
DECODING CRIMES
UNVEILING NORTH KOREA'S
CYBER THREATS
PSCORE
People for Successful COrean REunification

Ver. 1.0

Decoding Crimes:

Unveiling North Korea's Cyber Threats

People for Successful COrean REunification

(PSCORE)

This report was created with the support of
the Embassy of Canada to the Republic of Korea

ACKNOWLEDGMENTS

We want to thank the following people for their contribution to this report:

Publisher: Kim Tae-hoon

Editor in chief: Nam Bada

Authors:

Elma Duval, Yunah Jang, Camille Retailleau, Kim Young-Sung, Nam Bada

Co-Authors:

Simon Lunding, Anita Osae, Jasmin Ringel, Wang Hong Zhun

Interviewers:

Nam Bada, Elma Duval, Yunah Jang, Jasmin Ringel

Other contributors:

Sam Boezeman, Laura Demeulenaere, Gaia Gentile, Kim Ho, Bertille Holtz, Annsophie Mueller, Helena Nikolajew, Sean Oh, Lou Perruchot, Frederike Schötker, Park Hanna

Cover design:

Giorgia Natalia Patti, Mariana Sotelo

Created with the help of ChatGPT, Canva and Affinity

We would also like to express our sincere appreciation to all the North Korean defectors and the Human Rights Activists who shared their experiences for this report. Without their contributions, this report would not have been possible.

GREETINGS

In an era where the digital frontier increasingly shapes the landscape of human rights, PSCORE presents this report “Decoding crimes: Unveiling North Korea’s cyberthreats." This document goes beyond research; it sheds light on North Korea’s persistent and evolving cyber threats, which often go unnoticed and are underestimated.

The global community cannot afford to overlook the significant impact of state-sponsored cyber activities. These are not distant, abstract concerns—they have real-world consequences for individual’s freedoms, security, and dignity worldwide. Our analysis highlights how such operations are not merely about data breaches but are tools of control and manipulation.

This report seeks to shift the conversation about cybersecurity from a purely technical issue to one that is deeply intertwined with human rights. It underscores the need for cohesive international efforts, stronger accountability measures, and proactive responses to these growing digital threats.

We present this report as a call to action. The insights and evidence within are meant to provoke thought, inspire responsibility, and catalyze meaningful responses. Cyber threats are not a distant challenge for tomorrow—they are a pressing reality today, demanding vigilance, collaboration, and resolve from all of us.

Kim Tae-Hoon
President of PSCORE

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

- CEDAW - Convention on the Elimination of All Forms of Discrimination Against Women
- CRC - Convention on the Rights of the Child
- CRPD - Convention on the Rights of Persons with Disabilities
- CSOs - Civil Society Organizations
- HRC - Human Rights Council
- ICC - International Criminal Court
- ICCPR - International Covenant on Civil and Political Rights
- ICESCR - International Covenant on Economic, Social and Cultural Rights
- IT - Information Technology
- NGOs - Non-Governmental Organizations
- OHCHR - Office of the High Commissioner for Human Rights (informally named as United Nations Human Rights Office (UNHR Office)
- PoE - Panel of Experts
- UDHR - Universal Declaration of Human Rights
- UN ECOSOC - United Nations ECOnomic and SOcial Council
- UNSC - United Nations Security Council
- WMD - Weapon of Mass Destruction

ABSTRACT

This report demonstrates the direct connection between North Korea's cyber threats and Human Rights violations through extensive interviews, data analyses, and survey findings. It unequivocally reveals that North Korea's cyber activities have caused significant harm to individuals, which is underscored by our numerous testimonies on the reality of these violations.

Although cyber threats are not yet universally recognized as a form of Human Rights violation under international law, this report argues that the trajectory of global policy is shifting toward such recognition. By presenting evidence, this study aims to contribute to this shift and establish cyber threats as a critical component of Human Rights discourse.

North Korea's cyber capabilities, notorious for their severity, serve as a key focus of this analysis. The report draws upon evidence from diverse sectors to substantiate the claim that North Korea's cyber activities result in profound Human Rights violations.

The findings are organized into the following parts: an examination of North Korea's cyber threat landscape and its implications for Human Rights; an analysis of the legal, international, and regional responses to these threats; and recommendations to address the growing intersection of cybersecurity and Human Rights.

Through this comprehensive assessment, the report not only highlights the urgent need to address cyber threats as a form of Human Rights violation but also reinforces the call for stronger legal frameworks and international cooperation to mitigate their impact.

Introduction

"Cyber space has kicked the doors wide open, anyone can walk through and many are. Malicious activity is on the rise by most state and non-state actors and by outright criminals."

- UN Secretary-General António Guterres[1]
20 June 2024

"Modern life is inseparable from the online world, but because of these threats, it feels impossible to live safely."

- Sa Hye-Jun [2]
North Korean defector

In an age where digital technologies permeate nearly all aspects of modern society, the intersection of cybersecurity and Human Rights represents a critical yet insufficiently regulated domain. State-sponsored cyber operations, particularly those conducted by North Korea, pose not only a significant threat to global stability but also profoundly undermine fundamental Human Rights and freedoms. This report seeks to critically examine this pressing issue, highlighting how cyber threats function as instruments of both external aggression and internal repression, with far-reaching implications for individuals and institutions alike. Through a mixed method approach that combines testimonies from qualitative interviews with victims, a comprehensive survey, and secondary sources

[1] António Guterres, 'Secretary-General's Remarks to the Security Council's High-Level Debate on "Maintenance of International Peace and Security: Addressing Evolving Threats in Cyberspace,"' United Nations, June 20, 2024, https://www.un.org/sg/en/content/sg/statement/2024-06-20/secretary-generals-remarks-the-security-council%E2%80%99s-high-level-debate-%E2%80%9Cmaintenance-of-international-peace-and-security-addressing-evolving-threats-cyberspace%E2%80%9D

[2] Sa Hye-Jun, interview by Nam Bada, PSCORE, October 24, 2024.

we provide insights into the dual-sided nature of this issue—examining both the external impacts of North Korea's cyber activities against institutions, organizations, and, most critically, individuals and the internal Human Rights violations suffered by the regime's cyber agents. Our findings demonstrate that North Korea's cyber operations are not only tools of global disruption but also mechanisms that systematically infringe on several fundamental Human Rights. By drawing upon the voices of those most affected, we aim to elevate cyber threats as a critical component of Human Rights discourse, as cyber threats are not yet universally recognized as a form of Human Rights violations under international law. Therefore, this analysis makes a compelling case for such recognition and advocates for stronger international legal frameworks to address them.

The report begins by laying a foundational understanding by introducing key concepts of Human Rights and cybersecurity, and the nature and scope of cyber threats. This opening also examines North Korea's international commitments and charts the evolution of its cyber operations, establishing a framework for the subsequent discussion. The analysis then shifts to a thorough investigation of North Korea's cyber capabilities and practices. This section delves into the regime's methods for executing cybercrimes, focusing on key targets. It also unpacks the sophisticated techniques employed to further their pernicious interests. Then, the study addresses the Human Rights implications of these cyber activities. It identifies specific rights violated and examines the tangible consequences for victims, including psychological and long-term impacts. In addition, this segment sheds light on the internal Human Rights abuses faced by North Korean cyber operatives, offering a dual perspective on the issue. To conclude, the report then evaluates the responses to North Korean cyber threats at the international and national levels. It assesses their effectiveness and highlights the challenges in countering the regime's activities. Based on these findings, the study emphasizes the urgent need for global recognition of cyber threats as a significant form of Human Rights violations.

Methodology

The methodology of this report is mainly grounded in primary research, combining interviews and surveys to provide firsthand insights into the impact of North Korean cyber threats. Central to the analysis are 15 semi-structured interviews conducted face-to-face or via phone with North Korean defectors, Human Rights activists, and professionals directly impacted by cyberattacks. Semi-structured interviews facilitated an open and flexible dialogue, allowing participants to share their experiences freely within a structured framework. This approach balanced methodological rigor with adaptability, encouraging candid discussions and uncovering nuanced insights that would otherwise remain obscured in overly structured formats. The interviews examined both the technical and emotional dimensions of cyberattacks, addressing hacking methods, their immediate and long-term consequences, and the coping mechanisms employed by those affected. To safeguard participants' privacy and ensure their well-being, pseudonyms enabled interviewees to speak openly without fear of repercussions. The findings underscored not only the resilience of those impacted by these attacks but also their unwavering commitment to continuing their advocacy and professional endeavors despite the considerable challenges they face.

No.	Date	Name (some pseudonyms)	Profession
1	September 2nd, 2022	Kim Hyun-seong	North Korean Defector
2	October 21st, 2022	Jeong Sung-jae	North Korean Defector
3	June 1st, 2024	Jeon Dong-min	IT expert
4	July 8th, 2024	Kim Ji-min	IT expert
5	October 6th, 2024	Kim Ju-won	IT Workers

No.	Date	Name (some pseudonyms)	Profession
6	October 23rd, 2024	Daily NK reporter	Reporter
7	October 24th, 2024	Kang Shin-sam	NGO president
8	October 24th, 2024	Sa Hye-Jun	Media and production
9	November 13th, 2024	Jung Yuna	Youtuber / Influencer
10	November 15th, 2024	Na Jeong-Seok	IT Worker
11	December 15th, 2024	Heo Jeong-Yoon	NGO president
12	December 17th, 2024	Jang Hui-Joo	North Korean Defector
13	December 17th, 2024	Park Seong-Min	Media and production
14	December 24th, 2024	Lee Sang-Hyuk	North Korean Defector
15	December 23rd, 2024	John Smith	NGO President

Complementing the interviews, an online survey titled *"북한 사이버 위협(해킹 포함) 관련 설문"* (Survey Related to North Korea's Cyber Threats, Including Hacking) was conducted by PSCORE in late 2024. Of the 226 participants, 198 responses were selected and analyzed, with 54 identifying as hacking victims. The survey captured diverse perspectives from defectors of varying socio-economic and geographic backgrounds as well as different years of defection, offering a broader quantitative context to the qualitative findings. The period covered in the analysis extends from the interviewees' arrival in South Korea to the present. By integrating interviews and survey data, this report delivers a comprehensive analysis of North Korean cyber threats, exposing their risks to privacy, personal security, and Human Rights while underscoring the urgent need for strengthened cybersecurity measures.

Through this unique lens and comprehensive assessment, PSCORE offers an in-depth understanding and instrumental evidence that distinguishes our work from other NGOs. This report bridges the gap between cybersecurity and Human Rights advocacy, laying the groundwork for tangible progress in addressing one of the most insidious threats of our digital time.

1. Cybersecurity and Human Rights: Concepts, Treaties and Threats

The opening section introduces a comprehensive overview, which includes a detailed examination of the three generations of Human Rights, alongside a conceptual definition of cybersecurity. This section outlines the nature and scope of cyber threats, laying the groundwork for the subsequent analysis. Furthermore, it delves into North Korea's global commitments, tracking the evolution of its cyber operations and providing the critical context necessary for understanding the study's broader implications. The following definitions are designed to offer readers a solid foundation in the key terminologies that recur throughout the analysis. The report seeks to eliminate potential confusion and enhance comprehension by establishing clear and precise definitions. This approach facilitates accessibility for a diverse audience, enabling a more effective engagement with the content.

1.1. Human Rights According to the International Legislation

According to the Universal Declaration of Human Rights (UDHR), "Human Rights are rights we have, simply because of our existence as human beings which are not granted by any state".[3] These universal rights apply to all of us, irrespective of nationality, sex, ethnic origin, skin color, religion, language, or any other status. They range from the most fundamental - the right to life - to basic necessities, such as the rights to food, education, work, health, and liberty. The UDHR, adopted by the UN General Assembly in 1948, was the first legal document to outline the fundamental Human Rights that should be universally protected.[4]

However, in the evolving digital age, the concept of Digital Human Rights remains underdeveloped and not yet widely accepted. With growing digital reliance, there is a push to recognize digital rights as fundamental Human Rights by 2030, marking an important step toward addressing inequalities in digital access and opportunities.[5] To understand the broader framework of Human Rights, it is useful to explore the three generations of Human Rights theory, which categorizes Human Rights based on their historical development and conceptual focus. This theory provides valuable insight into the evolution of Human Rights, the conceptual distinction, and how they can adapt to emerging societal challenges, including those posed by the digital age. Below, we outline the three generations of Human Rights, first classified this way by the Czech-French jurist Karel Vasak in 1977.

[3] United Nations General Assembly, *Universal Declaration of Human Rights*, 217 A (III), December 10, 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[4] OHCHR, "What Are Human Rights?," accessed January 15, 2025, https://www.ohchr.org/en/what-are-human-rights.
[5] United Nations, *Transforming Our World: The 2030 Agenda for Sustainable Development*, 2015, https://sdgs.un.org/2030agenda.

1.1.1. The First Generation of Human Rights: Civil and Political Rights

The first generation of Human Rights[6], also known as 'blue rights', were derived in the 18th century, primarily focusing on protecting individual freedoms from infringement by governments and private entities. These rights emphasize civil and political liberties and are often categorized as negative rights[7], which include the right to security (Article 5 of the Human Rights Act[8] issued by the parliament of the United Kingdom in 1998), the right to privacy (Article 17 of the International Covenant on Civil and Political Rights (ICCPR))[9], and the freedom of expression (Article 19 of the ICCPR), serving to protect individuals from state and private interference, focusing on freedom from arbitrary power rather than entitlements.

1.1.2. The Second Generation of Human Rights: Economic, Social, and Cultural Rights

The second generation of Human Rights, sometimes referred to as 'red rights', was formulated in the 19th century[10] and influenced by socialist traditions. They emphasize the importance of equal social conditions and access to resources, addressing social, economic, and cultural needs. As opposed to the first generation of Human Rights, the second generation mainly focuses on positive rights instead of negative rights to counter capitalistic endeavors. They impose the duty of fulfilment on governments provided the availability of resources. Drawing from socialist traditions, these positive rights - such as the right to education (Article 13 of the ICESCR), the right to participate in cultural life (Article 15 of the ICESCR), and the right to privacy in the

---

[6] Karel Vasak, "Three Generations of Human Rights," 1977.
[7] Negative rights are rights that restrains others from violating one's' rights
[8] UK Parliament, *Human Rights Act 1998*, https://www.legislation.gov.uk/ukpga/1998/42/contents.
[9] United Nations, "International Covenant on Civil and Political Rights, Adopted by the General Assembly of the United Nations on 16 December 1966," Reference C.N.467.1997.TREATIES-10 (Depositary Notification), https://treaties.un.org/doc/publication/cn/1997/cn.467.1997-eng.pdf.
[10] Ibid.

digital age (A/HRC/48/31) - focus on ensuring equal access to resources and addressing social inequalities.

1.1.3. The Third Generation of Human Rights: Collective or Solidarity Rights

The third generation of Human Rights,[11] also known as 'Solidarity Human Rights' or 'green rights' - emphasizing the interconnectedness of human societies and their relationship with the natural world, emerged in the 20th century to address collective interests and values that benefit all of society, often requiring international cooperation to address global challenges. These rights are a reconceptualization of the first two generations of Human Rights reflecting the rise of nationalism, the revolution of rising expectations, and the realization of the state's powerlessness in certain critical aspects. These rights are often inspirational rather than judicial, possessing an ambiguous character. Examples include the right to global digital cooperation (Roadmap for Digital Cooperation), the right to access to technology and knowledge sharing (Venice Statement),[12] and the right to peace (Declaration on the Right of Peoples to Peace).[13]

These three generations of Human Rights demonstrate the evolution of global values, responding to the challenges of humanity over time while emphasizing the correlation between individual freedoms, social justice, and responsibilities of the global society. The third generation is particularly relevant to Digital Human Rights because it addresses the collective challenges and opportunities of globalization and technological advancement. Just as the third generation seeks to secure rights for future generations by promoting sustainable development and global collaboration, the recognition of Digital Human Rights seeks to ensure everyone can benefit from the digital revolution without

[11] Ibid.

[12] UNESCO and International Bioethics Committee, *Venice Statement on the Right to Enjoy the Benefits of Scientific Progress and its Applications,* Venice: UNESCO, 2009.

[13] United Nations General Assembly, *Declaration on the Right of Peoples to Peace*, A/RES/39/11, November 12, 1984.

discrimination or exclusion. However, although its framework is widely discussed, its acceptance remains disproportionate. Critics argue that collective rights lack the enforceability of individual rights, making their practical implementation challenging. Nonetheless, proponents emphasize their importance in addressing global issues, such as climate change, access to technology, and digital inequality.

1.2. Background - North Korea's Global Commitments and Cyber Threats: From Treaties to Threats

1.2.1. North Korea's Treaty Commitments

North Korea has ratified five key UN Human Rights treaties, committing to uphold specific Human Rights standards. However, its actions often contradict these obligations, significantly impacting its citizens' quality of life. Below, a short, comprehensive list of the DPRK's breaches has been made to provide context for why these cyberattacks have taken place, which will be elaborated in the coming sections of the paper.

