidents*…, pp. 1–26.

10 J.A. Guerrero-Saade, C. Raiu, *Walking in your enemy's shadow: when fourth-party collection becomes attribution hell*, Virus Bulletin, 2017, pp. 1–12.

11 K.E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, "UCLA Law Review" 2020, vol. 67, pp. 559–597.

12 T. Rid, B. Buchanan, *Attributing Cyber Attacks*…, pp. 4–37.

Moreover, a significant analytical challenge remains the high risk of errors and manipulation, including deliberate conducted false flag operations aimed at attributing responsibility to an entity other than the actual perpetrator[13].

In the context of North Korea's activities, whose *modus operandi* is often imitated by other hacker groups, there is an increased risk of erroneous or deliberate attribution of its operations carried out by other entities. Such measures open up space to political manipulation and cover-up activities, which are part of broader information campaigns carried out by third countries. For this reason, quantitative data should be treated with considerable caution, as they may reflect not only the actual scale of activities, but also the effects of erroneous or intentionally distorted attributions.

In the light of these findings, it is crucial to understand the extent to which activities aimed at acquiring financial resources in cyberspace have become a permanent and systematically used component of North Korea's operational strategy. The regime's ability to conduct revenue-generating coordinated activities indicates the growing professionalism and institutional embedding of this approach within state structures. At the same time, due to the limited transparency of attribution processes and the incomplete reliability of quantitative data, it is necessary to maintain a critical interpretative approach. However, analysis of this phenomenon remains essential for understanding the contemporary dynamics of cyber threats and the tools used in asymmetric actions taken by isolated regimes.

Forced labour as a means of generating income

Understanding the relationship between the regime and the individual requires taking into account the high degree of arbitrariness that characterises the North Korean system of government. As a modern totalitarian state, the Democratic People's Republic of Korea has extensive mechanisms of control and repression at its disposal, which are difficult to analyse in relation to Western values such as human rights, the rule of law, democratic legitimacy of power and transparency of state institutions. Another important factor in this context is the influence of propaganda and mechanisms of repression on the average citizen. This complex dimension of analysis has been addressed by eminent researchers. For instance, Jan Baszkiewicz, thoroughly described the mechanisms of control and subordination of individuals in totalitarian systems. His approach allows us to see that in countries operating under strict ideological control, terror and violence serve not only as tools of repression,

[13] F. Skopik, T. Pahi, *Under false flag: using technical artifacts for cyber attack attribution*, "Cybersecurity" 2020, vol. 3, pp. 1–20. https://doi.org/10.1186/s42400-020-00048-4.

but also as stabilisers of the system, shaping the social dynamics of loyalty and fear[14]. In this context, the public sector in the DPRK operates under conditions that are significantly different from those characteristic of democratic countries.

For years, North Korea has used forced labour as one of the key tools for generating income for the regime by sending citizens to work both domestically and abroad. This practice covers many sectors, including construction, shipbuilding, agriculture, catering, mining and IT. Reliable sources also point to the involvement of North Korean workers in armed conflicts, particularly in the ongoing Russian-Ukrainian war[15]. Posted workers are often subject to strict state control, and a significant portion of their wages is confiscated and transferred directly to the regime's budget[16].

The North Korea's involvement in the IT sector goes beyond hacking. For years, the regime has been implementing a coordinated programme to infiltrate the global IT market by employing North Korean specialists in remote positions in foreign companies, particularly in the US (so-called IT worker schemes). By operating under false identities and using stolen personal data, North Korean IT specialists find employment in international companies, especially in the technology, finance and industrial sectors. Their activity is a significant source of income for the regime and pose a serious threat to global security. With access to internal corporate networks, they can conduct intelligence operations and, in the long term, lay the groundwork for cyber attacks[17].

The US has repeatedly taken legal actions against North Korean schemes to infiltrate the IT sector, aimed at generating revenue for the regime and gaining access to corporate systems. The US has repeatedly taken legal action against North Korean schemes to infiltrate the IT sector, aimed at generating revenue for the regime and gaining access to corporate systems. One example of such actions is the indictment in December 2024 of 14 North Korean citizens for participating in a long-standing practice of illegally obtaining employment as remote IT specialists, which allowed for the transfer of at least USD 88 million to Pyongyang[18].

---

[14] J. Baszkiewicz, *Władza* (Eng. Power), Wrocław 1999, pp. 165–166.

[15] J. Garamone, *Pentagon Says 10K North Korean Troops in Kursk Oblast*, U.S. Department of War, 4 XI 2024, https://www.defense.gov/News/News-Stories/Article/Article/3955757/pentagon-says-10k-north-korean-troops-in-kursk-oblast/ [accessed: 18 III 2025].

[16] S.R. Stewart, *DPRK Overseas Financial Networks*, w: *People for Profit: North Korean Forced Labour on a Global Scale*, R.E. Breuker, I.B.L.H. van Gardingen (eds.), Leiden 2018, pp. 120–125.

[17] C. Starks et al., *Staying a Step Ahead: Mitigating the DPRK IT Worker Threat*, Mandiant, 23 IX 2024, https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat [accessed: 8 III 2025].

[18] United States of America v. J. Song Hwa, R. Kyong Sik, K. Ryu Song et al., United States District Court for the Eastern District of Missouri, CR 4:24CR648 MTS/JSD, 2024.

The structure of North Korea's cyber sector

The development of North Korean information technology sector began as early as the 1980s, but the most important stages of intensification of these activities took place in the late 1990s. During this period, a series of five-year development strategies were implemented, aimed at advancing science and technology, with a particular focus on information technology. These initiatives resulted in increased domestic production capacity for software and hardware, as well as priority development of numerical control technology, fibre optic infrastructure and communications networks for government, research and military applications[19].

The literature on the subject almost unanimously indicates that the Reconnaissance General Bureau (RGB), North Korean intelligence agency established in 2006, is responsible for most offensive operations (Figure 1)[20]. In addition to elite hacking units operating within RGB , there are also less specialised formations in North Korea that conduct operations in cyberspace but remain subordinate to other state institutions[21].

The United Front Department, operating within the structures of the Central Committee of the Worker's Party of Korea, plays a key role in propaganda operations. One of its fundamental tools is an extensive network with thousands of members whose activities focus on promoting pro-regime narratives and systematically undermining the credibility of opponents. This mechanism is based on coordinated disinformation activities conducted in the digital space and is commonly referred to as army of trolls[22]. An analysis conducted as part of research on propaganda strategies has shown that North Korea, unlike most countries, does not base its activities in this area on automation, but uses human resources as the main tool for carrying out information operations [23].

---

[19] J. Jun, S. LaFoy, E. Sohn, *North Korea's Cyber Operations*…, pp. 52–53.