The International Covenant on Civil and Political Rights - 1966

The International Covenant on Civil and Political Rights (ICCPR) falls under the first generation of Human Rights. It was ratified by North Korea in 1981[14] and has a total of 53 articles, which require parties to protect a wide range of civil and political rights, including the Right to Privacy (Article 17) as well as the freedom of expression and access to information (Article 19). Moreover, the surveys conducted on North Korean defectors by PSCORE in 2022 revealed a lack of basic rights, particularly in areas such as privacy and freedom of expression.

According to the survey conducted on September 2, 2022, regarding the Right to Privacy (Article 17), respondents were asked, *"If*

[14] United Nations, "International Covenant on Civil and Political Rights, Adopted by the General Assembly of the United Nations on 16 December 1966," Reference C.N.467.1997.TREATIES-10 (Depositary Notification), https://treaties.un.org/doc/publication/cn/1997/cn.467.1997-eng.pdf.

internet access had been available in North Korea, do you think it would have made a difference in terms of the right to privacy within the country, and in what ways?"[15] A defector's response shed light on how the use of the internet would have allowed them to appreciate the right to privacy, stating;

> *"Through the internet, when people see discussions about privacy rights and personal freedoms, they start to see them as natural and essential. Instead of accepting privacy violations as normal, they become more aware of their rights and take steps to protect them."*
>
> - Kim Hyun-Seong[16]

> *"There was a high demand and curiosity for information. People were eager to access new information, but the restrictive environment and heavy monitoring made it difficult to obtain useful resources."*
>
> - Jeong Sung-Jae[17]

Additionally, with regards to freedom of expression and access to information (Article 19), defectors were asked; *"If internet access had been available in North Korea, do you think it would have made a difference in terms of the ability to voice opinions in North Korea, and in what ways?"*. The respondent observed that having access to the internet might have changed people's ability to express themselves and have access to information.

[15] Kim Hyun-Seong, interview by Nam Bada, Eunhye Kim, Omer, Clara, PSCORE, September 2, 2022.
[16] Ibid.
[17] Ibid.

"I think expressing opinions is somewhat different. The inability to express opinions is mainly due to control. When you're exposed to not just your own thoughts but also the perspectives of many others, you gain a broader understanding and new insights."

- Kim Hyun-Seong[18]

These responses reflect North Korea's suppression of Articles 17 and 19. Furthermore, the state sought to withdraw from the ICCPR in 1997[19], but the United Nations Human Rights Committee rejected the withdrawal, stating that countries cannot unilaterally withdraw from the covenant.

The International Covenant on Economic, Social, and Cultural Rights - 1966

The International Covenant on Economic, Social and Cultural Rights (ICESCR) falls under the second generation of Human Rights. North Korea ratified the treaty in 1981[20], which consists of 31 articles regarding rights related to the right to work under fair conditions (Articles 6 and 7), the right to an adequate standard of living, including food, clothing, and housing (Article 11) and the right to education and participation in cultural life (Articles 13 and 15).

In 2020, North Korea adopted the "Reactionary Ideology and Culture Rejection Act"[21] (반동사상문화배격법) banning its citizens from distributing or consuming any South Korean content, like K-pop and K-dramas. Violators may be liable for punishment including years of

[18] Ibid.
[19] United Nations, "International Covenant on Civil and Political Rights, Adopted by the General Assembly of the United Nations on 16 December 1966," Reference C.N.467.1997.TREATIES-10 (Depositary Notification), https://treaties.un.org/doc/publication/cn/1997/cn.467.1997-eng.pdf.
[20] Ibid.
[21] *Daily NK*, "Anti-Reactionary Thought Law: Bans on External Culture in North Korea (English Translation)," *Daily NK*, March 2023.

hard labor. The state also tightly censors and monitors online information, preventing people from having access to music, movies, and books.

In 2022, a survey asked defectors about how they thought internet access in North Korea could improve their quality of life. "*Do you think having internet access in North Korea would improve the quality of life for its people? What other consequences do you think it would have for North Korea?"*[22] A respondent expressed their confidence in its impact, stating;

> *"I am 100% confident that there will be significant improvement. If North Koreans were able to access the external internet, they would become aware of democracy, economic development, and how people live in the outside world. They would also learn about fundamental human rights."*
>
> - Kim Hyun-Seong[23]

North Korea's Central Information Technology Guidance Organization and other relevant bodies also block the inflow of reactionary ideology and culture through electric waves by strengthening supervision and control on frequency settings for entertainment equipment such as radio and television. There are also systematic monitoring and public reporting systems against materials considered hostile.[24]

1.2.2. United Nations Convention against Cybercrime - 2024

As mentioned, legal protection against cybercrime is an emerging and developing concept in the rapidly growing digital world. In

[22] Kim Hyun-Seong, interview by Nam Bada, Eunhye Kim, Omer, Clara, PSCORE, September 2, 2022.
[23] Ibid.
[24] *Daily NK*, "Anti-Reactionary Thought Law: Bans on External Culture in North Korea (English Translation)," *Daily NK*, March 2023.

December of 2024, the General Assembly of the United Nations adopted the United Nations Convention against Cybercrime, the first global treaty to help protect states from cyber threats. In its statement of purpose, the convention calls to strengthen measures to prevent cybercrime through international cooperation and to "promote, facilitate and support technical assistance and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countries[25]". Additionally, the treaty aims to connect these efforts to fundamental Human Rights, including freedom of expression, conscience, opinion, religion or belief, peaceful assembly and association. As the treaty is meant to help protect states from cyber threats, it requires the criminalization of "illegal hacking" that targets electronic data and IT systems, thus violating the "respect of the sovereign equality and territorial integrity" of states. [26]

[25] United Nations General Assembly. *United Nations Convention against Cybercrime*. A/RES/79/243. December 24, 2024.
[26] Ibid.

2. Examining North Korea's Cyber Capabilities and Practices

The second section analyses North Korea's strategic approaches and technical capacities regarding cybercrime. The methods used, such as phishing emails, information espionage, cyber terrorism, and financial warfare, are also illustrated in detail. The analysis provides insights into the organizational structure of North Korea's cyber units, including the Reconnaissance General Bureau, a North Korean Intelligence agency, and highlights hacking groups such as the Lazarus Group and Kimsuky. Additionally, particular attention is paid to the diverse range of actors targeted in these attacks, from governmental agencies to private entities, including Human Rights groups and individuals. North Korea’s cyber capabilities have become a critical area of focus in understanding the intersection of cybersecurity and Human Rights violations. Employing a variety of methods, North Korean cyber operations exploit vulnerabilities to achieve their objectives, often leaving profound repercussions, which will be explored in the subsequent section.

2.1. Definition of Terms

The following section provides definitions and clarifications for key terms essential to understanding this report's context.

2.1.1. Cybersecurity

As cybersecurity has become a crucial issue, there have been many attempts to define the term. Cybersecurity can be understood as "the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, and technologies that can be used to protect the cyber environment and organization and user's asset".[27] A US Congressional research report further defines the term as a broad and arguably somewhat vague concept with no actual agreed-upon definition in the global context.[28] The report states that cybersecurity usually refers to one or more of the following three aspects: (1) a set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and device's software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, (2) the state or quality of being protected from such threats, or (3) the broad field of endeavor aimed at implementing and improving those activities and quality.[29] However, the term does not have a globally agreed-upon definition. A consensual definition would enable the international community to work together more effectively to provide a legal framework.

[27] International Telecommunication Union, "Recommendation X.1205", 2008.
[28] Ibid.
[29] Eric A. Fischer, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, Congressional Research Service Report RL32777, February 22, 2005, https://sgp.fas.org/crs/natsec/RL32777.pdf.

2.1.2. Cyber Threat and Cyber Attack

Currently, there is no standard amongst the security community on how to clearly define and differentiate between the terms "cyberattack" and "cyber threat", causing these terms to be used interchangeably. For purposes of clarity, we define them as follows:

A cyber threat is "an indication that a hacker or malicious actor is attempting to gain unauthorized access to a network to launch a cyberattack"[30] through malware - short for "malicious software".

As for cyberattacks, unlike traditional hostilities, they can also take place during times of peace and may be considered a modern form of warfare. States might employ digital tools and recruit hacker groups to conduct cyberattacks against other states[31], but also against international organizations and institutions, individuals, and groups of individuals or companies, making them vulnerable and putting their safety at risk. These attacks can be considered as "an exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks, and stealing both data and money."[32] They also include activities such as website defacement, theft of intellectual property, denial of service attacks, and destructive malware. Representing a major threat to the security of targeted states, but also institutions, individuals, or groups of individuals, they require urgent countermeasures. Governments, international organizations, civil society, companies, and cybersecurity experts must work together to address this challenge.[33]

---

[30] IBM, "Types of cyberthreat", March 2024. https://www.ibm.com/think/topics/cyberthreats-types

[31] Khatuna Burkadze. "International Legal Definition of a Cyberattack". *Journal Iustitia*, 2022.

[32] Padmavathi G. and Uma M. "A Survey on Various Cyberattacks and Their Classification". *International Journal of Network Security*, *15*(5), 390-396 (2013).

[33] Niculae Iancu, Andrei Fortuna, Cristian Barna, and Teodor Mihaela, *Countering Hybrid Threats: Lessons Learned from Ukraine* (Amsterdam: IOS Press, 2016).

2.1.3. IT Personnel

IT professionals are highly qualified experts responsible for developing and managing an organization's information technology infrastructure. Their main tasks include system administration, network management, cyber security, and technical support to ensure secure and efficient IT operations. In the case of North Korea, IT personnel are often state-sponsored specialists who are specifically selected and intensively trained to conduct both defensive and offensive cyber operations.[34] Within this structure, there are a variety of different roles. However, this analysis focuses exclusively on two key roles: North Korean Hackers and Programmers. Other aspects fall outside the focus of this report.

- **Hackers** are individuals, also known as 'threat actors', who engage in malicious activities by breaking into computers and computer networks to cause harm.[35] Due to internet restrictions, hackers usually come from abroad, from countries like China.[36] Various hacking groups in North Korea engage in espionage, financial warfare, and sabotage.

- **Programmers** are individuals who develop programs for data to be processed by a computer[37]. They often play a dual role in either developing spyware and trojan viruses to conduct cyber espionage, sabotage, or internal tools for cyber defense to protect North Korea's digital infrastructure. In the case of North Korea's role in cyber threats, programmers, however, earn money not by stealing or extortion, but simply by making websites or programmes for foreign companies. In Germany, for example, North Korean representatives take on contract work for

[34] *Joint Cybersecurity Advisory*, "North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media," 2023.
[35] Tyson Brooks, "The Professionalization of the Hacker Industry," *International Journal of Computer Science & Information Technology (IJCSIT)* 14, no. 3 (2022): 87–95, https://doi.org/10.5121/ijcsit.2022.14307.
[36] Jason Bartlett, Rep., *Exposing the Financial Footprints of North Korea's Hackers* (Center for a New American Security, 2020).
[37] *Collins English Dictionary*, s.v. "PROGRAMMER," accessed 2025, https://www.collinsdictionary.com/dictionary/english/programmer.

businesses and send it to North Korea, where the programmers are located.[38]

2.2. Analyzing North Korea's Cyber Strategies and Operational Capabilities

2.2.1. North Korean Cyberattack Strategies

Cyberattacks are typically categorized into three types: information espionage, cyber terrorism, and financial warfare, based on their objectives. The latter is the most relevant and important for our research. This categorization of the operations is based on the objectives observed. It was first proposed by Kong Ji-Young, Lim Jong In, and Kim Kyoung Gon, in their paper "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," presented in 2018 at CyCon in Tallinn. They divided the objectives into three main categories: Information Espionage, Cyber Terrorism, and Financial warfare.[39]

[38] Yoo-Hyang Kim, "North Korea's Cyberpath," *Asian Perspective* 28, no. 3 (2004): 191–209, https://doi.org/10.1353/apr.2004.0018, 205.

[39] Ji-Young Kong, Lim Jong In, and Kim Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies", *11th International Conference on Cyber Conflict (CyCon)*, vol. 900, Tallinn, Estonia, 2019, 1–20, https://doi.org/10.23919/CYCON.2019.8756954.

TABLE 1. CATEGORIES OF OPERATIONS BASED ON OBJECTIVES[40]

Objectives	Cyber Operations	Period	Remarks
Information Espionage	Campaign Kimsuky	2009-2018	Variants and affiliations have been found up until 2018
	Operation KHNP	Dec 15, 2024	Causing social chaos in South Korea
Cyber Terrorism	Operation DarkSeoul	March 20, 2013	The attackers shared TTPs with malicious activities from 2007
	Operation BlockBuster	Nov 24, 2024	The Interview movie that plotted the assassination of Kim Jong-un kindled the attack The FBI attributed this attack to North Korea
Financial Warfare	Bangladesh Central Bank Heist	Feb.04-05, 2014	Stealing bank credentials and sending fraudulent transactions to SWIFT
	WannaCry	May 2017	Demanding ransoms for files taken hostages The FBI attributed this

Espionage in this context is the acquisition of sensitive information through cybersecurity breaches. It has become part of the broader trend of espionage. Indeed, before its cyber espionage, North Korea had already been caught in several espionage missions.[41] Phishing emails and malware sent through links can also be considered espionage if their purpose is to steal information.[42]

[40] Ji-Young Kong, Lim Jong In, and Kim Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies", *11th International Conference on Cyber Conflict (CyCon)*, vol. 900, Tallinn, Estonia, 2019, 1–20, https://doi.org/10.23919/CYCON.2019.8756954.

[41] Dick K. Nanto, *North Korea: Chronology of Provocations, 1950-2003*, Washington, DC: Congressional Research Service, 2003.

[42] According to Checkpoint, a phishing attack is a form of social engineering attack in which the attacker sends a malicious message to the intended recipient. Often, this includes clicking on a malicious link or opening an infected attachment.

NATO defines cyber terrorism as "A cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."[43] Often, these attacks are combined with espionage, but there are also cases where the goal was purely to disrupt major events. This was first showcased in 2009, when North Korean threat actors targeted the websites of various South Korean and U.S. government entities, rendering them inaccessible.[44]

Financial warfare attacks have the goal of monetary gain. North Korea first conducted financial attacks in 2016 when it targeted the National Bank of Bangladesh and appropriated 81 million dollars. Since then, financial attacks have become the biggest focus of North Korea's cyber activity.[45] Multiple banks across several continents[46] have been targeted with different techniques utilized by the perpetrators, such as malware deployments (remote access trojans[47] (RATs), banking trojans, and ransomware[48]). At the same time, cryptocurrency companies have also been targeted in order to acquire money. Stolen value from cryptocurrency has, in fact, made up a large percentage of funds acquired by North Korea in 2023, with news outlets reporting the earnings from

---

https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/spear-phishing-vs-phishing/

[43] Center of Excellence Defence Against Terror, *Responses to Cyber Terrorism (NATO Science for Peace and Security)*, Texas: IOS Press, 2008.

[44] Chong-Woo Kim, "The Evolution of North Korean Cyber Threats," *The Asian Institute for Policy Studies*, 2019.

[45] Elisabeth Suh, Rep., *North Korea's Cyber Capabilities and Strategy*, Report, Berlin: German Council on Foreign Relations, 2022. https://dgap.org/en/research/publications/north-koreas-cyber-capabilities-and-strategy-0

[46] 'Office of Public Affairs | Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe | United States Department of Justice', 17 February 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[47] According to Checkpoint, a "Trojan horse malware is malware designed to look like a legitimate and desirable program while concealing malicious functionality. Once the seemingly legitimate program is executed, the malicious functionality is run as well." https://www.checkpoint.com/cyber-hub/cyber-security/what-is-trojan/.

[48] According to Checkpoint, "ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files." https://www.checkpoint.com/cyber-hub/cyber-security/what-is-trojan/.

stolen cryptocurrency estimated to be around 600 million dollars[49]. There are many tactics that the General Bureau has made use of to financially violate the individual rights of people for its own gain. It is important to take this into consideration when looking at the level of threat North Korean cyber-attacks pose to societies across the world.[50]

North Korea continues to employ cyber-enabled financial crimes to bypass sanctions and fund state operations. A recent U.S. case revealed an Arizona woman's guilty plea in a scheme that generated $17 million by illegally placing North Korean IT workers in U.S. companies under false identities.[51] This feat was primarily achieved by creating a 'laptop farm', where she, at home, would use the computers received, thus making it look like the IT workers she co-conspired with were workers from within the US. This aligns with findings from the TRM Labs 2025 Crypto Crime Report, which highlights North Korea as the largest state sponsor of cryptocurrency theft, responsible for over $600 million in stolen crypto in 2024 alone. These illicit activities provide a critical financial lifeline for the regime, providing insight into the motivation behind these attacks.[52]

Additionally, North Korea conducts sophisticated cyber operations against South Korean institutions, with documented attacks targeting government agencies, the judiciary, and defense contractors. Its cyber warfare units have successfully breached the Supreme Court's systems, extracted sensitive military intelligence, and compromised classified data related to defense technologies.