[20] K. Ji Young, L. Jong In, K. Kyoung Gon, *The All-Purpose Sword: North Korea's Cyber Operations and Strategies*, in: *2019 11th International Conference on Cyber Conflict: Silent Battle*, T. Minárik., S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (eds.), Tallinn 2019, pp. 2–6; M. Barnhart et al., *Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations*, Mandiant, https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government#intelligencesubmenu [accessed: 19 XII 2024]; K. Chung, K. Lee, *Advancement of Science and Technology*…, pp. 23–26.

[21] M. Barnhart et al., *Not So Lazarus*…

[22] Ibid.

[23] S. Bradshaw, P.N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project, Oxford Internet Institute, 2017, p. 13.

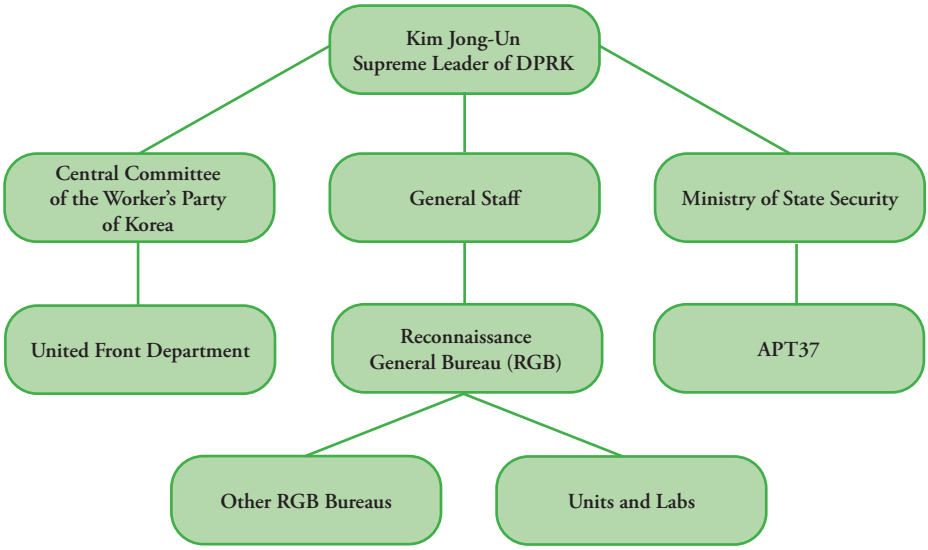

Figure 1. Cyber sector structure of the Democratic People's Republic of Korea.

Source: own elaboration based on: M. Barnhart et al., *Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations*, Mandiant, 23 III 2022, https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government#intelligencesubmenu [accessed: 19 XII 2024].

The structure of North Korean cyber groups is characterised by a high degree of specialisation and strict subordination to state security agencies. Among these entities, Group APT37, which is likely subordinate to the Ministry of State Security, is of particular importance. Its activities focus on gathering intelligence for the military, political and economic interests of North Korea. The group has been operating since at least 2012, initially focusing on the public and private sectors in South Korea. Since 2017, an expansion of its activities has been noted in Japan, Vietnam and the Middle East region. Group APT37 is interested in strategic sectors such as the chemical, electronics, aviation, automotive and healthcare industries. In recent years, its activity has clearly decreased, which, according to specialists from Mandiant, may indicate a consolidation of its structures within the framework of RGB[24].

The most important body conducting offensive operations remains Unit 121, operating within the framework of RGB. It is an elite structure whose members are carefully selected, and the unit itself consists of specialised subgroups responsible for various activities. One of these subgroups is Lab 110, which is sometimes

[24] M. Barnhart et al., *Not So Lazarus*…

identified with the name Lazarus. However, it is worth noting that in open sources, this name is often used collectively and covers various clusters of cyber activity related to North Korea[25]. There is no complete consensus on the boundaries between individual groups, which results both from the complex and dispersed nature of these structures and from the regime's deliberate policy of maintaining a high level of secrecy regarding its activities[26].

Smaller operational teams operate within Lab 110, among which the following stand out: TEMP.Hermit, APT38 and Andariel[27]. TEMP.Hermit, active since 2013, plays a key role in acquiring strategic data and focuses its activities on public administration as well as defence, telecommunications and finance sectors[28]. APT38 specialises in activities aimed at generating financial resources. It is responsible for some of the most serious attacks on financial institutions worldwide, including coordinated actions targeting the SWIFT interbank transfer system, banks, cryptocurrency exchanges and casinos. The losses caused by this formation amount to hundreds of millions of dollars[29]. Andariel, on the other hand, focuses its activities on foreign companies, government agencies, financial infrastructure and the defence sector. In addition to espionage, the group is involved in operations aimed at generating funds[30].

The Kimsuky group, which probably operates within the structures of the Ministry of State Security, is an important element of North Korean cyber landscape. This group, active since at least 2012, initially focused its activities on targets in South Korea, such as government institutions, research organisations as well as policy and security experts. In later years, its activities also extended to the United States, Russia, Europe and institutions of the United Nations. Kimsuky specialises in cyber intelligence focused on gathering information on foreign policy, national security, sanctions and nuclear programmes, targeting individuals with access to sensitive data in these areas[31].

The entire North Korean cyber operations system forms a highly organised, multi-level structure in which individual groups pursue intelligence, propaganda,

---

[25] The concept of the Lazarus group is understood differently by various centres and sources. The author uses this concept in the article in various contexts, depending on the sources he refers to.

[26] K. Chung, K. Lee, *Advancement of Science and Technology*…, pp. 23–26.

[27] *Lazarus Group*, MITRE ATT&CK, https://attack.mitre.org/groups/G0032/ [accessed: 17 XII 2024].

[28] M. Barnhart et al., *Not So Lazarus…*

[29] *APT38*, MITRE ATT&CK, https://attack.mitre.org/groups/G0082/ [accessed: 16 XII 2024].

[30] *Andariel*, MITRE ATT&CK, https://attack.mitre.org/groups/G0138/ [accessed: 16 XII 2024].

[31] M. Barnhart et al., *Not So Lazarus…; Kimsuky,* MITRE ATT&CK, https://attack.mitre.org/groups/G0094/ [accessed: 17 XII 2024].

destructive and financial objectives. In doing so, they support the strategic interests of the regime and its ability to project power globally.

Overview of the most profitable campaigns – banking sector

In 2016, news spread around the world about an attack on the Central Bank of Bangladesh, which ended with the theft of USD 81 million[32]. It was not possible to recover them because they had been laundered by employees of one of the Philippine banks involved in the practice[33]. This attack was the culmination of the process of shaping the North Korea's operational objectives in cyberspace. Until now, its activities have been limited mainly to infiltration, disruption, sabotage and intelligence operations. As a result of the attack, the group's range of targets has been expanded to include large-scale financial operations, which have generated significant financial gains for the regime's budget[34].

The nature of this aggressor's activities stood out among other criminal groups. Research has shown that hackers from North Korea sometimes spent up to several months conducting in-depth analysis of the target environment. A lot of time was devoted to learning about the internal policies and procedures used by the victims, with the aim of reducing the risk of detection by anomaly detection systems[35]. One of the final stages of reconnaissance was locating the server responsible for communication with the SWIFT system. The attackers had to establish a connection with numerous systems operating within a complex network topology. The goal was achieved due to the measures taken and the large scale of the operation. North Korean cybercriminals sought to steal a total of nearly one billion dollars. According to reports from the Federal Reserve Bank of New York, this institution contacted the Central Bank of Bangladesh after detecting an unusually high number of transactions directed to private entities and non-governmental organisations. As a result of the measures taken, the suspicious transactions were stopped and

[32] A. Haertle, *Jak zniknęło 81 milionów dolarów – historia prawdziwa* (Eng. How USD 81 million vanished – a true story), Zaufana Trzecia Strona, 20 III 2016, https://zaufanatrzeciastrona.pl/post/jak-zniknelo-81-milionow-dolarow-historia-prawdziwa/ [accessed: 19 XII 2024].

[33] M. Kabir, *Lessons Learned From the Bangladesh Bank Heist*, ISACA, 6 XII 2023, https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist [accessed: 18 XII 2024].

[34] *Dark Web Profile: Lazarus Group*, SOCRadar, https://socradar.io/apt-profile-who-is-lazarus-group/ [accessed: 13 IV 2024].

[35] J. DiMaggio, *Sztuka wojny cyfrowej*…, pp. 68–75.

the banks managed to block false transfers worth between USD 850 million and USD 870 million, preventing them from being transferred to the criminals' accounts[36].

After conducting a preliminary investigation, the Federal Reserve Bank reconstructed the detailed course of the transaction. The accounts presented show that during the acceptance of the first batch of transactions, several of the 30 orders were referred for further verification in terms of compliance with applicable sanctions. Subsequently, as a result of manual analysis, the Federal Reserve Bank of New York determined that the activity was potentially suspicious and that payment orders should not be executed without prior inquiry to the central bank[37].

The attack itself began with targeted phishing campaign that sent 25 emails. Post-compromise analysis revealed that malware had been downloaded onto at least three devices. The malicious code registered itself as a system service in an operating environment based on SWIFT Alliance[38], supported by Oracle Database. The software monitored financial messages transmitted over the SWIFT network and extracted key data such as transaction reference numbers and account numbers, which enabled the manipulation of data in the database. The key element of the attack was modifying local SWIFT Alliance Access installations by patching *liboradb.dll* module – the attackers replaced the conditional jump instruction with two NOP instructions[39]. This allowed security verification mechanisms to be bypassed. Additionally, the malware enabled continuous monitoring and modification of SWIFT messages by parsing files in designated system directories and generating valid SQL commands. As a result, records in the local database were deleted or modified. The patching process involved scanning active processes in search of the *liboradb.dll* file and modifying its memory, which enabled critical security controls to be bypassed and transaction data to be manipulated[40]. Subsequent analyses of the incident proved that the Central Bank of Bangladesh had committed numerous acts of negligence related to both the direct security

[36] *Dark Web Profile: Lazarus Group*…

[37] Federal Reserve Bank of New York, Responses to Rep. Maloney Letter of March 22, 2016, https://www.newyorkfed.org/medialibrary/media/newsevents/statements/2016/Maloneyletter.pdf [accessed: 11 XII 2024].

[38] SWIFT Alliance is the main communication server enabling connection to the SWIFT network. It enables the management of financial data flows, integrates various message formats and supports financial information exchange protocols.

[39] NOP instruction is a processor instruction that does not cause any changes in the state of the machine, except for incrementing the operation counter by one to indicate the next operation.

[40] S. Shevchenko, *Two Bytes to $951M*, BAE Systems, 25 IV 2016, https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html [accessed: 26 IV 2024].

of the sensitive system's infrastructure and its ability to detect threats in a timely manner.

Following this incident, individuals and organisations were held accountable, and it also led to the imposition of direct sanctions on the North Korean regime. On 8 June 2018, the U.S. Department of Justice published a notice about a crime committed by a citizen of the DPRK, Park Jin Hyok. The notification contained allegations of several cybercrimes[41]. They also included the attack on the Polish Financial Supervision Authority in 2016, which seriously threatened the Polish banking sector[42]. The identification of North Korea as the perpetrator of the Central Bank of Bangladesh attack was also used as evidence during the first ever imposition of sanctions for cyber attacks by the EU Council[43].

Overview of the most profitable campaigns – cryptocurrencies

In March 2022, one of the most serious hacker attacks in the cryptocurrency environment took place. The cybercriminals targeted the infrastructure of the Ethereum sidechain[44], which is part of the blockchain ecosystem[45] of the *Axie Infinity* game. Blockchain technology gains immense popularity, attracting millions of users with the ability to freely transfer digital assets. The attack was carried out by Lazarus Group known for its activities targeting the cryptocurrency sector. The hackers exploited the weakest point of the network, its validators, combining social engineering techniques with protocol security vulnerabilities. They managed to gain control over five of the nine private keys belonging to Ronin Network. The unauthorised access gained in this way allowed them to authorise transactions as a trusted entity. They then proceeded with a transaction

---

41 United States of America v. Park Jin Hyok, United States District Court for the Central District of California, MJ18-1479, 2018, pp. 23–125.

42 *Atak teleinformatyczny na polski sektor finansowy* (Eng. ICT attack on the Polish banking sector), Rządowe Centrum Bezpieczeństwa, in: https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [accessed: 5 IV 2024].

43 *Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*.

44 Ethereum is a decentralised blockchain platform that enables the creation and operation of smart contracts and decentralised applications. In addition to serving as a platform, Ethereum also has its own cryptocurrency, known as ether (ETH).

45 Blockchain is a decentralised ledger technology that enables transactions to be recorded in the form of a series of data blocks linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transactions, thus forming a chain of blocks.

in which they transferred the equivalent of USD 600 million in ether and USDC cryptocurrencies. This theft has been considered one of the largest in the history of decentralised finance[46].

After the successful theft, Lazarus Group began the complex process of laundering the stolen funds to make them harder to trace. To this end, the funds were transferred between multiple addresses, converted into other cryptocurrencies and passed through decentralised exchanges and mixers, which increase anonymity of transactions. Initially, some of the funds ended up on centralised exchanges, but when these began cooperating with law enforcement agencies, the hackers changed their strategy and started using tools that allowed them to conceal the flow of funds. As a result, a significant portion of the stolen assets were dispersed, making it difficult to recover them[47].