---

[49] Sheila Chiang, 'North Korea Crypto Hacking Activity Soars to Record High in 2023, New Report Shows', CNBC, 24 January 2024, https://www.cnbc.com/2024/01/24/north-korea-crypto-hacking-activity-soars-to-record-high-in-2023-new-report-shows.html.

[50] Jeeseon Hwang and Kyung-Shick Choi, 'North Korean Cyber Attacks and Policy Responses: An Interdisciplinary Theoretical Framework', *International Journal of Cybersecurity Intelligence & Cybercrime* 4, no. 2 (2021): 4–24, https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1103&context=ijcic.

[51] U.S. Department of Justice, 'Arizona Woman Pleads Guilty to Fraud Scheme That Illegally Generated $17 Million in Revenue for North Korea,' United States Attorney's Office, District of Columbia, February 7, 2024, https://www.justice.gov/usao-dc/pr/arizona-woman-pleads-guilty-fraud-scheme-illegally-generated-17-million-revenue-north.,

[52] TRM Labs, TRM 2025 Crypto Crime Report, 2025, http://www.trmlabs.com/files/report-2025-crypto-crime-report.

2.2.2. North Korea's Cyber Crime Capabilities: The Reconnaissance General Bureau's Structures and Functions

North Korea has a complicated network of cyber organizations composed of various different agencies. However, it is assumed that most of North Korea's foreign cyber activity is conducted by the Reconnaissance General Bureau (RGB), which oversees six departments. The first department handles the training of agents and provides technical assistance for infiltrations. The second department gathers intelligence about hostile forces. The third department manages signal intelligence and is among the most crucial in administering North Korea's cyber threats. The fifth department mainly deals with inter-Korean relation affairs (four is skipped based on the Korean superstition that it is a number of bad luck because, when pronounced, the number sounds like the Korean word for 'death' /sa/). The sixth department is similar to the second department, as it oversees military contracts and policy. The seventh and last department handles military logistics.[53][54]

The third and fifth departments in North Korea's cyber activities are the most active. It is believed, for example, that the hacking organization Lab 110 operates under the administration of the third department. Other North Korean cybercrime organizations that are not regulated but supported by the government include TEMP.Hermit, which collects strategic intelligence (espionage and phishing), APT38, which is intended to commit financial cyber crimes and has been credited for stealing millions of dollars at a time across multiple countries (financial attacks), Andariel, which primarily focuses its operation on sabotaging governments and military personnel but also engages in financial attacks on the side, and Bureau 325, which was created during the coronavirus

[53] Lankov, Andrei, "On the Great Leader's Secret Service: North Korea's Intelligence Agencies: NK News," NK News - North Korea News, May 1, 2017, accessed January 15, 2025. https://www.nknews.org/2017/05/on-the-great-leaders-secret-service-north-koreas-intelligence-agencies/.

[54] Barnhart, Michael, Michelle Cantos, Jeffery Johnson, Elias Fox, Gary Freas, and Dan Scott.,"Not so Lazarus: Mapping North Korea Cyber Threat Groups to Government Organizations," Google Blog, March 23, 2022. https://cloud.google.com/blog/topics/threat-intelligence/mapping-North Korea-groups-to-government/?hl=en.

epidemic to gather intelligence regarding the coronavirus, and operates under administration of the third department of the RGB.[55]

The Fifth Bureau focuses on inter-Korean relations and oversees the threat group Kimsuky, which primarily engages in espionage, frequently targeting organizations in the U.S. and South Korea. The bureau is also likely linked to the United Front Department, which is responsible for producing cyber propaganda aimed at foreign audiences.[56]

However, on the 9th plenary Session of the 8th Central Committee of the Workers' Party of Korea in December 2023, there was a shift in the organization of the North Korean bureau system. Yet, as we do not have enough insights about the current organisation, there might be some changes in the content above.

2.3. Analyzing North Korea's Cyber Practices: Identifying Key Targets

As mentioned previously, North Korea's cyber operations fall into three main categories: Information espionage, financial warfare, and cyber terrorism. These activities target a range of victims, including governmental agencies, international organizations, critical infrastructure, and private entities, with South Korea and the United States being the most frequently targeted nations.

2.3.1. Financial and Private Organizations

Financial attacks are another significant component of North Korea's cyber activities, used to circumvent international sanctions and secure funds for the regime. One method involves the AppleJeus malware, developed by the Lazarus Group, which creates fake cryptocurrency trading platforms to steal sensitive information. This malware has been used to steal cryptocurrency in over 30 countries, generating a substantial revenue stream for North Korea. Similarly, the

[55] Ibid.
[56] Ibid.

Dark Seoul cyberattack in 2013 disrupted tens of thousands of South Korean computers, including those tied to ATMs, payment terminals, and mobile banking services, causing significant financial damage.[57] Another major example of financially motivated cybercrime is the 2016 Central Bank of Bangladesh heist, where North Korean hackers used spear-phishing techniques to infiltrate the bank's network and steal $81 million from its account at the Federal Reserve Bank of New York.[58]

Additionally, the health care sector has also been a victim. For example, North Korea launched ransomware campaigns (Maui) against Healthcare and Public Health Sector organizations and critical infrastructure sector entities in May 2021.[59] These attacks, attributed to North Korea state-sponsored cyber actors, aimed to encrypt servers responsible for healthcare services, such as electronic health records. As a result, hospitals that were hacked were forced to halt planned consultations, with potentially detrimental effects on patient care.[6061] Additionally, during the COVID-19 pandemic, North Korean hackers targeted hospitals and vaccine manufacturers, including Pfizer and AstraZeneca, to steal proprietary data.[62]

Companies in the blockchain and cryptocurrency industry, as well as individual investors holding significant amounts of cryptocurrency or high-value non-fungible tokens (NFTs), have become prime targets of the North Korean regime. These victims are often lured into downloading

---

[57] Martin David, "Tracing the Lineage of Dark Seoul," *Sans Institute*, 2021. https://www.giac.org/paper/gsec/31524/tracing-lineage-darkseoul/126346.

[58] Balu Ramkumar, Rep., *Bangladesh Bank Cyber Heist: Incident Analysis*, Report, Georgia Institute of Technology, 2022. 1–4.

[59] 'North Korea Cyber Threat Overview and Advisories | CISA', accessed 23 September 2024, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea.

[60] Associated Press, 'North Korean Charged in Cyberattacks on US Hospitals, NASA and Military Bases', SecurityWeek, 25 July 2024, https://www.securityweek.com/north-korean-charged-in-ransomware-attacks-on-american-hospitals/.

[61] Kim, Min-hyung. 2022. "North Korea's Cyber Capabilities and Their Implications for International Security" *Sustainability* 14, no. 3: 1744. https://doi.org/10.3390/su14031744.

[62] Elisabeth Suh, Rep., North Korea's Cyber Capabilities and Strategy (German Council on Foreign Relations, 2022).

malicious cryptocurrency applications designed for Windows and macOS, which serve as entry points for cyberattacks. [63]

In addition to espionage and financial attacks, North Korea uses cyber operations for cyber-terrorism or system destruction. A key example is the 2014 Sony Pictures Entertainment hack, which was carried out in response to the release of *The Interview*, a satirical film mocking Kim Jong-un.[64] North Korean hackers encrypted and deleted files, leaked confidential company data, and attempted to coerce Sony into canceling the movie's release. Ironically, the attack drew more attention to the film, amplifying its publicity despite its poor reviews.[65]

2.3.2. Public Institutions and Organizations

South Korea and the US are amongst the primary targets of cyber attacks by North Korean hacking groups, although other countries have also fallen victim to cyber attacks initiated by North Korea[66]. Those activities include hacking into the network at South Korean universities to steal personal information from 'South Korean Elites' by creating phishing servers.[67] Alongside this, they also utilize opinions from experts in Japan, the U.S, Europe, etc., in different relevant fields (such as diplomacy) about North Korea to plan its own responses and political line[68].

Information espionage attacks often focus on critical infrastructure to steal sensitive information. A prominent example is the

---

[63] 'TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies | CISA', 20 April 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a.

[64] "The Interview," IMDb, December 24, 2014, https://www.imdb.com/title/tt2788710/.

[65] Stephan Haggard and Jon R. Lindsay, Rep., "North Korea and the Sony Hack: Exporting Instability Through Cyberspace," (East-West Center, 2015), 2.

[66] '국립외교원', accessed 10 October 2024, https://www.ifans.go.kr/knda/hmpg/mob/pblct/PblctView.do;jsessionid=hX6792qsCLHa5ilXKJd4mbB-.public22?pblctDtaSn=14095&clCode=P07&menuCl=P07&pageIndex=1#.

[67] 'Inside Pyongyang's Mind: An Overview of the Kim Regime's Persistence in Masterminding Illicit Cyber Activities and ROK's Responses', accessed 24 September 2024, http://www.ifans.go.kr/knda/ifans/eng/pblct/PblctView.do?pblctDtaSn=14227&clCode=P19&koreanEngSe=ENG.

[68] Ibid.

hack of Korea Hydro and Nuclear Power Co. (KHNP), South Korea's sole nuclear power plant operator. North Korean hackers obtained worker data, reactor blueprints, and training manuals, attempting to extort KHNP into halting its nuclear operations. A related incident occurred in November 2019 when North Korean hackers attacked the Kudankulam Nuclear Power Plant in India, raising concerns that stolen information could be used to advance North Korea's nuclear program.[69] [70] Similarly, in May 2021, North Korea targeted the Korea Atomic Energy Research Institute (KAERI), potentially compromising energy research vital to South Korea's energy security.[71] Furthermore, the APT43 hacker group, linked to North Korea, has conducted targeted attacks on South Korean and U.S. government organizations.[72]

Human Rights Organizations and Research Institutes

While advocacy for North Korean human rights is primarily driven by Non-Governmental Organizations (NGOs) and Civil Society Organizations (CSOs), it is important to distinguish these from government-established human rights institutions. This analysis will focus specifically on civil society organizations dedicated to North Korean human rights advocacy, examining their unique role and contributions to the field. Various organizations in South Korea and overseas have been working to shed light on the Human Rights violations occurring in North Korea. From conducting research on these violations to advocacy, these organizations work to protect North Korean defectors in a multitude of ways. Increasingly, these organizations have become victims of cyberattacks, which have repeatedly been traced back to the North Korean government. Consequently, undisclosed, private

[69] Ibid.
[70] Gary Cohen, "Throwback Attack: Korea Hydro and Nuclear Power Highlights the Vulnerability of Critical Systems," *Industrial Cybersecurity Pulse*, March 16, 2023.
[71] Elisabeth Suh, Rep., North Korea's Cyber Capabilities and Strategy (German Council on Foreign Relations, 2022).
[72] Cybersecurity and Infrastructure Security Agency, "#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund North Korea Malicious Cyber Activities," 2023. https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_North Korea_ACTIVITIES.PDF.

information of the organizations is stolen in addition to personal information of members. Due to hacking incidents in NGO coalition group chats and cases of email impersonation, these organizations have had to implement preventive measures to protect against cyber threats

Social engineering is also used against employees of research centres, think tanks, academic institutions, and news media organizations to illicitly access private documents, research, and communications of their targets. Spear Phishing campaigns are led[73] against journalists, academics, or other individuals linked to North Korea policy circles.[74]

2.3.3. Individuals at Risk: North Korean Defectors and Human Rights Activists

The cyber threat from North Korea has been analyzed at a macro level, focusing on institutions and organizations. Yet, there is also a need to address the persistent cyberattacks faced by North Korean defectors and their families on a micro level. Even outside of institutional affiliations, they remain at constant risk from the North Korean regime. Whether residing in South Korea or abroad, these individuals are vulnerable to targeted attacks by North Korean authorities. According to a study from 2018, around 997 North Korean Defectors in South Korea were victims of a large-scale cyber-attack. Their names, addresses, and dates of birth were leaked, and the risk of these types of attacks may potentially endanger the defectors' families who remain in North Korea.[75]

A key concern when examining cybercrime by North Korean actors is the extension of the threat not only to individuals but also to their social networks, including family members and friends. While the persecution of activists through cyberattacks alone has serious

[73] Spear phishing is described as the use of false email and digital communications. https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf

[74] National Security Agency (US), 'North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media', n.d., https://media.defense.gov/2023/Jun/01/2003234055/-1/-1/0/JOINT_CSA_DPRK_SOCIAL_ENGINEERING.PDF.

[75] 'North Korea Defector Hack: Personal Data of Almost 1,000 Leaked', 28 December 2018, https://www.bbc.com/news/world-asia-46698646.

consequences, the explosive nature of such attacks is evident in the potential compromise of personal information. This escalation underscores a shift from individual to collective vulnerability, highlighting the systematic nature of the threat.

At the micro level, the extent of the stress is apparent, as the statements of those affected illustrate. Through our research, we interviewed Mr. Kang Shin-Sam, the head of the Unification Academy, which focuses on educating young South Koreans about North Korean issues and the future of unification. Therefore, he is often targeted by North Korean cyberattacks. Kang Shin-Sam describes how he has removed all personal information from his computer and written it down on a piece of paper to minimise the risk of a data leak. However, he expresses great concern that not only his own data but also information exchanged between him, his family, and his friends could have been passed on to North Korea. This uncertainty has paralysed him for weeks and underlines the far-reaching psychological stress that such attacks can cause.

> *"All my personal information is on my computer. I took out all my passwords and other information and wrote them down on a piece of paper, which is quite inconvenient. I'm very worried because I'm not the only one in the photos, and that the information that was exchanged between family, and friends may have been passed on to North Korea. I've been paralyzed for about a month. People around me are threatened."*
>
> - Kang Shin-Sam[76]

A DailyNK reporter describes a similar form of stress. Daily NK is a South Korea-based news outlet that provides independent reporting on North Korea, often using sources inside the country. He reports a constant feeling of anxiety and pressure that permeates his daily life. He describes a loss of freedom of expression and severe limitations on his

[76] Kang Shin-Sam, Interview by Nam Bada, Elma Duval, Yunah Jang. PSCORE, 24th October 2024.

ability to voice his opinions. Threats impact not only his personal liberty but also social interactions within his environment, significantly undermining the fundamental right to peace and free expression. [77]

> *"In daily life, there's also a sense of anxiety. So sometimes when I do things like this, my wife says, "Why are you doing that?" and she gets worried. She doesn't know how those people might react, and she thinks it might not be good if too much personal information gets exposed or if we react too much."*
>
> - A DailyNK Reporter[78]

2.4. North Korea's Hacking Methods

As elaborated previously in this report, the cases of North Korean cyber-attacks, though not entirely new, are part of a program initiated by the DPRK in 2009 that aims to impact and potentially undermine countries such as the US and South Korea. This is, among other things, due to their political and historical ties. Specifically, it began with Operation Flame, the first Distributed Denial-of-Service (DDoS) cyberattack (an attack that overwhelms a server or network with excessive traffic, causing it to slow down or crash) initiated on behalf of the North Korean state. Since this part of the report will focus on the human rights violations caused by North Korean cyber-attacks, the following subsections will consider multiple perspectives, ranging from those of international organizations, individuals, and even the IT workers. By doing this, we will be able to establish a more holistic picture of how these cyber-attacks have impacted various sectors of society and how they are perceived.[79]

---

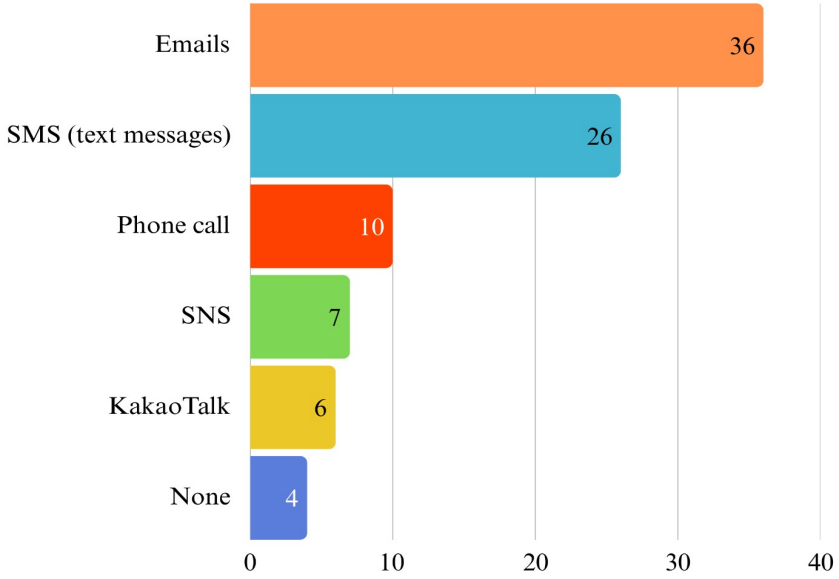
[77] Daily NK Reporter, Interview by Nam Bada, Duval Elma, Yunah Jang PSCORE, 23rd October 2024.