It was this security incident that contributed significantly to the tightening of measures of the U.S. Department of the Treasury against tools used to launder stolen funds. The Office of Foreign Assets Control systematically imposed sanctions on virtual currency mixers, such as Blender.io[48], Sinbad.io[49] and Tornado Cash[50], which played a key role in concealing income from cybercrime.

At the end of February 2025, the first reports emerged of a new theft targeting the Bybit exchange. It amounted to nearly USD 1.5 billion[51], which exceeds the total value of losses associated with cryptocurrencies attributed to North Korean hacker groups throughout 2024 (equivalent to USD 1.34 billion)[52]. Several

---

46 *Back to Building: Ronin Security Breach Postmortem*, Roninchain, 27 IV 2022, https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364 [accessed: 13 XII 2024].

47 *North Korea's Lazarus Group identified as exploiters behind $540 million Ronin bridge heist*, Elliptic, 14 IV 2022, https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge [accessed: 11 IV 2024].

48 *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, U.S. Department of the Treasury, 6 V 2022, https://home.treasury.gov/news/press-releases/jy0768 [accessed: 11 IV 2024].

49 *Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency*, U.S. Department of the Treasury, 29 XI 2023, https://home.treasury.gov/news/press-releases/jy1933 [accessed: 11 IV 2024].

50 *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. Department of the Treasury, 8 VIII 2022, https://home.treasury.gov/news/press-releases/jy0916 [accessed: 13 XI 2024].

51 *Bybit Hack: Leveraging Transparency for Collaboration in the Wake of Record-Breaking Theft*, Chainalysis, 24 II 2025, https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk/ [accessed: 10 III 2025].

52 Ibid.

months after the incident, both the US Federal Bureau of Investigation (FBI)[53] and independent blockchain analysis entities, including Chainalysis, claimed that a hacker group linked to the DPRK was behind the attack on the Bybit exchange[54]. Preliminary findings by investigators pointed to TraderTraitor group, also known as UNC4899, which the FBI officially linked to this incident[55]. Previously, the group was responsible for an attack on Japanese DMM Bitcoin Exchange, in which USD 308 million[56] was stolen, which was one of the largest single cybercrime operations in 2024. The Bybit reaction also points to North Korea as the perpetrator of the attack. General Director Ben Zhou announced decisive actions against Lazarus Group and stressed the need for global cooperation in combating cybercrime sponsored by the state[57]. The exchange has launched "Lazarus Bounty" recovery action programme, the name of which indicates the perpetrators of the attack[58].

The Sygnia report and NCC Group analysis show that the attack on the Bybit exchange was multi-stage and began with the compromise of the development environment associated with Safe{Wallet}, most likely as a result of social engineering techniques. The attackers gained access to the infrastructure and modified elements of the user interface by introducing malicious JavaScript code, which replaced the content of the transaction at the moment of its authorisation by authorised employees of Bybit. As a result, a transaction was approved, resulting in the attackers gaining control of the portfolio and stealing approx. 400 000 ether tokens[59]. Both analyses also noted that after the theft, the malicious

---

53 Federal Bureau of Investigation, *North Korea Responsible for $1.5 Billion Bybit Hack*, Internet Crime Complaint Center, 26 II 2025, https://www.ic3.gov/PSA/2025/PSA250226 [accessed: 15 III 2025].

54 *2025 Crypto Crime Mid-year Update: Stolen Funds Surge as DPRK Sets New Records*, Chainalysis, 17 VII 2025, https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/ [accessed: 10 X 2025].

55 Federal Bureau of Investigation, *North Korea Responsible for $1.5 Billion Bybit Hack*…

56 Federal Bureau of Investigation, *FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com*, 23 XII 2024, https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-usd-from-bitcoindmmcom [accessed: 10 X 2025].

57 B. Zhou (@benbybit), *Join us on war against Lazarus*, message on the X portal, 25 II 2025, https://x.com/benbybit/status/1894397098323579333 [accessed: 13 III 2025].

58 *ByBit*, Lazarus Bounty, https://www.lazarusbounty.com/en/ [accessed: 13 III 2025].

59 *Bybit – What We Know So Far*, Sygnia, 16 III 2025, https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/ [accessed: 10 X 2025]; M. Rivas, R. Santos, J. Sanz, *In-Depth Technical Analysis of the Bybit Hack*, NCC Group, 10 III 2025, https://www.nccgroup.com/research-blog/in-depth-technical-analysis-of-the-bybit-hack/ [accessed: 10 X 2025].

code was removed from the frontend, which hampered the investigation, and that the stolen funds were quickly dispersed among numerous wallets and transferred through decentralised exchanges and mixers, which combined with transaction masking highlights, indicates a high degree of sophistication on the part of the attackers[60].

The evidence cited indicates, with relatively high probability, the involvement of entities linked to North Korea, although at the time of writing this article, the attribution processes had not yet been ultimately completed.

Revenues from cybercriminal activities against the backdrop of sanctions regime

In response to the first nuclear tests conducted in 2006 by the DPRK, sanctions were imposed on the regime with the aim of limiting nuclear weapons proliferation and halting the development of weapons programmes. At that time, the UN Security Council introduced, among other things, an arms embargo, the freezing of assets of entities involved in the North Korean nuclear programme and partial restrictions on the import and export of goods that could support the development of weapons of mass destruction[61].

In parallel with the UN's regulations, independent sanctions were implemented by the EU[62], and the United States, South Korea, Japan and Australia, among others, applied unilateral measures[63]. Since 2016, sanctions against North Korea have been systematically tightened by both the UN and the EU in response to the regime's successive nuclear tests and ballistic missile tests. In addition to earlier restrictions on trade, the financial sector and the energy sector, restrictions on exports and imports, freezing of assets and a ban on economic cooperation have been extended. Personal

[60] Ibid.

[61] *UN Documents for DPRK (North Korea): Security Council Resolutions*, Security Council Report, https://www.securitycouncilreport.org/un_documents_type/security-council-resolutions/page/2?c-type=DPRK+%28North+Korea%29&cbtype=dprk-north-korea#038;cbtype=dprk-north-korea [accessed: 10 II 2025].

[62] *Unijne sankcje wobec Korei Północnej – kalendarium* (Eng. Timeline – EU sanctions against North Korea), Rada Europejska, Rada Unii Europejskiej, https://www.consilium.europa.eu/pl/policies/sanctions-against-north-korea/timeline-eu-sanctions-against-north-korea/ [accessed: 10 II 2025].