[78] Daily NK Reporter, Interview by Nam Bada, Duval Elma, Yunah Jang PSCORE, 23rd October 2024.

[79] Kim Chong Woo and Carolina Polito, "The Evolution of North Korean Cyber Threats," *The Asan Institute for Policy Studies*, August 2019, https://www.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/.

Cyberattacks undermine all three generations of Human Rights by endangering personal security, eroding freedoms, and disrupting essential infrastructures and services. First-generation rights (civil and political liberties) are threatened when attacks target critical systems like hospitals or power grids, jeopardizing individual safety and restricting freedom of expression. These breaches create a chilling effect on open communication and impede the rule of law. The undermining of second-generation rights (economic, social, and cultural) exacerbates economic vulnerabilities, widens social inequalities, and blocks access to scientific progress. Meanwhile, third-generation rights (collective and solidarity) are compromised when large-scale intrusions destabilize entire regions, weaken international cooperation, and infringe on privacy—ultimately undermining global peace and shared development.

FIG.1: PROPORTIONS OF COMMUNICATION METHODS USED FOR HACKINGS



Over the past few years, North Korea has become increasingly creative in its hacking methods, yet phishing emails remain the most common hacking occurrence. Still, as social media developed, hacking now also occurs on personal social media accounts, such as YouTube, Facebook, X, etc. According to a survey conducted by PSCORE in

December 2024 of 198 North Korean defectors, emails were found to be the most common hacking method, with 40% of the respondents having experienced email hacking. Yet, it is worth noting that more than half of the attacks North Korean defectors were victims of, occurred through different methods, namely emails (36 times), text messages (26 times), phone calls (10 times), social media (7 times), or Kakao talk (messengers, 6 times), as shown in Figure. 1.

2.4.1. Detailed Description of Hacking Techniques

Phishing and Email Tactics

FIG. 2: TYPE OF EMAIL ADDRESSES USED FOR THE HACKING

Even though North Korea has diversified its hacking methods over the past few years, phishing emails remain the most common. According to the same survey, 54.5% of the victims received emails coming from personal email addresses, meaning that hacking victims usually exchange emails with individuals who are seemingly identified as 'real people.' Moreover, 5% of the respondents received hacking emails from companies, and 16% received them from organisations working to

advocate for Human Rights in North Korea, or in similar fields, as shown in Figure. 2.

According to interviews held by PSCORE in October 2024, it has been observed that hacking attempts have become increasingly frequent. Notably, Mr Kang Shin-Sam from the Unification Academy (통일아카데미) states:

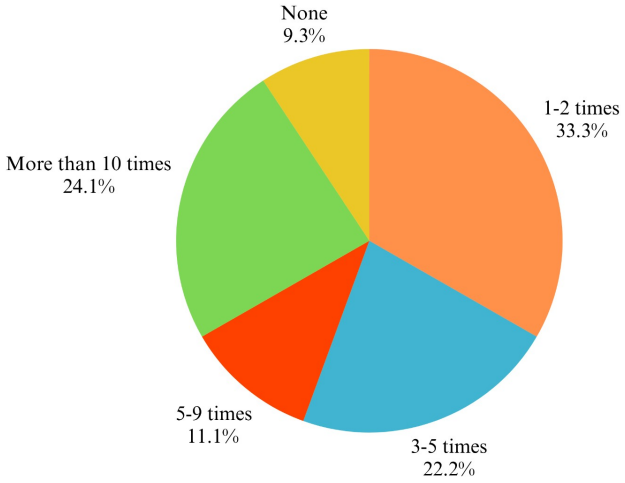
"It has increased sharply recently, what I mean is that, if you count both addresses, I receive 5-6 emails every week."

- Kang Shin-Sam[80]

Because of the constant phishing emails, strong protection and diligence measures are taken to ensure that emails are not sent by fraudulent people. Before opening any link, file, or document received via email, he always verifies with the sender by phone to confirm its legitimacy, ensuring he can safely review the email's content. Such constraining procedures, even if burdensome, are necessary in order to limit the risks and repercussions of hacking. Indeed, checking the email address is not enough since, according to Mr Kang Shin-Sam, sometimes the email address that sent the hacking files was identical to a real one, making it impossible to identify malware.

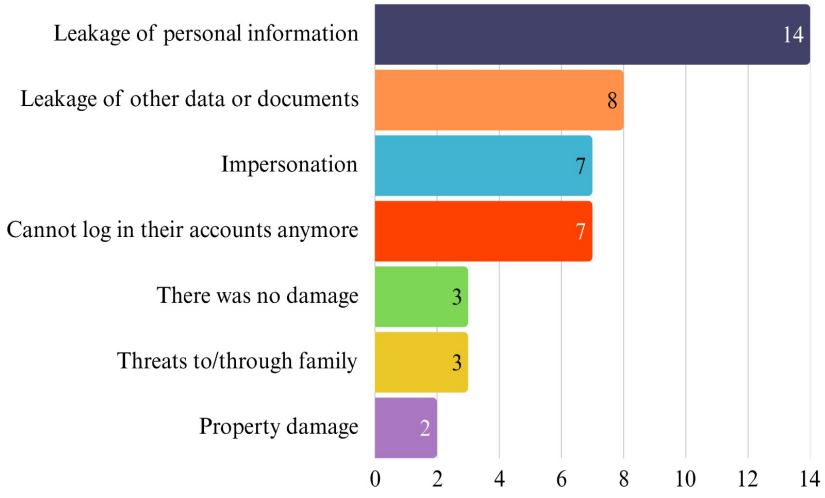
[80] Kang Shin-Sam, interview by Nam Bada, Elma Duval, and Yunah Jang, PSCORE, October 24, 2024.

FIG. 3: FREQUENCY OF HACKING EMAILS RECEIVED



Moreover, a major challenge for victims is that once they experience a cyberattack, they are more likely to be targeted again. This is supported by our study's findings, where more than 55% of respondents fell victim to these cyber attacks multiple times (Figure 3). This leads to restlessness and persistent anxiety for victims, who must constantly remain vigilant in their online activities.

FIG. 4 : ASSESSMENT OF DAMAGES LINKED TO HACKING INCIDENTS

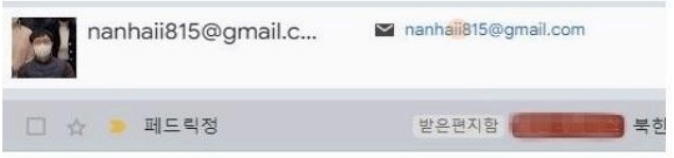


According to our survey, cyberattacks have various consequences, such as identity theft, leakage of personal information or documents, and accounts being deleted, as shown in Figure. 4.

Documented Hacking Cases

IMAGE 1: ORIGINAL EMAIL ADDRESS

IMAGE 2: ADDRESS USED BY THE HACKER



These images depict two email addresses, the first one being an official one used by Kang Shin-Sam from the Reunification Academy (통일아카데미), and the second one being a copy of the email created by a North Korean threat actor. In Image 1, the email address is nahai815@gmail.com, while in Image 2, it is nahaii815@gmail.com with an additional ‘i’. Moreover, the official address does not have a profile picture, while the second usurps the identity of Kang Shin-Sam by adding one. The email sent by the second email address contained a ‘registration link’ that was a hacking attempt.

Another example of an email hacking incident is the one where Mrs. Heo Jeong-Yoon was a victim of cyberattack. As the president of an NGO, she faces a lot of pressure, intimidation, and hacking attempts, the latest incident taking place in November 2024. The attack began with an email that appeared to be from an official address, presenting itself as a request for research materials, interviews, or appearance approvals. The

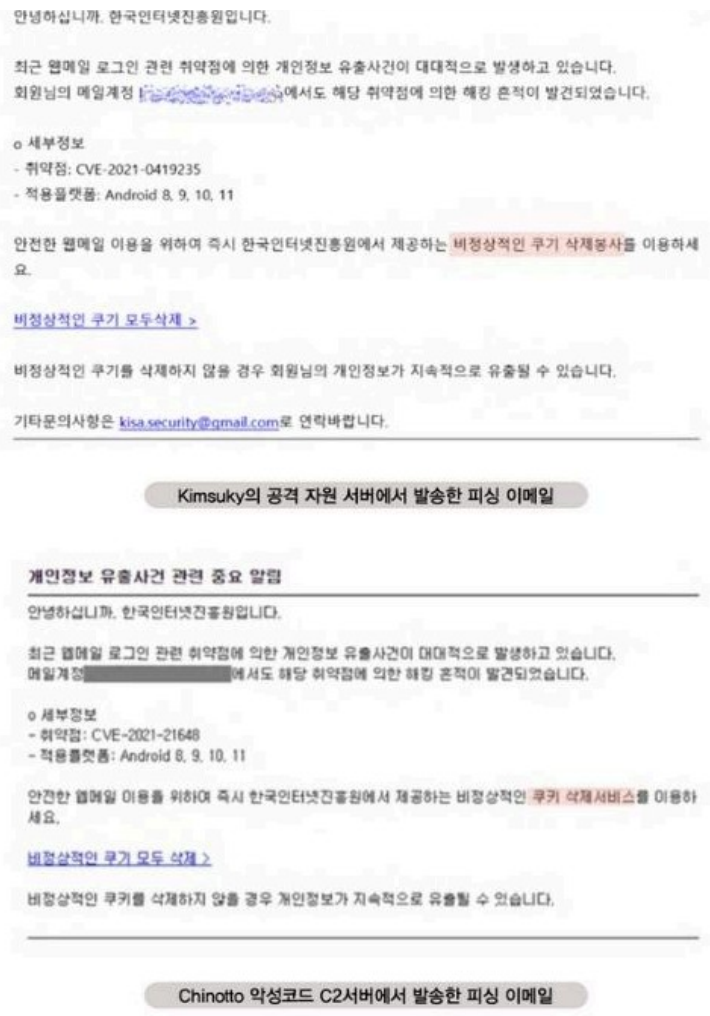
hacker impersonated a TV producer and used convincing details, including follow-up correspondence through a personal email, to gain her trust. They included a malicious link disguised as a questionnaire on a familiar topic, which opened a legitimate-looking page to avoid suspicion. As she usually receives many TV interview requests, and as the process seemed ordinary, she believed it to be a standard request. Trusting its legitimacy, she clicked the link and unknowingly compromised her security. Suspicion arose when the interaction deviated from standard practices, prompting her to verify the sender's identity, which led to the discovery that the 'production designer' was fake. This incident mirrors similar hacking attempts she experienced in June and November 2024, indicating a recurring threat. As a regular target of such attempts, Mrs. Heo Jeong-Yoon is very cautious about her communication and about the people she opens links or emails from, yet in this case, the hacker's very convincing identity appropriation was a flawless coverture she was unable to identify as malicious.[81]

Some ways to identify North Korean hacking codes or hacking attempts are through the use of cyber forensic linguistics and sociolinguistics. Indeed, through the examination of the language patterns in phishing emails, malware messages, or code scripts, it is possible for experts to identify, or at least narrow down the possible origin of the hacker.[82] According to the South Korean cybersecurity platform Genians, the use of specific terms helps to highlight the origin of the hacking.

In the email shown in Image 3, the term '비상적인 쿠키 삭제 봉사' /bi-sang-jeog-in ku-ki sag-je bong-sa/ is used instead of the more natural Korean phrase '쿠키 삭제 서비스' /ku-ki sag-je seo-bi-seu/, making it sound unnatural to native (South) Korean speakers.[83]

[81] Heo Jeong-Yoon, interview by Nam Bada, PSCORE, December 15, 2024.
[82] Ria C. Perkins, 'The Application of Forensic Linguistics in Cybercrime Investigations,' Policing: A Journal of Policy and Practice 15, No. 1 (2021): 68–78.
[83] Dongwook Kim, Seulgi Lee, Taewoo Lee, and JaeKwang Lee, TTPs#9: 개인의 일상을 감시하는 공격전략 분석, 2021, 32.

IMAGE 3: KISA EMAIL EXAMPLE



Identification of North Korean cyberattack by the South Korean government. (Report published by Korean Internet and Security Agency [KISA]).[84]

[84] Kim, Dongwook, Seulgi Lee, Taewoo Lee, and JaeKwang Lee. *TTPs#9:* 개인의 일상을 감시하는 공격전략 분석 *[TTPs#9: Analysis of Attack Strategies Monitoring Personal Daily Life].* Reviewed by Dae-Kyu Shin and Jaehong Sim. 2021.

Additionally, in Image 4, the North Korean term ‘련동’ /lyeon-dong/ is used instead of the term ‘연동’ /yeon-dong/. Using ㄹ/l/ instead of ㅇ is a specific North Korean language pattern.[85]

IMAGE 4: GENIANS CYBERATTACK IDENTIFICATION

North Korean cyberattack identification by private cybersecurity firm Genians. Identified by uncommon usage of certain Korean words and cross-referencing code from other North Korean cyberattacks.

One of the main difficulties in identifying North Korean hackers is their continuous development and accumulation of knowledge on their targets, societal codes, and their ability to convincingly imitate individuals, using sophisticated tactics to manipulate or deceive people into trusting them. The hackers seem to have learned how to accompany their links with less suspicious messages. In the same way, rather than just sending the link to documents immediately or a malware-holding file by email, they know how to deceive their targets by acting like a trusted contact first.

[85] Genians Security Center, Kimsuky APT 그룹의 Storm 작전과 BabyShark Family 연관 분석, October 30, 2023, 5.

2.4.2. Websites Intrusion Tactics

Another big-scale incident affected the news outlet DailyNK in 2001. Even if this hacking incident is less recent, it demonstrates how diverse and inventive North Korean hackers are in their activities. In 2001, North Korean hackers illegally accessed the DailyNK website by adding malicious code to the original one, causing users of outdated browsers to get hacked. The problem was discovered when the site went down, prompting an investigation that revealed that it had been compromised through vulnerabilities at the server provider, which had poor security measures. If the website had not crashed, it would probably have gone unnoticed. Visitors to the homepage, especially those using old versions of browsers, were contaminated, though the exact method of infection and the extent of the damage remained unclear. The breach went unnoticed for 2-3 months until public sector access to the site was blocked due to security alerts. The issue gained widespread attention after being covered by U.S. media, which was subsequently picked up by Korean outlets, further tarnishing the site's credibility. To address the issue, the organization switched to a more secure server provider with assistance from an international NGO, resolving the vulnerabilities and preventing future attacks. The incident underscored the critical importance of robust server security, as breaches not only compromise functionality but also severely damage trust and public perception.

One of the main issues for human rights organizations is that employees are occasionally tasked with website operations while they often lack IT expertise, taking on the role as part of broader responsibilities rather than as specialists. Not all North Korean human rights organizations have access to IT security experts, so this problem can occur anywhere. This creates a sense of vulnerability, as they face the possibility of attacks beyond their control that could harm both the organization and themselves. This situation underscores the urgent need for better training, stronger support systems, and more robust preventive measures to address cybersecurity threats effectively.

2.4.3. Social Media Targeting Tactics

Not only do hacking attempts occur through emails, but they are also prevalent across social media and messenger platforms. As displayed in Figure 1, 8% of the 198 participants of the survey experienced a hacking attempt, presumably from North Korea. Additionally, several interviewees discussed their experiences with such incidents, consequently expressing their concerns using social media platforms. One of them is Jung Yuna, a Korean influencer who defected from North Korea in 2006. Interested in the influencer industry after defecting, she began running a YouTube channel to discuss various issues relating to North Korea. Gaining many followers during COVID-19, she has been able to grow her channel rapidly, covering moments of her daily life and continuing to discuss aspects of the North Korean experience.