[63] *Democratic People's Republic of Korea Sanctions*, U.S. Department of State, https://www.state.gov/democratic-peoples-republic-of-korea-sanctions/ [accessed: 11 II 2025].

sanctions have also been imposed on individuals and entities associated with the North Korean arms programme[64].

In 2022, China and Russia opposed tougher sanctions against North Korea, arguing that the existing restrictions had not produced the desired results. Both countries described the draft resolution as counterproductive and inhumane. As a result, the UN Security Council was unable to adopt a resolution strengthening sanctions in response to the regime's ballistic missile tests. Despite the support of 13 members of the Council, the proposal submitted by the US was vetoed. The opposition of China and Russia, based on their belief that sanctions are ineffective and that dialogue is necessary, contrasts with the stance of other Council members, who are pushing for more decisive action against violations by North Korea. This impasse in the UN Security Council not only highlights the difficulties in reaching consensus on issues crucial to international stability, but also emphasises the need to seek new, more effective diplomatic solutions to reduce tensions on the Korean Peninsula[65].

The weakening of sanctions enforcement mechanisms culminated in the closure of the UN Panel of Experts on sanctions towards North Korea. This panel, operating since 2009 under the UN Security Council resolution 1874, played a key role in monitoring and reporting violations of sanctions imposed on the DPRK. Its activities were officially terminated in March 2024 as a result of a veto by the Russian Federation, which is another example of the growing division within the UN Security Council and the weakening of mechanisms for monitoring the enforcement of sanctions. The lack of an independent body to monitor the implementation of restrictions and analyse methods of circumventing them by the DPRK will make it much more difficult to monitor compliance with sanctions. This implies a potential weakening of pressure mechanisms on Pyongyang which has repeatedly demonstrated its ability to circumvent restrictions through networks of intermediaries and illicit transactions, often with the tacit support of some of states[66].

---

[64] O. Pietrewicz, *Ograniczenia polityki sankcji wobec Korei Północnej* (Eng. Limitations of the sanctions policy towards North Korea), Polski Instytut Spraw Międzynarodowych, 27 II 2018, https://pism.pl/publications/Limitations_of_the_Sanctions_Policy_towards_North_Korea [accessed: 19 XI 2024].

[65] *Security Council Fails to Adopt Resolution Tightening Sanctions Regime in Democratic People's Republic of Korea, as Two Members Wield Veto*, United Nations, 26 V 2022, https://press.un.org/en/2022/sc14911.doc.htm [accessed: 3 VIII 2024].

[66] *Update: DPRK (North Korea): Vote on Panel of Experts Mandate Renewal*, Security Council Report, 22 III 2024, https://www.securitycouncilreport.org/whatsinblue/2024/03/dprk-north-korea-vote-on-panel-of-experts-mandate-renewal.php [accessed: 3 II 2025].

Parallel to the diplomatic impasse, cybercrime activity in North Korea is on the rise. According to the March 2023 report of the UN Panel of Experts on sanctions towards North Korea, in 2022, the North Korean hackers stole the equivalent of between USD 630 million and over a billion dollars in cryptocurrency attacks[67]. The latest report from March 2024 indicates an amount of USD 750 million in 2023 and reports on an investigation into nearly 60 cyber attacks conducted between 2017 and 2023 linked to cryptocurrencies valued at approx. USD 3 billion[68].

Chainalysis report of 2025 confirms that North Korea maintains a dominant position in cybercrime related to cryptocurrencies. According to this report, in 2023 the North Korean hackers carried out 20 attacks on cryptocurrency exchanges and platforms, stealing the equivalent of approx. USD 660 million. In 2024, the number of incidents more than doubled to 47, and the total value of stolen funds reached, as mentioned, USD 1.34 billion, which is a twofold increase compared to the previous year. Hackers associated with Kim Jong Un's regime accounted for 61% of the total value of cryptocurrencies stolen in 2024, confirming their leading role in global cybercrime[69].

Taking into account the value of the funds gained by North Korean hackers, it seems reasonable to compare them with the country's available budget estimates for defence expenditure and GDP. However, it should be emphasised that these data should be interpreted with caution, due to both limited access to sources and the risk of attribution errors, including operations under false flag. Due to the hermetic nature of the DPRK regime, it is not possible to accurately estimate military expenditure, but the available data allows for approximate figures to be calculated. According to estimates by the U.S. Department of State, North Korea may have spent approx. USD 4 billion on defence in 2019, which represented 26% of its estimated GDP. It was the highest percentage among the 170 states analysed[70]. Stockholm International Peace Research Institute presented lower estimates, indicating that in 2018 North Korea's military expenditure amounted to approx. USD 1.6 billion[71].

---

[67] *Final report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (S/2023/171)*, UN Documents for DPRK (North Korea), 2023, pp. 74–78.

[68] *Final report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (S/2024/215)*, UN Documents for DPRK (North Korea), 2024, pp. 60–65.

[69] *The 2025 Crypto Crime Report*, Chainalysis, https://www.chainalysis.com/wp-content/uploads/2025/02/the-2025-crypto-crime-report-release.pdf [accessed: 8 III 2025].

[70] *World Military Expenditures and Arms Transfers 2021 Edition*, U.S. Department of State, 30 XII 2021, https://www.state.gov/world-military-expenditures-and-arms-transfers-2021-edition/ [accessed: 13 XII 2024].

[71] *SIPRI Military Expenditure Database*, Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/SIPRI-Milex-data-1949-2022.xlsx [accessed: 15 XII 2024].

To illustrate more fully the significance of the funds obtained from cybercrime, it is also worth referring to estimates of the total size of North Korea's economy. According to the report by the Bank of Korea, North Korea's real GDP amounted to approx. KRW 32 trillion, which, at the exchange rate current at the time of writing, corresponded to approx. USD 28 billion[72].

The data collected indicates that cybercrime is now not only a permanent feature of the DPRK's financial system, but also likely a tool that is becoming increasingly embedded in the institutional structure of the state's economy.

International reaction and its impact on North Korea's cyber activity

Public attribution in cyberspace, often equated with public stigmatisation (naming and shaming[73]), is sometimes seen as a deterrent, showing that it is possible to identify the perpetrators of attacks. However, as shown by the analysis presented in the work of Michael Poznansky and Evan Perkoski, the effectiveness of this tool is debatable, especially when it comes to entities that treat cyber activities as a means of projecting power. The authors emphasise that a decision of the perpetrator of a cyber attack to reveal their identity is closely linked to the goals they wish to achieve. States most often operate in secret when their goal is espionage or sabotage – in such cases, the success of the operation does not require the victim's cooperation, and anonymity minimises the risk of conflict escalation and retaliation. Disclosing one's role becomes important in coercive operations (cyber coercion), when achieving the desired result requires the target to know the identity of the aggressor and understand the threats of further action behind the attack[74].

In the light of this distinction, the public attribution of cyber activities as a standalone tool faces significant limitations with regard to states whose priority is global power projection, such as North Korea. This regime has repeatedly been involved in operations targeting Western countries, including the attack on the Central Bank of Bangladesh and ransomware campaigns, such as WannaCry

---

[72] *Gross Domestic Product Estimates for North Korea in 2023*, Bank of Korea, 26 VII 2024, https://www.bok.or.kr/eng/bbs/E0000634/view.do?nttId=10086116&menuNo=400423&relate=Y&depth=400423&programType=newsDataEng [accessed: 11 II 2025].

[73] *Naming and shaming* is a term which means a strategy of enforcing standards and human rights by publicly condemning countries that commit violations.

[74] M. Poznansky, E. Perkoski, *Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution*, "Journal of Global Security Studies" 2018, vol. 3, no. 4, pp. 402–416. https://doi.org/10.1093/jogss/ogy022.

in 2017. In both cases, the US decided to publicly assign responsibility for the attacks, which can be interpreted as an attempt to weaken Pyongyang's international position and influence its future strategic decisions. However, practice to date has not confirmed the clear effectiveness of this approach, which raises questions about the actual effectiveness of public attributions in relation to isolated regimes.

The effectiveness of public attribution as a deterrent tool may be significantly limited in the case of North Korea for several reasons. Firstly, totalitarian regimes, such as the North Korean, are characterised by low susceptibility to pressure from the international community, and disclosure of their activities in cyberspace rarely translates into real political costs within the system of power. Secondly, limited integration of North Korea with global digital infrastructure and its peripheral position in the international economic system means that retaliatory measures, both cybernetic and economic, do not have a sufficiently strong impact on this entity. The asymmetry in the degree of digitalisation and dependence on global technology networks between North Korea and highly developed Western countries reduces the potential effectiveness of retaliation. Thirdly, public attribution of attacks may generate unintended effects that strengthen the regime and contribute to building its position as an entity with advanced cyber capabilities and capable of projecting power globally, which may be part of a broader deterrence policy strategy pursued by Pyongyang.

Attribution also serves to legitimise retaliatory actions, including economic sanctions or defensive operations. For example, identification of North Korea as the perpetrator of the attack on the Central Bank of Bangladesh, as indicated, was used during the first-ever imposition of sanctions by the EU Council for cyber attacks[75].

According to some researchers, it can be convincingly argued that, in accordance with the international law, states should carry out proper and reliable attribution before taking retaliatory action in response to a cyber attack, especially if such action could otherwise violate international norms[76]. The process requires the presentation of credible and clear evidence that unequivocally identifies the perpetrator, and confirms their responsibility for a specific attack. This requirement complies with the principles of proportionality and necessity, which are fundamental elements of the international law. Reliable attribution not only legitimises state actions, but

[75] *Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.*

[76] M. Finnemore, D.B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, "European Journal of International Law" 2020, vol. 31, no. 3, pp. 975–1003. https://doi.org/10.1093/ejil/chaa056.

also minimises the risk of conflict escalation and supports stability in international relations, while limiting the arbitrariness of decisions taken[77].

The most intense unilateral actions against North Korea's cyber attacks can be considered those taken by the US, including the aforementioned notification of a crime committed by the DPRK's citizen – Park Jin Hyok. Since then, the US consistently have been using indictments as a tool to attribute cyber attacks to North Korea[78]. An example is the indictment concerning Rim Jong Hyok, who carried out attacks mainly on hospitals and private companies in the health care sector of the US and South Korea using malware such as ransomware[79].

There is no doubt that the DPRK has significantly contributed to the dynamic development of Western countries' approach to the phenomenon of attribution of cyber attacks. Although profit-driven criminal activity does not seem to occur less frequently in North Korea than a few years ago (the latest data indicate an upward trend), it should be remembered that the practice of such criminal activity by state regimes is relatively new. It has been going on for just over a decade. More and more countries and international organisations are deciding to counteract this by using measures such as public attribution or sanctions. Although these measures do not have sufficient support in international law, their more frequent use seems promising, because it gradually increases the political and operational costs for the DPRK.

Conclusions

Criminal cyber activity is one of the most important sources of funding for the North Korea's regime. In the context of international sanctions imposed on the DPRK, the scale of funds obtained in this way should not be underestimated, especially in light of the growing likelihood that they contribute to the financing of arms programmes.

Analysis of available data indicates a consistent increase in the effectiveness of cyber operations conducted by North Korea. Both the analysis of figures from publicly available reports and the noticeable decline in the effectiveness of mechanisms monitoring compliance with sanctions do not indicate that this

[77] Ibid.

[78] United States of America v. Park Jin Hyok, United States District Court for the Central District of California, CR 2:18-cr-00759, 2018; United States of America v. J. Chang Hyok, K. Il, and P. Jin Hyok, United States District Court for the Central District of California, CR 2:20-cr-00614-DMG, 2020.

[79] United States of America v. Rim Jong Hyok, United States District Court for the District of Kansas, 24-20061-HLT-ADM, 2024, pp. 1–17.

practice will change radically. On the contrary, the DPRK's hacking operations since around 2013 have shown increasing effectiveness, posing a significant challenge to international efforts to enforce restrictions.

The dissolution of one of the key bodies monitoring the DPRK's activities – the UN Panel of Experts on sanctions towards North Korea – is a worrying sign. This decision has significantly weakened the international system for monitoring North Korean sanctions violations and the ability to report such activities to the UN. This may result in a further intensification of the regime's criminal activity in cyberspace, especially as the dissolution of the panel seems to coincide with increased military and economic cooperation between North Korea and the Russian Federation[80].

Despite difficult conditions, there are visible signs of growing interest in developing capabilities to attribute responsibility for cyber attacks to specific state actors. Initially, these actions were launched mainly by the United States, but since the beginning of the third decade of the 21st century, there has been a noticeable increase in the number of international attribution coalitions and greater involvement of actors such as the EU (supranational nature of the organisation). Scientific activity aimed at improving the mechanisms of state accountability for their cyber activities is also increasing. Although these trends represent a step towards greater transparency and accountability for cyber operations, their dynamics does not seem intense enough to effectively curb cybercrime in the coming years. The possible effects of these measures should rather be considered in the long term.