In 2023, Jung Yuna experienced a hacking attempt, which rattled her and destabilized her platform. On August 9, the channel was compromised and converted into a platform for AI-driven investment scams. The hackers used the channel to stream live broadcasts, encouraging viewers to invest in questionable financial schemes. Suspecting the involvement of a North Korean hacking group, she acted quickly to alert others about the potential dangers. Following the hack, the channel's name and content were completely altered, and its subscriber base was wiped out. She uploaded a video on Facebook to explain the situation since her YouTube channel was essentially gone.. Over the next two weeks, she persistently reported the incident to Google, describing it as a cybercrime. Eventually, Google restored the channel to its original state, just as it had been before the hacking. However, it is not possible to completely return to the previous state, as the number of views on her videos is not as high as before the hacking. [86]

Jang Hui-Joo is another North Korean defector who defected in 2007 after being sent to a political prison camp 교화소 (Gyohwaso). He now regularly posts on Facebook about North Korean issues to spread awareness among the public. He experienced a hacking incident

[86] Yuna Jung, interview by Nam Bada, Elma Duval, and Yunah Jang, PSCORE, November 13, 2024.

involving unauthorized access to his Facebook account, which he noticed due to some unusual activity that indicated a breach. The hacked Facebook account displayed posts and comments that the user did not make, including inappropriate content like adult material. He observed unauthorized logins from various locations, including foreign IP addresses, suggesting a connection to North Korean entities. Similarly to Jung Yuna, Jang Hui-Joo's hacking incident demonstrates a violation of their freedom of expression, posing significant barriers to being able to freely interact with their audience[87].

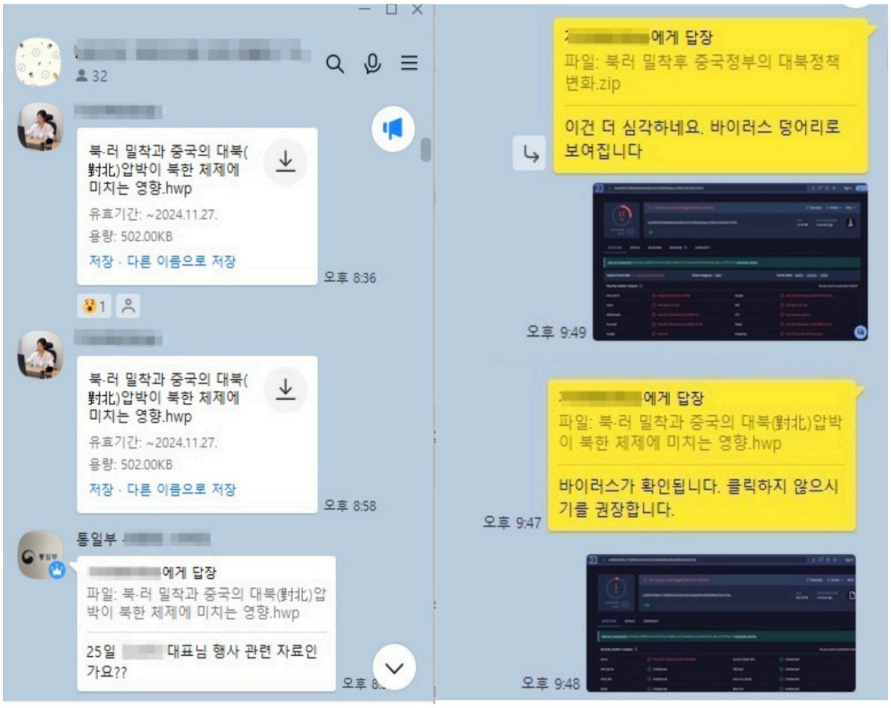
Similarly, a DailyNK reporter describes a similar form of stress, causing him to avoid being active on social media altogether. He says that in the past, he was more active on social media, but now he is not, due to concerns about sharing too much personal information, such as announcing his travel plans. He reports a constant feeling of anxiety and pressure that permeates his everyday life. [88]

2.4.4. Instant Messaging Intrusion Tactics: The KakaoTalk App as a Target

Another common network through which hacking occurs is group chats on KakaoTalk. North Korea closely targets Human Rights organizations as well as NGOs, and one of their main strike forces is through group chats, as many people are gathered in a trusted environment, making people less likely to identify disguises. Such attacks happen on a very regular basis and are perfected every time by learning from past mistakes.

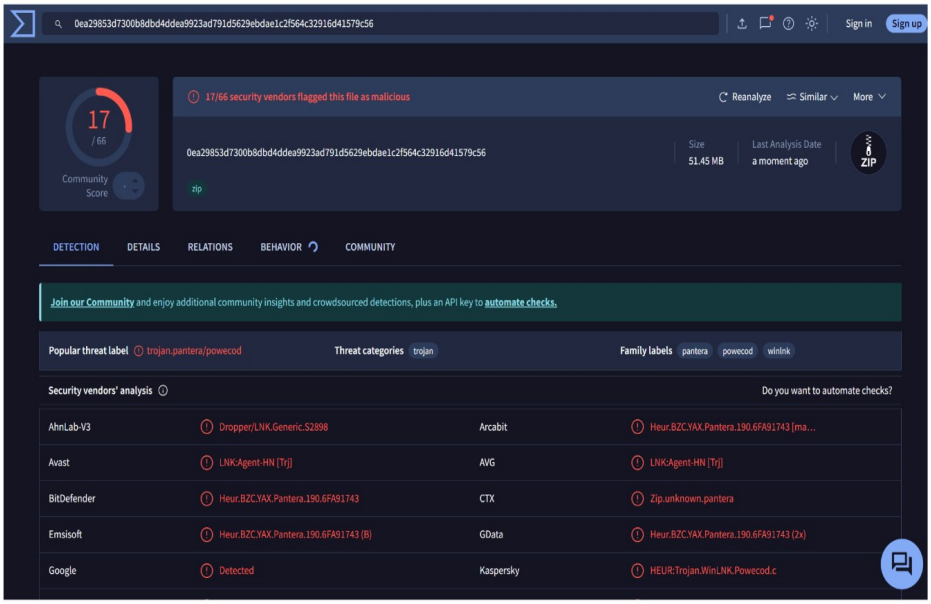
[87] Jang Hui-Joo, Interview by Nam Bada, PSCORE, December 17, 2024.
[88] Daily NK Reporter, Interview by Nam Bada, Elma Duval, and Yunah Jang, PSCORE, October 23, 2024.

IMAGE 5: KAKAO GROUPCHAT HACKING



A significant example of this occurred on the 11th of November 2024, in a group chat composed of members of the South Korean Ministry of Unification and members of NGOs working for Human Rights in North Korea. A member from this group chat happened to send a Hangul Word Processor file named '북.러 밀착과 중국의 대북 압박이 북한 체제에 미치는 영향' (Effect from North Korea and Russia's close ties and China's pressure on North Korea). The first file was sent at 8:36 pm; then the same file was sent to the same group chat again at 8:58 pm. As the file was sent without explanation, a group chat member asked if it was related to a future meeting. Then again, a document was sent, this time in a zip format, '북러 밀착후 중국정부의 대북정책 변화'(Changes in the Chinese government policy toward North Korea after tightened relations between Russia and North Korea). However, both documents were then identified as containing viruses (Image 6), one for the first document and seventeen for the second one.

IMAGE 6: PROOF OF THE PRESENCE OF MALWARES



A few people in this group chat, including someone from the Unification ministry, opened the file, causing the victims of those phishing files to feel anxious. Afterward, it was confirmed through the person from the hacked account that the files were sent from an unknown hacker as a result of a previous hacking incident. After such an attack, infected phones or computers were formatted to avoid a wider expansion of the viruses. This hacking attempt was identified by the South Korean cybersecurity platform Genians as coming from North Korea.[89]

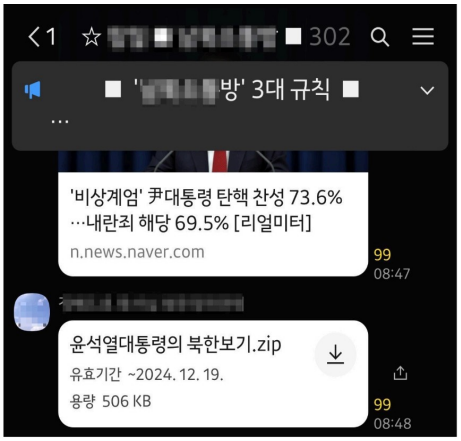
One of the things that helped to identify the hacking mentioned above was the absence of a message accompanying the file. Yet, as time passes, the hackers are also improving their techniques and disguising themselves much more efficiently. On the 3rd of December 2024, an NGO leader, who was in multiple group chats related to North Korean Human Rights organisations and North Korean defectors themselves, became another hacking victim.

[89] Genians Security Center, K 메신저로 유포된 'APT37' 그룹의 악성 HWP 사례 분석, February 7, 2025, https://www.genians.co.kr/blog/threat_intelligence/k-messenger.

Simultaneously, two different group chats were hacked.

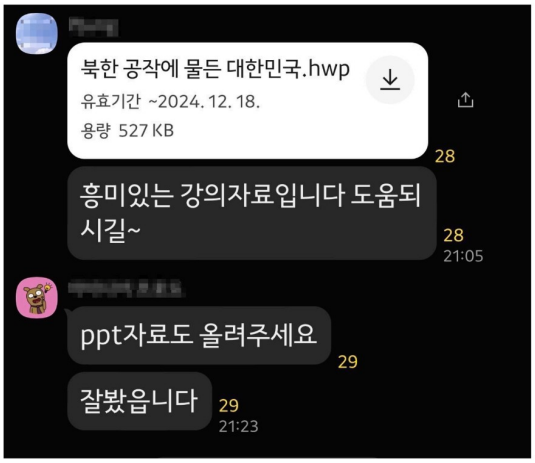
In the first group chat, a file titled '윤석열 대통령의 북한 보기' (President Yoon Seok-Yeol's perspective on North Korea) was sent at 8:48 pm. This group chat is very active, as links and documents are being sent regularly, making it easy to hide this document among the others.

IMAGE 7: FIRST SIMULTANEOUS KAKAO GROUPCHAT HACKING



In the second group chat, a file titled '북한 공작에 물든 대한민국' (South Korea influenced by North Korean maneuvers) was sent from his account at 9:05 pm. It was accompanied by the following message :

IMAGE 8: SECOND SIMULTANEOUS KAKAO GROUPCHAT



‘흥미 있는 강의 자료입니다 도움되시길 ~’

“It's interesting lecture material. I hope it can help~”

The next day, the account owner was able to send messages again, informing the members of the group chats that this was not his doing but a hacking attempt from North Korea. Consequently, he made sure to leave the group chats to avoid further spreading the virus.

Such viruses are not only dangerous due to the violation of individuals' online safety but also because they often result in the illicit sharing of personal data. A significant concern is that the primary perpetrator of these attacks is North Korea, a regime notorious for its ruthlessness, brutality, and atrocious behavior, as they are not only terrorizing and punishing individuals but also their families. These cyberattacks pose a dual threat, endangering the online and offline safety of NGO staff members and human rights workers. The source being North Korea exacerbates the fear and severity of these threats, as they go beyond isolated hacking incidents. By creating an environment of mistrust and fear, these cyber threats hinder collaboration among groups striving to improve human rights in North Korea. Furthermore, the persistent risk of malware spreading from infected devices amplifies the challenge, perpetuating an ongoing cycle of vulnerability and disruption.

“There is greater hesitation in sharing data and information, and I am hesitant to receive data from others or share my own data with partners.”

- Kang Shin-Sam[90]

[90] Kang Shin-Sam, interview by Nam Bada, Elma Duval, and Yunah Jang, PSCORE, October 24, 2024.

3. North Korean Cyber Threats and Human Rights Violations

This chapter explores the psychosocial consequences of cybersecurity breaches, portraying the vulnerabilities of individuals and communities targeted by North Korean cyber operations. The impacts of cyberattacks extend far beyond financial losses and technological disruptions. North Korea's cyber threats cause tangible damage to individuals, including psychological distress and long-term harm to the mental health of victims. Therefore, this section discusses fundamental Human Rights violations in the context of cyber threats, such as the right to security, the right to privacy, and the right to freedom of expression. Cyber operatives working under the regime face severe Human Rights violations, underscoring the systemic exploitation that enables these cyber operations to persist. By illustrating the impacts of North Korea's cyber activities, this chapter emphasizes the global implications of these threats and the necessity for coordinated international responses.

3.1. Consequences for Victims: Long-Term Effects of North Korean Cyberattacks

3.1.1. Current Research on Psychosocial Health

As cyber crimes, ranging from cyberstalking, harassment, phishing, and hacking, have increased, they have caused not only technological and economic problems, such as information leakage, but also significant personal consequences. Research into the psychosocial impacts of cyberattacks has made significant strides in recent years. For victims of cyberattack, effects include distress such as anxiety, panic, low mood, and symptoms of somatization. The experiences of crimes also heighten their perceived fear and reluctance to utilize digital tools in daily life, which may have detrimental impacts on victims' psychological and social well-being.[91] [92]

Researchers have increasingly recognized the psychological aspect of harm as a result of cybercrimes. Dr. Elias Aboujaoude, a Stanford professor of psychiatry and behavioral sciences, pointed out that personal data leakage may lead to anxiety, depression, and PTSD in victims.[93] Similarly, Dr. Ryan Louie, in his talk at the RSA Conference in 2020, also mentioned similar standpoints that cybersecurity incidents may cause mental health issues, such as depression, anxiety, PTSD-related symptoms, paranoia, and other illnesses.[94]

According to a study by Button et al. (2020), many victims experienced strong emotional reactions following computer misuse

[91] Ido Kilovaty, "Psychological Data Breach Harms," *SSRN Electronic Journal*, 2021, http://dx.doi.org/10.2139/ssrn.3785734.
[92] Alexia Palassis, Craig P. Speelman, and Julie A. Pooley, "An Exploration of the Psychological Impact of Hacking Victimization," *SAGE Open* 11, no. 4 (2021): 215824402110615, https://doi.org/10.1177/21582440211061556.
[93] Elias Aboujaoude, "Protecting Privacy to Protect Mental Health: The New Ethical Imperative," *Journal of Medical Ethics* 45, no. 9 (2019), https://jme.bmj.com/content/45/9/604.full.
[94] Ryan Louie, MD, PhD, "Quick Look: #Psybersecurity: Mental Health Impact of Cyberattacks," YouTube video, February 17, 2020, https://youtu.be/JxGar7_2KLA.

incidents. Survey data showed that three-quarters of those affected reported stress, while around seven in ten noted anxiety. Over half expressed fear, embarrassment, shame, or self-blame, and nearly half felt anger. Isolation also emerged as a concern for around two in five respondents. Around two in five also indicated symptoms of depression, panic, or anxiety-related illnesses, and a similar proportion experienced stress-related conditions.[95]

Budimir et al. (2022) examined victims' emotional experiences following cybersecurity breaches, emphasizing that these incidents often produce powerful negative reactions similar to those experienced after physical security breaches. Fear and anger emerged as the most common emotions, underpinned by uncertainty, lack of control, and perceived invasion of privacy. Victims frequently reported appraisals of unknown consequences, personal vulnerability, and potential harm to their social or professional lives. The experts further mentioned that strong negative emotions may have significant consequences that possibly unfold over time. Such consequences may include increased distrust, suspicion, and antisocial behavior (externalization), as well as depression and anxiety (internalization).[96]

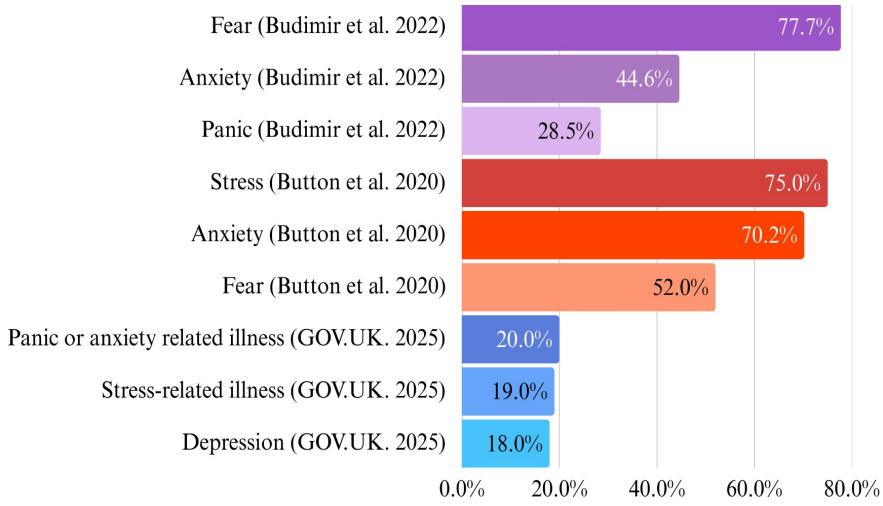
According to the report and analysis issued by the UK government, victims often reported an initial sense of shock and a subsequent loss of confidence, particularly regarding their online activities, as they fear further breaches or misuse of stolen data. Anxiety and worry are common, with some individuals feeling compelled to significantly alter their routines or avoid certain technologies. Others developed trust issues, not only toward unfamiliar digital platforms but also in interpersonal relationships if someone they knew or a known contact was implicated in the incident. In some cases, the emotional toll

[95] Button, M., L. Sugiura, D. Blackbourn, D. W. J. Shepherd, V. Wang, and R. Kapend. *Victims of Computer Misuse: Main Findings*. University of Portsmouth, 2020. https://researchportal.port.ac.uk/files/20818559/Victims_of_Computer_Misuse_Main_Findings.pdf.