It is worth to emphasise that the effectiveness of public attributions with regard to the North Korea remains limited, as a regime that is highly isolated internationally does not necessarily respond in a conventional manner to being held accountable. The deterrent function of public attributions may be of secondary importance compared to their leading role in shaping political narratives and mobilising support for specific state actions in the area of security. In this context, it is important to strengthen international cooperation mechanisms and continue efforts to adequately document sanctions violations. The efforts of attribution coalitions may partially fill the gap left by the UN Panel of Experts on sanctions towards North Korea, but their effectiveness will depend on the level of engagement of the international community and the ability to build a broad consensus on responsibility for cyber operations.

---

[80] O. Guseinova, *Unequal Partnership: North Korea's Uneven Bargain with Russia*, Friedrich Naumann Foundation for Freedom Korea, 2024, https://shop.freiheit.org/#!/Publikation/1997 [accessed: 10 X 2025]; O. Pietrewicz, *Wzmocnienie wsparcia Korei Północnej dla rosyjskiej wojny przeciwko Ukrainie* (Eng. North Korea increasing its support for Russia in the war in Ukraine), Polski Instytut Spraw Międzynarodowych, 18 XI 2024, https://www.pism.pl/publications/north-korea-increasing-its-support-for-russia-in-the-war-in-ukraine [accessed: 10 X 2025].

Bibliography

Banks W., *Cyber Attribution and State Responsibility*, "International Law Studies" 2021, vol. 97, pp. 1039–1072.

Baszkiewicz J., *Władza* (Eng. Power), Wrocław 1999.

Bradshaw S., Howard P.N., *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project, Oxford Internet Institute, 2017.

Chung K., Lee K., *Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of highlights and Unmanned Aerial Vehicle*, Seoul 2017.

DiMaggio J., *Sztuka wojny cyfrowej. Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej* (Eng. The art of cyberwarfare: an investigator's guide to espionage, ransomware and organised cybercrime), Warszawa 2023.

Eichensehr K.E., *The Law and Politics of Cyberattack Attribution*, "UCLA Law Review" 2020, vol. 67, pp. 520–598.

Finnemore M., Hollis D.B., *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, "European Journal of International Law" 2020, vol. 31, no. 3, pp. 969–1003. https://doi.org/10.1093/ejil/chaa056.

Guerrero-Saade J.A., Raiu C., *Walking in your enemy's shadow: when fourth-party collection become attribution hell*, Virus Bulletin, 2017.

Ji Young K., Jong In L., Kyoung Gon K., *The All-Purpose Sword: North Korea's Cyber Operations and Strategies*, in: *2019 11th International Conference on Cyber Conflict: Silent Battle*, T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (eds.), Tallinn 2019.

Jun J., LaFoy S., Sohn E., *North Korea's Cyber Operations: Strategy and Responses*, Center for Strategic & International Studies, 2023.

Lin H., *Attribution of Malicious Cyber Incidents*, "Aegis Paper Series" 2016, no. 1607, pp. 1–55.

Mueller M., Grindal K., Kuerbis B., Badiei F., *Cyber Attribution: Can a New Institution Achieve Transnational Credibility?*, "The Cyber Defense Review" 2019, vol. 4, no. 1, pp. 107–122.

Poznansky M., Perkoski E., *Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution*, "Journal of Global Security Studies" 2018, vol. 3, no. 4, pp. 402–416. https://doi.org/10.1093/jogss/ogy022.

Rid T., Buchanan B., *Attributing Cyber Attacks*, "Journal of Strategic Studies" 2015, vol. 38, no. 1–2, pp. 4–37. http://dx.doi.org/10.1080/01402390.2014.977382.

Skopik F., Pahi T., *Under false flag: using technical artifacts for cyber attack attribution,* "Cybersecurity" 2020, vol. 3, pp. 1–20. https://doi.org/10.1186/s42400-020-00048-4.

Stewart S.R., *DPRK Overseas Financial Networks*, in: *People for Profit: North Korean Forced Labour on a Global Scale*, R.E. Breuker, I.B.L.H. van Gardingen (eds.), Leiden 2018, pp. 120–125.

Yin R.K., *Studium przypadku w badaniach naukowych. Projektowanie i metody* (Eng. Case study research. Design and methods), Kraków 2015.

Internet sources

2025 Crypto Crime Mid-year Update: Stolen Funds Surge as DPRK Sets New Records, Chainalysis, 17 VII 2025, https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/ [accessed: 10 X 2025].

Andariel, MITRE ATT&CK, https://attack.mitre.org/groups/G0138/ [accessed: 16 XII 2024].

APT38, MITRE ATT&CK, https://attack.mitre.org/groups/G0082/ [accessed: 16 XII 2024].

Atak teleinformatyczny na polski sektor finansowy (Eng. Cyberattack on the Polish financial sector), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [accessed: 5 IV 2024].

Back to Building: Ronin Security Breach Postmortem, Roninchain, 27 IV 2022, https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364 [accessed: 13 XII 2024].

Barnhart M., Cantos M., Johnson J., Fox E., Freas G., Scott D., *Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations*, Mandiant, https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government#intelligencesubmenu [accessed: 19 XII 2024].

Bybit – What We Know So Far, Sygnia, 16 III 2025, https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/ [accessed: 10 X 2025].

Bybit Hack: Leveraging Transparency for Collaboration in the Wake of Record-Breaking Theft, Chainalysis, 24 II 2025, https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk/ [accessed: 10 III 2025].

ByBit, Lazarus Bounty, https://www.lazarusbounty.com/en/ [accessed: 13 III 2025].

Dark Web Profile: Lazarus Group, SOCRadar, https://socradar.io/apt-profile-who-is-lazarus-group/ [accessed: 13 IV 2024].

Democratic People's Republic of Korea Sanctions, U.S. Department of State, https://www.state.gov/democratic-peoples-republic-of-korea-sanctions/ [accessed: 11 II 2025].

Federal Bureau of Investigation, *FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin. DMM.com*, 23 XII 2024, https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of--308-million-usd-from-bitcoindmmcom [accessed: 10 X 2025].

Federal Bureau of Investigation, *North Korea Responsible for $1.5 Billion Bybit Hack*, Internet Crime Complaint Center, 26 II 2025, https://www.ic3.gov/PSA/2025/PSA250226 [accessed: 15 III 2025].

Federal Reserve Bank of New York, Responses to Rep. Maloney Letter of March 22, 2016, https://www.newyorkfed.org/Maloneyletter.pdf [accessed: 11 XII 2024].

Garamone J., *Pentagon Says 10K North Korean Troops in Kursk Oblast*, U.S. Department of War, 4 XI 2024, https://www.defense.gov/News/News-Stories/Article/Article/3955757/pentagon-says-10k-north-korean-troops-in-kursk-oblast/ [accessed: 18 III 2025].