[96] Budimir, Sanja, Johnny R. J. Fontaine, Antal Haans, Nicole M. A. Huijts, George Loukas, and Etienne B. Roesch. "Victim's Negative Emotion Processes in Cybersecurity Breach Situations: A Testimony of Anger and Fear-Related Emotion Processes." *SSRN*, May 6, 2022. https://ssrn.com/abstract=4101947.

extended to feelings of shame or guilt, especially when victims believed they should have recognized scam indicators or employed stronger online security practices. Overall, the report emphasizes that these emotional and psychological repercussions can persist over time, underscoring the need for accessible support services and clear guidance to help victims regain confidence and mitigate ongoing distress.[97]

FIG. 5: PSYCHOLOGICAL IMPACTS AND MENTAL SYMPTOMS OF CYBERCRIMES VICTIMS



Quantitative data cited from these studies offers valuable insights into the prevalence and intensity of emotional reactions and psychological impacts of cybercrimes, as shown in Figure. 5.[98] To strengthen our findings, we incorporated data from three research sources that surveyed similar psychological symptoms among cybercrime victims.

The 2025 GOV.UK study was particularly noteworthy due to its large sample size of over 2,500 participants and its government-backed

[97] Experiences of victims of fraud and cyber crime. (2025, January 14). GOV.UK. https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime/experiences-of-victims-of-fraud-and-cyber-crime

[98] *See supra* note 93-95.

research panel, adding greater reliability to its conclusions. Despite differences in sample sizes and methodology in these studies, the overlap in reported symptoms—such as fear, anxiety, panic, and stress-related illnesses—reinforces the significance of these psychological effects. By comparing different studies, we aim to provide a more reliable and comprehensive understanding of the severity of these psychological impacts.

3.1.2. Current Research on Physical Health

The stress from data breaches can lead to further complicated physical health problems, including headaches, fatigue, and insomnia. For example, heightened anxiety may trigger gastrointestinal issues, elevated blood pressure, or weakened immune responses. According to a 2020 survey by the nonprofit organization Identity Theft Resource Center, nearly 85% of the affected cases reported disturbances in sleeping habits, 77% reported increased stress levels, and nearly 64% said they had trouble concentrating. Symptoms of aches, pains, headaches, and cramps emerged for nearly 57%.[99]

Findings from *The Victims of Computer Misuse* report highlight several health-related impacts experienced by cybercrime victims. More than half of the surveyed victims reported difficulty sleeping. Changes in appetite, weight loss, or weight gain affected 38% of victims, indicating a broader physiological response to stress. Alarmingly, 23% of respondents disclosed self-harm, and 20% reported having suicidal thoughts, underscoring the severe psychological burden that computer misuse crimes can impose.[100]

The study by Budimir et al. (2022) highlights several physical symptoms and health impacts experienced by victims of cybersecurity breaches. Victims frequently reported high autonomic arousal, including symptoms such as rapid heartbeat, sweating, dry mouth, and tension.

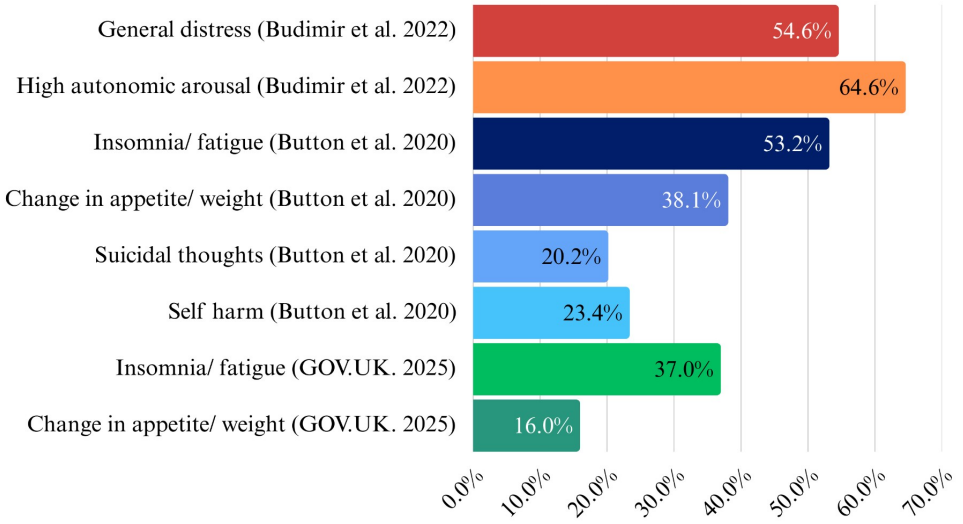
[99] Jessica Gyunn, "Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes," *USA Today*, February 24, 2020; *see also* Ido Kilovaty, *supra* note 73.
[100] *See supra* note 93.

Many also experienced general distress, often describing heaviness in the stomach, headaches, and shakiness. Some individuals reported temperature fluctuations, with sensations of heat in the head, chest, or abdomen, while others experienced cold hands or chills. The physiological responses to cybersecurity breaches often mirror those seen in victims of physical security threats, such as burglary, with high stress levels triggering bodily reactions.[101]

Similar findings from both public surveys and academic research underscore the profound and multifaceted health consequences of fraud and cybercrime victimization, emphasizing the need for comprehensive support systems to address both the psychological and physical well-being of affected individuals.[102]

As illustrated in Figure 6, data from these studies provides key insights into the prevalence and intensity of physical symptoms and behavioral impacts experienced by cybercrime victims.[103]

FIG. 6: PHYSICAL SYMPTOMS AND BEHAVIORAL IMPACTS UPON VICTIMS OF CYBERCRIME

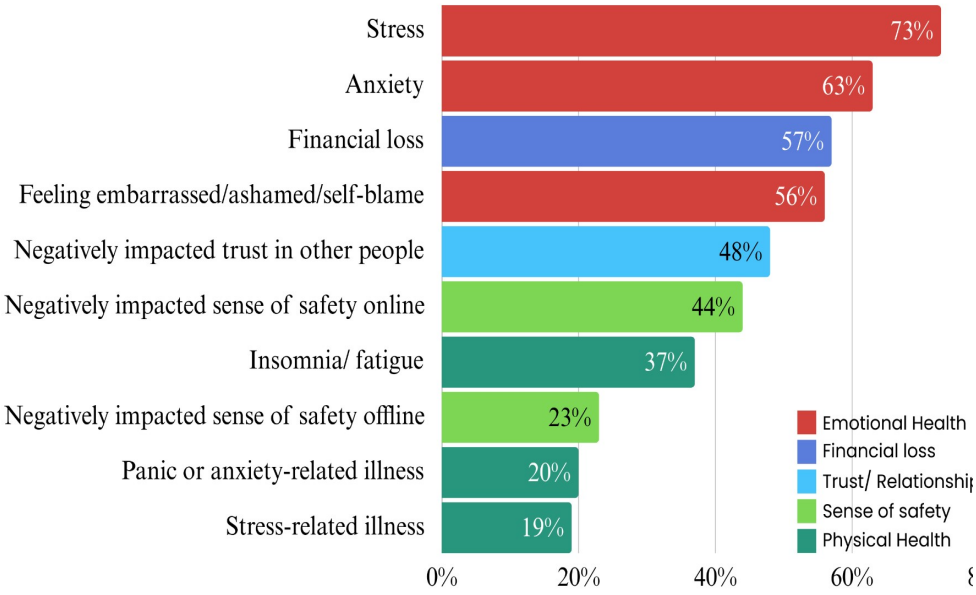


[101] *See supra* note 94.
[102] *See supra* note 95.
[103] *See supra* note 93-95.

Despite this, several limitations remain in the research on the health impacts of cyberattacks since emotions and psychological effects are difficult to quantify due to their subjective nature.[104] Current methodologies lack uniform standards for assessing emotional reactions to cyberattacks. Furthermore, most studies focus on immediate health impacts rather than long-term follow-ups for consequences. Longitudinal studies are needed to understand the persistence of impacts over time.

3.1.3. Overall Negative Impacts on Victims of Cybercrimes

FIG. 7: OVERALL NEGATIVE IMPACTS UPON VICTIMS OF CYBERCRIMES (based GOV.UK survey)

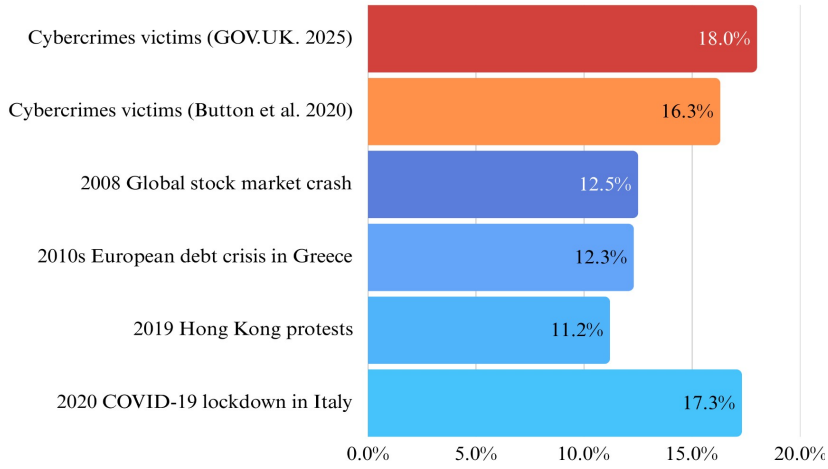


One of the largest-scale studies on cybercrime victims highlights a wide range of impacts extending beyond financial losses, including health effects and disruptions to daily lives. This is depicted in Figure 7.

[104] Karen Renaud, Verena Zimmermann, Tim Schürmann, and Carlos Böhm, "Exploring Cybersecurity-Related Emotions and Finding That They Are Challenging to Measure," *Humanities and Social Sciences Communications* 8, no. 1 (2021): https://doi.org/10.1057/s41599-021-00746-5.

Raising awareness of the full spectrum of harm can help direct the most appropriate response and resources to support victims.

FIG. 8: DEPRESSION RATES OF AFFECTED POPULATION ACROSS EVENTS



On the other hand, although psychological research has studied traditional, political or financial crises have been studied, there remains a gap in exploring and comprehending the psychological and health impacts of digital events such as cyberattacks, despite the potentially comparable levels of harm.

Figure 8 reflects the depression rate surveyed on the victims of cyberattacks and other stressful events. The research findings confirm that cyberattacks cause equally high levels of psychological distress on affected people compared with other stressful events, including the 2008 global stock market crash[105], the European debt crisis in the 2010s,[106]

[105] Rossi, R., Socci, V., Talevi, D. et al. (2020). COVID-19 pandemic and lockdown measures impact on mental health among the general population in Italy. Frontiers in Psychiatry, 11. https://doi.org/10.3389/fpsyt.2020.00790.

[106] Economou, M., Angelopoulos, E., Peppou, L.E. et al. Enduring financial crisis in Greece: prevalence and correlates of major depression and suicidality. Soc Psychiatry Psychiatr Epidemiol 51, 1015–1024 (2016). https://doi.org/10.1007/s00127-016-1238-z.

political unrest (e.g. 2019 Hong Kong protests),[107] and health emergencies (e.g. 2020 COVID-19 pandemic).[108]

The comparative data presented in the charts provides only a limited understanding of the severity of symptoms across these scenarios. Each study referenced employed different definitions, methodologies, and assessment criteria, which makes direct comparisons across events more challenging. As such, it is not yet possible to measure the psychosocial impact of cyberattacks against other events using standardized benchmarks.

However, despite these limitations, the data shed light on an important insight: the psychosocial impacts of cyberattacks, as reflected in rates of mental symptoms, negative emotions, and somatic symptoms as stress responses, should not be underestimated. This underscores the need for further research and the development of frameworks to comprehensively evaluate the emotional and psychological toll of cyberattacks alongside other traumatic events. By doing this, it will also become more apparent how help could be provided to North Korean defectors who have been victims of such cyberattacks or those who may risk being affected due to having defected.

3.1.4. Impact Assessment on Victims of North Korean Cyberattacks

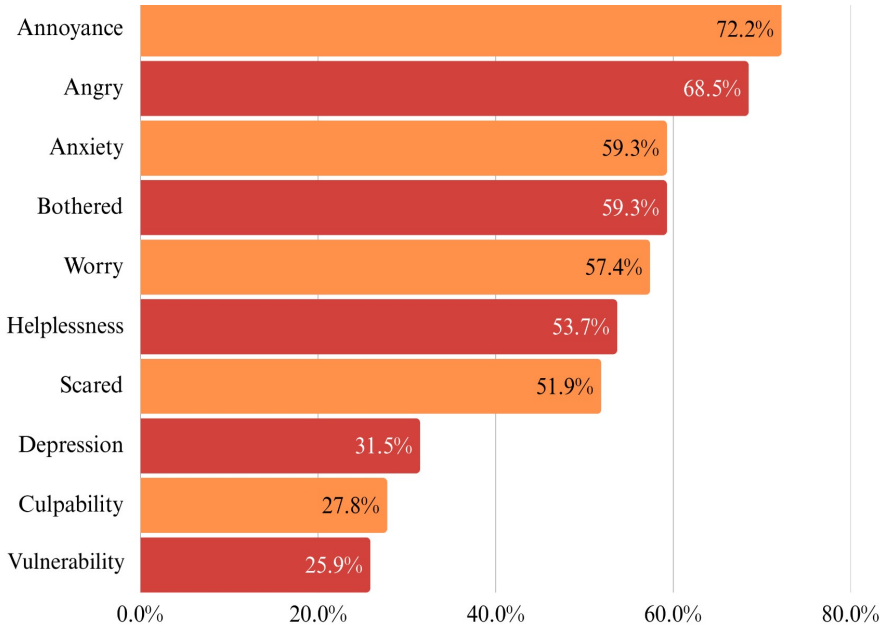
For North Korean defectors, the personal consequences of cyberattacks are often more devastating. These individuals often endure significant psychosocial vulnerabilities stemming from the severe hardships of life in North Korea, the trauma of the defection process, and the challenges of resettling in a foreign society. Many defectors face ongoing psychological stress, including anxiety, fear, and a persistent sense of insecurity, which cyberattacks can exacerbate. These attacks not

[107] Ni, M. Y., Yao, X. I., Leung, K. S. M. et al. (2020). Depression and post-traumatic stress during major social unrest in Hong Kong: a 10-year prospective cohort study. The Lancet, 395(10220), 273–284. https://doi.org/10.1016/s0140-6736(19)33160-5.

[108] Rossi, R., Socci, V., Talevi, D. et al. (2020). COVID-19 pandemic and lockdown measures impact on mental health among the general population in Italy. Frontiers in Psychiatry, 11. https://doi.org/10.3389/fpsyt.2020.00790.

only compromise their personal information but also exploit their fragile psychosocial state, amplifying feelings of vulnerability and helplessness.

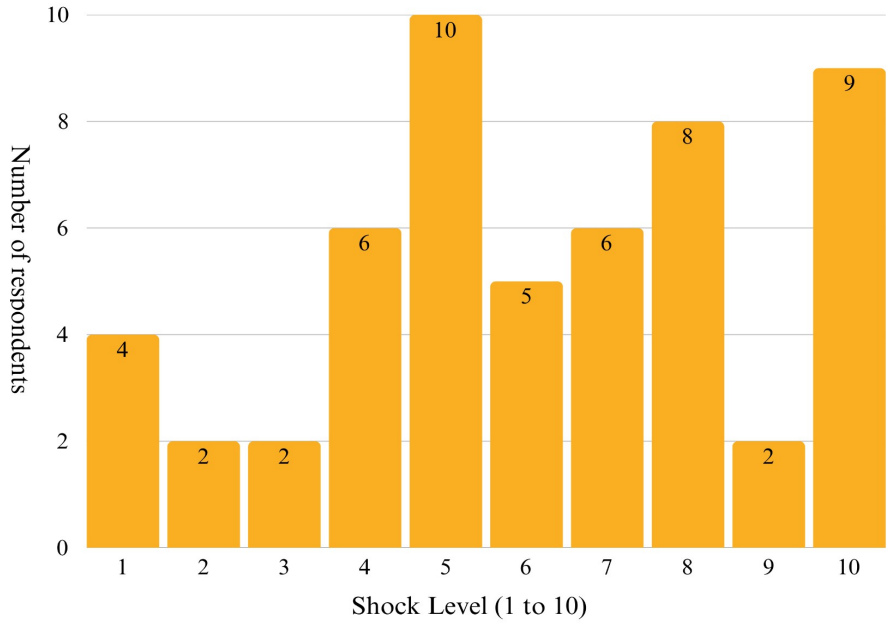
FIG. 9: FEELINGS RELATED TO CYBERATTACKS
(Feelings graded up to 3 and more on a scale of 5)



To better understand the emotional toll of cybercrimes on this vulnerable population, we conducted a comprehensive online questionnaire to examine their reactions to cyberattacks. The results illustrated in the figure below reveal a wide spectrum of emotional responses. Participants were asked to rate the intensity of feelings such as anxiety, anger, helplessness, and depression on a scale from 1 to 5. Additionally, more than 60% of respondents reported experiencing heightened levels of anxiety and annoyance, while a significant number of people also reported feeling scared, helpless, and deeply vulnerable. Many defectors and victims feared retribution from North Korea, but when they faced it firsthand, the consequences were even more severe than they had anticipated.