Gross Domestic Product Estimates for North Korea in 2023, Bank of Korea, 26 VII 2024, https://www.bok.or.kr/eng/bbs/E0000634/view.do?nttId=10086116&menuNo=400423&relate=Y&depth=400423&programType=newsDataEng [accessed: 11 II 2025].

Guseinova O., Unequal Partnership: North Korea's Uneven Bargain with Russia, "Friedrich Naumann Foundation for Freedom Korea" 2024, https://shop.freiheit.org/#!/Publikation/1997 [accessed: 10 X 2025].

Haertle A., *Jak zniknęło 81 milionów dolarów – historia prawdziwa* (Eng. How USD 81 million vanished – a true story), Zaufana Trzecia Strona, 20 III 2016, https://zaufanatrzeciastrona.pl/post/jak-zniknelo-81-milionow-dolarow-historia-prawdziwa/ [accessed: 19 XII 2024].

Kabir M., *Lessons Learned From the Bangladesh Bank Heist*, ISACA, 6 XII 2023, https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist [accessed: 18 XII 2024].

Kimsuky, MITRE ATT&CK, https://attack.mitre.org/groups/G0094/ [accessed: 17 XII 2024].

Lazarus Group, MITRE ATT&CK, https://attack.mitre.org/groups/G0032/ [accessed: 17 XII 2024].

North Korea's Lazarus Group identified as exploiters behind $540 million Ronin bridge heist, Elliptic, 14 IV 2002, https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge [accessed: 11 IV 2024].

Pietrewicz O., *Ograniczenia polityki sankcji wobec Korei Północnej* (Eng. Limitations of the sanctions policy towards North Korea), Polski Instytut Spraw Międzynarodowych, 27 II 2018, https://pism.pl/publications/Limitations_of_the_Sanctions_Policy_towards_North_Korea [accessed: 19 XI 2024].

Pietrewicz O., *Wzmocnienie wsparcia Korei Północnej dla rosyjskiej wojny przeciwko Ukrainie* (Eng. North Korea increasing its support for Russia in the war in Ukraine), "Biuletyn Polskiego Instytutu Spraw Międzynarodowych" no. 171 (2981), 18 XI 2024, https://www.pism.pl/publications/north-korea-increasing-its-support-for-russia-in-the-war-in-ukraine [accessed: 10 X 2025].

Rivas M., Santos R., Sanz J., *In-Depth Technical Analysis of the Bybit Hack*, NCC Group, 10 III 2025, https://www.nccgroup.com/research-blog/in-depth-technical-analysis-of-the--bybit-hack/ [accessed: 10 X 2025].

Security Council Fails To Adopt Resolution Tightening Sanctions Regime In Democratic People's Republic Of Korea, As Two Members Wield Veto, United Nations, 26 V 2022, https://press.un.org/en/2022/sc14911.doc.htm [accessed: 3 VIII 2024].

Shevchenko S., *Two Bytes to $951M*, BAE Systems, 25 IV 2016, https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html [accessed: 26 IV 2024].

SIPRI Military Expenditure Database, Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/SIPRI-Milex-data-1949-2022.xlsx [accessed: 15 XII 2024].

Starks C., Barnhart M., Long T., Lombardi M., Pisano J., Revelli A., *Staying a Step Ahead: Mitigating the DPRK IT Worker Threat*, Mandiant, 23 IX 2024, https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat [accessed: 8 III 2025].

The 2025 Crypto Crime Report, Chainalysis, https://www.chainalysis.com/wp-content/uploads/2025/02/the-2025-crypto-crime-report-release.pdf [accessed: 8 III 2025].

Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency, U.S. Department of the Treasury, 29 XI 2023, https://home.treasury.gov/news/press-releases/jy1933 [accessed: 11 IV 2024].

UN Documents for DPRK (North Korea): Security Council Resolutions, Security Council Report, https://www.securitycouncilreport.org/un_documents_type/security-council-resolutions/page/2?ctype=DPRK+%28North+Korea%29&cbtype=dprk-north-korea#038;cbtype=dprk-north-korea [accessed: 10 II 2025].

Unijne sankcje wobec Korei Północnej – kalendarium (Eng. Timeline – EU sanctions against North Korea), Rada Europejska, Rada Unii Europejskiej, https://www.consilium.europa.eu/pl/policies/sanctions-against-north-korea/timeline-eu-sanctions-against-north-korea/ [accessed: 10 II 2025].

Update: DPRK (North Korea): Vote on Panel of Experts Mandate Renewal, Security Council Report, 22 III 2024, https://www.securitycouncilreport.org/whatsinblue/2024/03/dprk-north-korea-vote-on-panel-of-experts-mandate-renewal.php [accessed: 3 II 2025].

U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats, U.S. Department of the Treasury, 6 V 2022, https://home.treasury.gov/news/press-releases/jy0768 [accessed: 11 IV 2024].

U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, U.S. Department of the Treasury, 8 VIII 2022, https://home.treasury.gov/news/press-releases/jy0916 [accessed: 13 XI 2024].

World Military Expenditures and Arms Transfers 2021 Edition, U.S. Department of State, 30 XII 2021, https://www.state.gov/world-military-expenditures-and-arms-transfers-2021-edition/ [accessed: 13 XII 2024].

Zhou B. (@benbybit),, *Join us on war against Lazarus*, message on the X portal, 25 II 2025, https://x.com/benbybit/status/1894397098323579333 [accessed: 13 III 2025].

Legal acts

Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (Official Journal of the EU L 246/4 of 30 VII 2020).

Other documents

United States of America v. J. Song Hwa, R. Kyong Sik, K. Ryu Song et al., United States District Court for the Eastern District of Missouri, CR 4:24CR648 MTS/JSD, 2024.

United States of America v. Rim Jong Hyok, United States District Court for the District of Kansas, 24-20061-HLT-ADM, 2024.

United States of America v. J. Chang Hyok, K. Il, and P. Jin Hyok, United States District Court for the Central District of California, CR 2:20-cr-00614-DMG, 2020.

United States of America v. Park Jin Hyok, United States District Court for the Central District of California, MJ18-1479, 2018.

United States of America v. Park Jin Hyok, United States District Court for the Central District of California, CR 2:18-cr-00759, 2018.

Final report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (S/2023/171), UN Documents for DPRK (North Korea), 2023.

Final report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (S/2024/215), UN Documents for DPRK (North Korea), 2024.

Sebastian Jeż

PhD candidate at the Doctoral School of Social Sciences of the University of Warsaw and cyber security specialist. Graduate of De Montfort University and University of Warsaw. Since 2016, he has been involved in the field of technical cybersecurity, and since 2020, he has been focusing on its offensive dimension and interdisciplinary research at the intersection of technology and political science.

Contact: s.jez@uw.edu.pl