These findings highlight the need to address both the technical and emotional dimensions of cybersecurity threats, particularly for vulnerable populations. Therefore, technical strategies of robust cybersecurity measures are essential to protect individuals from such attacks, it is equally important to provide psychological and emotional support to victims.

FIG. 10: DISTRIBUTION OF EMOTIONAL SHOCK LEVELS
(Scale from 1 to 10)



In addition to gauging emotional responses, we also assessed the severity of the emotional shock linked to hacking attempts. This was measured on a scale from 1 to 10, as shown in the accompanying chart. The data indicates that a substantial proportion of respondents experienced extreme emotional distress, with ratings of 7–10 dominating the responses. These findings underscore the deeply personal and invasive nature of cyberattacks, which extend far beyond technical or financial damage to inflict profound psychological harm.

In sum, this survey emphasizes the importance of integrating

mental health support into the broader framework of cybersecurity policy. For North Korean defectors and other at-risk groups, access to counseling services, community support, and educational initiatives on digital safety could mitigate the long-term psychological consequences of cyberattacks. Ultimately, protecting the rights and well-being of cyberattack victims requires a holistic approach that addresses both the technical and emotional dimensions of these threats.

3.2. Human Rights Violations

3.2.1. Right to Security

The right to security, protected under Article 9 of the ICCPR, ratified by North Korea in 1966, is fundamental to ensure individuals can live free from threats, harm, or fear. Yet, the interviews PSCORE conducted revealed that North Korean cyberattacks have significantly violated this right, leaving individuals in constant fear for their personal safety. These breaches create real, daily-life threats that disrupt the victims' ability to live securely and peacefully. [109]

One of these victims is Heo Jeong-Yoon, president of an NGO advocating for the protection of Human Rights in North Korea, who has been exposed to hacking and felt threatened in a profound and personal way. Following a hacking incident, sensitive data from her smartwatch was leaked, including her home address, the address of her son's school, and her office details. This exposed her and her family to severe security risks. She explained how the constant fear of being targeted affected even the most routine aspects of her daily life, such as leaving the office to buy food or ordering delivery, both of which she avoided due to safety concerns.

[109] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome, November 4, 1950, https://www.echr.coe.int/documents/d/echr/Convention_eng.

"Of course, I am afraid. I am afraid. When I work in the office, if I am hungry but don't have anything to eat, I can't go out because I'm too afraid, so I'd have to order delivery. But I can't even do that because I'm scared they might track me."

- Heo Jeong-Yoon[110]

Heo's fear extended to deep concern for her family's safety, particularly her child. She felt helpless and powerless and unable to address these threats effectively.

"When I see my child, I'm afraid something might happen to him. My family gives me the strength to endure, but now that even our personal information has been stolen, the government does nothing. Changing the resident registration number is meaningful, but I should move houses to do it, and I can't do that now."

- Heo Jeong-Yoon[111]

The interviews also revealed recurring anxiety among victims about the possibility of others' information being compromised due to hacking incidents. Many felt a profound sense of responsibility to protect the privacy and security of those connected to them, compounding their emotional burden. One interviewee shared :

"I'm constantly worried about the possibility of information being leaked and the harm it could cause to those connected to me."

- Sa Hye-Jun[112]

[110] Heo Jeong-Yoon, interview by Nam Bada, PSCORE, December 15, 2024.
[111] Ibid.
[112] Sa Hye-Jun, interview by Nam Bada, PSCORE, October 24, 2024.

3.2.2. Right to Freedom of Expression

According to Article 19 of the ICCPR, the right to the freedom of expression protects individuals from state and private interference. This right is violated by North Korea's cyberattacks. Jung Yuna, a North Korean defector and known YouTuber had her YouTube channel hacked by these attacks. Although the issue was resolved, the event left a lasting impact on her and her platform.[113] When asked about the impact in relation to Human Rights, she responded:

> *"Even though I came to South Korea and even became a South Korean citizen, it still seems like they want to control what I say, which is really disheartening. I'm living in a free, democratic country, yet they say if we go to China, we'll be kidnapped."*
>
> - Jung Yuna [114]

For Jung Yuna, it is evident that the North Korean government violated her freedom of expression by attempting to restrict her ability to communicate with her online audience freely.

In another interview, a DailyNK reporter described the loss of freedom of expression, emphasizing how restrictions on social media, driven by fear, limit his ability to share opinions. This fear has led him to scrutinize others' information, which not only undermines his own personal freedom but also disrupts social interactions in his social circle. As a result, these actions severely restrict the fundamental right to peace and freedom of expression. [115]

[113] Yuna Jung, interview by Nam Bada, Elma Duval, and Yunah Jang, PSCORE, November 13, 2024
[114] Ibid.
[115] Daily NK Reporter, interview by Nam Bada, Elma Duval, Yunah Jang, PSCORE, October 23, 2024.

3.2.3. Right to Privacy

Under Article 17 of the ICCPR, every individual has the right to privacy, protection from unlawful interference, and security of personal information. However, the interviewees detailed severe breaches of this right through targeted hacking campaigns that exposed their personal and professional data. For instance, Sa Hye-Jun, who is a North Korean defector, described the immense stress of knowing her private information is at risk. She also noted that these hacking incidents induced feelings of paranoia, prompting heightened caution and even anxiety regarding the idea of sharing personal data in various circumstances.

> *"In the information age, having my information exposed is a huge stress, a Human Rights violation."*
>
> - Sa Hye-Jun[116]

Similarly, as previously mentioned, Heo Jeong-Yoon experienced significant emotional trauma after hackers exposed private details about her family, including her son's school, placing them in direct danger.[117] These incidents, coupled with the broader reports from other victims, demonstrate how such hacking campaigns are used not only to infringe on their privacy but also as a means of intimidation and control, directly violating international Human Rights obligations.

3.2.4. Right to Just and Favorable Conditions of Work

Article 7 of the ICESCR guarantees the right to just and favourable conditions of work, yet despite being ratified by North Korea

[116] Sa Hye-Jun, interview by Nam Bada, PSCORE, October 24, 2024.
[117] Heo Jeong-Yoon, interview by Nam Bada, PSCORE, December 15, 2024.

in 1981, Human Rights violations continue to occur.[118] As presented earlier, in the three generations of Human Rights, the second generation mainly focuses on social rights and emphasizes the importance of equal social conditions.

Such favourable conditions are violated through North Korean cyberattacks. Indeed, among our interviewees, defectors working in radio or video-related fields and other online activities expressed annoyance at the attacks that are limiting their activities, but also a high concern for the safety of people they work with. Cyberattacks violate the right to work in two main ways: they hinder the development of credibility and trusted relationships, causing a loss of trust, and they also compromise people's private information exchanged in a professional context. This problem poses a significant burden to those who have to keep in contact with North Korean defectors, as the defectors they work with are more likely to have their information stolen or be monitored by North Korea.

> *"If information gets leaked, I could lose the trust I've been building, and I'm worried that I might be perceived as someone unreliable to work with."*
>
> - Sa Hye-Jun[119]

> *"I was most afraid of breaking the trust I had promised if the information was leaked."*
>
> - Park Seong-Min[120]

Moreover, Human Rights organizations are amongst the most targeted when regarding cyberattacks from North Korea. NGOs such as

[118] United Nations, "International Covenant on Civil and Political Rights, Adopted by the General Assembly of the United Nations on 16 December 1966," Reference C.N.467.1997.TREATIES-10 (Depositary Notification), https://treaties.un.org/doc/Publication/CN/1997/CN.467.1997-Eng.pdf.
[119] Sa Hye-Jun, interview by Nam Bada, PSCORE, October 24, 2024.
[120] Park Seong-Min, interview by Nam Bada, PSCORE, December 17, 2024.

the Unification Academy (통일아카데미), PSCORE, etc. receive hacking attempts via email or through messaging apps on a weekly basis. One Human Rights organization leader reported experiencing suspicions of being hacked, attributing this to his recent public recognition. The precaution he has taken is to refrain from opening any email he receives in Korean, clearly demonstrating a heightened sense of anxiety. He felt infuriated, as he was no longer able to conduct his activities as usual due to this invasion of privacy and felt that his right to peace was infringed upon. This is comparable to the experiences of other Human Rights organization leaders who report similar feelings of their freedom of expression being restricted and their right to security and safety being violated. This identification of Human Rights being violated clearly demonstrates the impact the cyber threats have on victims.

3.2.5. Right to Take Part in Cultural Life

Article 15 of the ICESCR provides the right to participate in cultural life.[121] This right is implicated by the cyber threats and attacks orchestrated by North Korea. Consequently, cyberattacks pose a tangible threat to individuals' ability to develop and maintain a social life. These following statements underline the profound psychological and social impacts of hacking, including the damage to people's ability to foster relationships. Without comprehensive cybersecurity measures, the digital realm risks becoming a space of fear and disconnection rather than one of opportunity and connection. Another very interesting point that was mentioned during our interviews is the fact that daily life and interpersonal relations cannot be separated from digital interactions.

[121] United Nations, "International Covenant on Civil and Political Rights, Adopted by the General Assembly of the United Nations on 16 December 1966," Reference C.N.467.1997.TREATIES-10 (Depositary Notification), https://treaties.un.org/doc/Publication/CN/1997/CN.467.1997-Eng.pdf.

"Modern people cannot be separated from the online world. Because of threats, it is impossible to live safely."

- Sa Hye-Jun[122]

By jeopardizing people's online activities, North Korea is consequently limiting their right to maintain social interactions with others, as well as the right to enjoy a cultural life. Indeed, much of cultural expression and social engagement takes place online, whether through social media, discussion forums, or streaming services that facilitate shared cultural experiences. By instilling fear of creating personal online accounts or simply participating in digital activities, the state effectively restrains these essential forms of interaction and expression. As a result, people are discouraged from exploring and enjoying the wide array of information and cultural content available online.

3.3. North Korean Domestic Human Rights Violations

While the North Korean regime works to target those external to the country, the scope of Human Rights violations also extends inwards, particularly to the regime's own workers. As such, it is essential to understand the inner workings of the North Korean government by shedding light on the working conditions of its employees. These range from construction workers to maritime workers who are sent abroad to work for the North Korean state under challenging working conditions. Coupled with such circumstances, workers are rarely compensated financially, with the regime withholding most of the funds earned by the workers for their own activities. These conditions undoubtedly violate various Human Rights. Such exploitation must be examined in the context of Human Rights to understand the severity of North Korea's cyber capabilities. It is critical to understand IT workers as victims of

[122] Sa Hye-Jun, interview by Nam Bada, PSCORE, October 24, 2024.

North Korea's cyber agenda.

3.3.1. History of North Korean IT Workers

Starting from 1958, North Korea began developing its software industry as a way to create a self-sufficient national economy. In the late 1990s, the state began developing software-centered technology while also opening the Korea Computer Center, the primary North Korean government information technology center. During this decade, the computer science colleges Kim Il-Sung University and Kimbuk Industrial University, the two leading software developer training units today, were established as a means for the state to begin training future IT workers.

In the beginning of the 2000s, North Korea began to expand its efforts, developing an overseas outsourcing program that constituted a new revenue source for the North Korean regime. From 2009 to 2012, the numbers of outsourcing projects boomed, with increasing numbers of IT workers being sent overseas. In correlation to this increase, the first graduate school of IT was opened in the Pyongyang University of Science and Technology. However, in 2016, there was a surge in IT training and dispatchment overseas. Since then, the North Korean regime has been developing fake employment, IDs, and startups. Moreover, during the COVID-19 pandemic, rapid growth was observed. [123]

Around 40-80% of the IT developers' involves securing a disguised identity, as maintaining this false identity is essential for conducting operations without leaving a trace. IT workers typically complete many projects under multiple fake identities at once. Such projects include developing major products such as anti-viruses (Shinki, Clocksae, Chambit, Sili), AI products (voice recognition, image recognition, speaker recognition, multilingual translator, document proofreading, etc.), and software features on both IOS and Android.

[123] Ji-min Kim, "Lecture on North Korean IT Workforce," 2024.

3.3.2. Revenue generation

The revenue from outsourced IT labor is strictly managed. Workers receive payments exclusively through third-party accounts, such as PayPal, ensuring that North Korean authorities retain full control over financial transactions. Of the earnings, 90-95% is seized by the state, leaving only a fraction for the workers themselves. This system is highly centralized, with 40% of IT teams operated by the military, another 40% by military-industrial institutions, and the remaining 20% managed by the Workers' Party and Cabinet. The vast majority of the revenue generated, around 80%, is allocated to military operations and weapon production, while the remaining portion funds party and state activities.

North Korea's overseas IT labor deployment operates entirely differently from standard foreign employment contracts. Instead of individual workers signing formal contracts with foreign companies, IT teams formed in North Korea are dispatched abroad to perform outsourced IT work, with their earnings being handed over to the North Korean government.

These workers are primarily sent to China and Southeast Asian countries, where they engage in money laundering and identity fraud to conceal their true nationality. The North Korean authorities instruct them to assume false identities, often posing as Chinese, Singaporean, or Japanese nationals. Before dispatching them, the government ensures the presence of local contacts who can handle any legal complications that may arise.

3.3.3. North Korean IT Worker Training

North Korea has developed an extensive process for picking and training their IT personnel and hackers. In what some call a 'training pipeline', young North Koreans with talent in mathematics or science are selected and sent to special middle and high schools. Afterward, they are sent to universities such as the Kim Il Sung University and the Kim Chaek University of Technology, which are particularly involved in producing a notably high number of threat actors. Many are sent abroad

after their university education to further develop their cyber knowledge. After becoming adequately skilled, they can be hired by the Reconnaissance General Bureau to start their cyber career.[124]

Kim Jong-un has described cyber warfare capabilities as 'a magic weapon' and repeatedly announced his perceived importance of developing cyber forces.[125] The streamlined process of turning math and science talents into threat actors fits this perspective.

Even at IT-focused universities, access to internet records is tracked and managed, and any downloaded data is provided only after censorship. Because North Korea's internet infrastructure is so limited, the government grants direct internet access to only a handful of individuals. According to interviewees, in practice, just one specialized company enjoys genuine internet access, while university students must rely on closed networks or simply printed textbooks.

After graduating from university, for around a year, future IT workers receive domestic training. From there, a group is chosen, formed into teams, and dispatched. Typically, each team trains together for a month before deployment, guided by a leader with significant responsibility. They must also craft new identities through so-called "ID laundering," a process nearly as impressive and indicative of their skills as any of their other activities.[126]

3.3.4. North Korean IT Worker Activities

IT workers are responsible for outsourced projects such as software development, website creation, and mobile application programming. More specifically, they are given assignments to handle tasks such as mobile OS modifications, AI applications, games, and smaller activities. These projects are completed for international clients

[124] Dylan Stent, "The Great Cyber Game," *New Zealand International Review* 43, no. 5 (2018): 6–9, 2.
[125] "N.Korea Boosting Cyber Warfare Capabilities," *The Chosun Daily*, November 5, 2013, https://www.chosun.com/english/north-korea-en/2013/11/05/NWRSKRXUWGKJNC42NMTELCNINY/.
[126] Na Jeong-Seok, Interview by Nam Bada, PSCORE, 15th December 2024.

under falsified identities. Assignments are typically completed in small teams, depending on the nature of the project. These teams work closely together for several years and follow a team leader or supervisor figure who closely monitors the activities of the IT workers. Not only that, but an individual from the state security department comes to the office to further survey the activities of the IT workers.

Their working hours typically exceed 10 hours, and they often work during nights to cater to international clients in various time zones. This strenuous working schedule often leads to sleep deprivation and irregular schedules. Workers live in cramped areas with 5-6 individuals, typically those in the same project team, sharing small accommodations. Furthermore, these workspaces are located in remote areas where workers are isolated from family members and any outside social interaction. Their freedom of movement is severely restricted, with only one walk permitted per day and occasional outings once a week. They are forced to work long hours in isolation, suffering from immense psychological stress due to the oppressive conditions.

Workers are required to meet strict monthly revenue targets, and failure to do so results in public humiliation and intense psychological pressure from team leaders. Some workers even face physical abuse as a means of coercion. Verbal threats and constant performance monitoring are common, creating a work environment where many workers experience psychological trauma. Some have even managed to escape to South Korea and other countries, seeking refuge from the unbearable conditions.

Additionally, these workers cannot obtain legal employment statuses. Due to UN sanctions prohibiting North Korea from officially deploying overseas workers, North Korean IT laborers must fabricate multiple layers of false identities. The effort, time, and fees required for this process further diminish their actual earnings.

However, despite these exploitative conditions, many IT workers still seek opportunities to work abroad because earning foreign currency, even in small amounts, is considered a rare opportunity in North Korea.

Since foreign currency exchange rates are highly favorable inside North Korea, even 5-10% of their earnings is a substantial amount compared to domestic wages. Many are not aware that their work is illegal but rather see it as a means to support their families and save money. As a result, they actively pursue these opportunities despite the risks and exploitative system.

The severe exploitation and coercive control mechanisms governing North Korea's overseas IT workers constitute clear violations of international labor and human rights standards. Stronger international oversight and intervention are necessary to address this systemic abuse and hold the North Korean regime accountable.[127][128]

3.4. Violations of North Korean IT Workers' Human Rights

3.4.1. Right to Security

Not only do we aim to address the violations of Human Rights as pertaining to hacking victims, but we also aim to shed light on the conditions of IT workers in order to highlight and address the corrupt North Korean cyber system as a whole. One factor contributing to such pressure is the constant surveillance workers are subjected to, with all communications and transactions being closely monitored. This intense scrutiny limits their internet use and access to information, further deepening their isolation. Besides closely watching IT workers, supervisors and team leaders also use screen monitoring installations. If these programs are turned off by the workers, they are flagged and reprimanded for doing so.

[127] Kim Ji-Min, interview by Nam Bada, PSCORE, August 2024.
[128] Na Jeong-Seok, interview by Nam Bada, PSCORE, December 15, 2024.

"[The supervisors] tell [the IT workers] that 'the moment you turn this program off you're already a bad guy' to make them aware that they are being intentionally monitored…"

- Kim Ji-Min[129]

Such involuntary monitoring creates stress and anxiety among the IT workers whose every action is closely observed.

"It's human to want social interactions and to communicate, but meeting and communicating in-person is blocked and online communication isn't allowed."

- Kim Ji-Min[130]

Such conditions create significant stress, violating both the right to peace and the right to security for individuals. Another factor for stress is the pressure to perform and meet high standards. IT workers are required to meet a large quota of earnings from their various projects. With tight supervision, these difficult quotas create feelings of anxiety in the workplace, as noted by our interviewees. Na Jeong-Seok is a former IT worker who entered the Information Industry Guidance Bureau of North Korea in 2012. He was selected to be dispatched to China as a 'researcher' after working in North Korea for 3 years. Na Jeong-Seok highlights the pressure to perform, linking it to the lack of sleep brought on by demanding workplace expectations, noting:

[129] Kim Ji-Min, interview by Nam Bada, PSCORE, August 2024.
[130] Kim Ji-Min, interview by Nam Bada, PSCORE, August 2024.

"I couldn't sleep and kept working. I was very stressed because my assignment wasn't going well."

- Na Jeong-Seok[131]

In another grave account from Kim Ji-Min, he mentions how the work-related stress and the pressure to perform take an immense toll on IT workers' mental health, making them vulnerable to conditions like depression and panic disorders. He mentions that his coworkers have taken their own lives due to these strenuous conditions. Such incidents illustrate how these difficult and intense conditions consume IT workers to an extreme extent. These sentiments and experiences clearly violate their right to security and right to peace.

3.4.2. Right to Have an Adequate Standard of Living

Article 25 of the UDHR declares that "everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control."[132] The conditions of IT workers fail to meet these standards, as they are placed in remote locations and social interactions are tightly restricted.

Additionally, several of the interviewees mentioned a lack of sleep due to the nature of their work. The daily lives of IT workers revolve around developing software and completing online assignments, often working late into the night. This nocturnal schedule disrupts their sleep patterns, leaving little room for rest or consistency. Kang Ju-Won is a former IT worker who worked in program development overseas in Southeast Asia under North Korea. When describing his work schedule,

[131] Na Jeong-Seok, interview by Nam Bada, PSCORE, December 15, 2024.
[132] United Nations General Assembly, *Universal Declaration of Human Rights*, 217 A (III), December 10, 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

he notes:

> *"We sleep a bit during the day, and since it's a system where we work during the night time, you do assignments through the Internet at night and continue to develop during the day. So it's a little difficult to develop a program but since it's the set routine, you can't do it a different way".*
>
> - Kim Ju-Won[133]

Although the perpetrators work in a wide range of sectors for North Korea related to cyber threats, many of the interviewees noted that their work routines are unpredictable, dictated by client demands, making it almost impossible to establish any semblance of a structured day.

3.4.3. Right to be Free from Slavery and Forced Labour

The Article 8 of the ICCPR prohibits slavery and forced labor, stating that "no one shall be held in slavery; slavery and the slave-trade in all their forms shall be prohibited."[134] The article states that "no one shall perform forced or compulsory labor," yet IT workers under the North Korean regime receive only partial compensation, contingent on meeting high quotas.

[133] Kim Ju-Won and Kim Bom-Seok, interview by Nam Bada, PSCORE, October 6, 2024.
[134] United Nations, "International Covenant on Civil and Political Rights, Adopted by the General Assembly of the United Nations on 16 December 1966," Reference C.N.467.1997.TREATIES-10 (Depositary Notification), https://treaties.un.org/doc/publication/CN/1997/CN.467.1997-eng.pdf.

"I only received about 5% of the money I earned as an allowance. It was big back then too. In North Korea, you have to do unpaid work"

- Na Jeong-Seok[135]

Although Na Jeong-Seok notes that his pay might have made his conditions better compared to unpaid workers, his funds were limited and he had little freedom to spend his small allowance. Despite the harsh conditions and meager compensation, these workers are required to hand over approximately 90 to 95% of their earnings to the North Korean regime. This contribution is framed as an act of patriotic duty, a testament to their loyalty to the state, even if it comes at the cost of their own well-being. However, these allowances are only given to workers who reach pre-determined quotas, placing immense pressure on the workers. According to Na Jeong-seok, quotas are set by the government and vary from worker to worker. Most of his coworkers sent money back to North Korea to their families, but because this was only permitted if workers could reach a high quota, IT workers felt immense pressure, undertaking the responsibility to support their families.

"Even if I can't secure the money for myself, there's a lot of pressure to fulfill the quota."

- Na Jeong-Seok[136]

Forced labor with no compensation in the case that individuals do not meet a quota clearly violates the ICCPR's Article 8. Paired with such difficult work conditions and little autonomy, it is essential to address such violations of Human Rights of IT workers employed by North Korea.

[135] Na Jeong-Seok, interview by Nam Bada, PSCORE, December 15, 2024.
[136] Na Jeong-Seok, interview by Nam Bada, PSCORE, December 15, 2024.

3.5. Other Implications

Although not formally ratified, North Korea's cybercrimes implicate other theoretical Human Rights violations such as the right to peace and human dignity.

The right to peace is widely recognized as a third-generation Human Right.[137] The concept has been repeatedly affirmed in international agreements, such as the 1984 Declaration on the Right of Peoples to Peace, where the UN General Assembly solemnly proclaimed that "the maintenance of a peaceful life for peoples is the sacred duty of each state."[138] Similarly, the 2016 Declaration on the Right to Peace[139] reaffirmed the significance of this right in global governance, though it remains categorized as a soft law.[140] [141] Also, we can see that the efforts to recognize the right to peace as a human right continue to grow, with conventions and declarations highlighting its importance as a collective and individual right.

The testimonies of North Korean Human Rights activists like Heo Jeong-Yoon and Kang Shin-Sam further illustrate the pressing need to formalize the right to peace. Heo Jeong-Yoon describes the emotional trauma caused by security breaches, while Kang Shin-Sam emphasizes that constant threats make it "*impossible to lead a safe life*."[142] These experiences reveal how the absence of a legally binding framework leaves individuals vulnerable to sustained violations of their peace and security, particularly in contexts of systemic intimidation and cyberattacks, while also enabling perpetrators to act with impunity due to

---

[137] Rakesh Kumar Singh, "Right to Peace as a Human Right," *Uttarakhand Judicial & Legal Review* 3, no. 2: 40–47, https://ujala.uk.gov.in/files/Ch5.pdf.

[138] United Nations General Assembly, *Declaration on the Right of Peoples to Peace*, A/RES/39/11, Adopted November 12, 1984, https://digitallibrary.un.org/record/74608?ln=en.

[139] United Nations General Assembly, *Declaration on the Right to Peace*, A/RES/71/189, Adopted December 19, 2016, https://digitallibrary.un.org/record/858594?ln=en (n.d.).

[140] Tuba Turan, "The 2016 UN General Assembly Declaration on the Right to Peace: A Step towards Sustainable Positive Peace within Societies?" *Human Rights Law Review* 23, no. 2 (March 10, 2023), https://doi.org/10.1093/hrlr/ngad007.

[141] Soft laws are non-binding guidelines, principles, or standards that influence behavior and decision-making without having the enforceability of formal legal obligations.

[142] Kang Shin-Sam, interview by Nam Bada, Elma Duval, and Yunah Jang, PSCORE, October 24, 2024.

the lack of prosecution mechanisms. While the right to peace remains aspirational, the growing recognition of its necessity in the international arena is a hopeful step toward its eventual codification and enforcement.

These cyber crimes also violate concepts of human dignity. While dignity has and can be defined in a myriad of ways, the precise definition need not be addressed to claim that human dignity has been violated. The abovementioned cyberattacks limit and infringe upon the Kantian conception of "dignity as autonomy" as the attacks impose fear and threat of imminent consequence, thus limiting action and autonomy.[143] The attacks also violate the Rousseauian conception of communitarian dignity that highlights the egalitarian understanding that all humans deserve a certain baseline of rights. When certain individuals are targeted due to status rather than wrongdoing, this egalitarian right is violated.[144]

[143] Christopher McCrudden, "Human Dignity and Judicial Interpretation of Human Rights," *European Journal of International Law* 19, no. 4 (September 1, 2008): 655–724, https://doi.org/10.1093/ejil/chn043.
[144] Ibid, 660.

4. Responses To the North Korean Cyber Threats

Cyber attacks have emerged as a significant threat to global security and Human Rights, calling for immediate international, regional, and domestic responses. There has been an increase in dialogue and recognition of the importance of cybersecurity from attacks by rogue states. However, no sanctions or counteractions have been put in place by the international community to address these issues. Various stakeholders, including the United Nations, individual nations, civil society, and the private sector, have taken action, but they have been limited in nature. This highlights the need for a comprehensive and collaborative approach to combat North Korean cyber threats effectively.

4.1. Relevant International Law

4.1.1. UN Response

In response to North Korea's nuclear and missile activities, the United Nations Security Council (UNSC) has been taking measures to the extent possible. Since 2006, it has adopted a total of twenty-one resolutions directly concerning North Korea's illegal activities.[145] These resolutions primarily aimed to curtail North Korea's ability to fund its ballistic missile programs by freezing assets, restricting trade in military goods and luxury items, and imposing financial sanctions. However, none of these resolutions directly address the growing issue of cybercrime, which has become a significant concern, according to professors V.K. Rai, S.K. Sonkar, and S. Nappo.[146] In their 2023 paper, they emphasize the urgent need for the international community to recognize cyberattacks and cybercrimes as violations of Human Rights. They argue that these attacks jeopardize personal privacy, freedom of expression, and human security—key pillars of Human Rights.

Among the most recent UNSC resolutions regarding North Korea is the Report of the Panel of Experts Pursuant to Resolution 2397 (S/2024/215)[147], which partly targets North Korean cyber activities and acknowledges the role of IT workers in cybertheft and attacks designed to fund the regime. While it marks progress, it does not address the Human Rights violations tied to these activities, such as breaches of privacy and freedom of expression. Other resolutions, such as 2397 (2017)[148] and

[145] United Nations Security Council, *Resolutions and Decisions of the Security Council: 1 August 2009 – 31 July 2010*, in *Security Council Official Records*, ISSN 0257-1455 (2010), https://digitallibrary.un.org/record/697781/files/S_INF_65-EN.pdf.

[146] V K Rai and Santosh Kumar Sonkar, "Why It Is Time to Start Treating Cybersecurity Like a Human Rights Issue," *International Journal For Multidisciplinary Research* 5, no. 3 (May 17, 2023), https://www.ijfmr.com/papers/2023/3/3071.pdf.

[147] United Nations Security Council, Report of the Panel of Experts Pursuant to Resolution 2397 (2017), March 2024, S/2024/215, https://docs.un.org/en/S/2024/215.

[148] United Nations Security Council, Resolution 2397 (2017), Adopted at the 8151st Meeting on December 22, 2017, S/RES/2397 (2017), https://documents.un.org/doc/undoc/gen/n17/460/25/pdf/n1746025.pdf?OpenElement.

2270 (2016)[149], have focused on restricting traditional revenue sources, including petroleum imports, labor exports, and coal trade, to limit funding for nuclear and missile programs. However, none directly confront North Korea's increasing use of cybercrime to bypass sanctions and sustain its operations.

This gap highlights the need for the international community to make its approach evolve accordingly with emerging threats, as cyber activities have become an increasingly prominent feature of North Korea's strategy to sustain its regime and evade international pressure. Addressing cybercrime would not only strengthen the existing sanctions regime but also provide a response to the challenges posed by North Korea.

4.1.2. Multilateral Tools

The Tallinn Manual (2013)

The Tallinn Manual was issued in February 2013 by NATO as a document clarifying how international law applies in cyberspace. It provides non-binding guidelines from an objective perspective, offering a global understanding of the legality of cyber operations. Its objective is to clarify legal rules concerning sovereignty, international security, state responsibility, and Human Rights protection in cyberspace. It addresses critical issues such as the use of force, self-defense, and international cooperation in cybersecurity.[150] The manual defines key notions such as the Principle of Sovereignty, which, even if not universally recognized, is clearly defined in physical worlds, and is unclear in cyberspace. It also defines the important notion of Due Diligence, which holds states accountable for their cyber activities, both within and beyond their

[149] United Nations Security Council, Resolution 2270 (2016), Adopted at the 7638th Meeting on March 2, 2016, S/RES/2270 (2016), https://main.un.org/securitycouncil/en/s/res/2270-%282016%29.

[150] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights", *Georgetown Journal of International Law*, 48. https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

borders. The manual also clarifies that a state has full responsibility for its cyber actors and activities. This clearly highlights the devoir that states must hold rogue actors accountable for their actions. Finally, Rule 35 of the manual affirms that "individuals enjoy the same international Human Rights with respect to cyber-related activities that they otherwise enjoy".[151] It also stresses the need for a legal framework that covers both conflict-related and peacetime cyber operations. As a document from an objective perspective, it does not directly address the North Korean threat but provides an essential general reference framework for the formulation of cybersecurity and cyber defense policies.

The Budapest Convention

In 2001, the European Council signed the Budapest Convention on Cybercrime - the first legally binding international treaty on cybercrime and widely regarded as the most significant global agreement on the subject. The Convention aims to provide a harmonised approach to combating cybercrime by providing a guideline for countries that develop domestic legislation on cybercrime and to permit "hundreds of practitioners from Parties to share experiences and create relationships that facilitate cooperation".[152] By June 2024, 75 States were Parties to the Convention - including the countries of the European Union, the United States, Japan, the Philippines, Nigeria, in Peru - and 16 countries had been invited to accede, including South Korea, South Africa, and Mexico. This Convention helps investigate transnational cybercrime and secure volatile electronic evidence. By effectively signing the convention, South Korea and other countries that have fallen victim to North Korean cyberattacks could benefit from this international cooperation. As a multilateral tool, this could enable them to strengthen their ties with signatory countries and to capitalize on their resources to tackle this issue more successfully. In turn, this could also reinforce

[151] Michael N. Schmitt, "International Human Rights Law", *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*", Cambridge University Press, 2017, pp. 179-208.

[152] "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols", Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

international pressure on North Korea, and states targeted by cyber threats could, therefore, advocate specific sanctions against North Korean cyber units.

The United Nations Convention on Cybercrime (2024)

More recently, in December 2024, the United Nations General Assembly also adopted the United Nations Convention against Cybercrime[153], a legally binding global treaty aimed at strengthening multilateral cooperation in the fight against cybercrime. It is the first international criminal justice treaty negotiated in over 20 years and the first one focusing on cybercrime.[154] The General Assembly's President, Philémon Yang, highlighted the connection between cyberthreats and Human Rights, stating that "With the adoption of this Convention, Member States have at hand the tools and means to strengthen international cooperation in preventing and combating cybercrime, protecting people and their rights online".[155] The Convention emphasizes the impact of cybercrimes on a wide range of actors, including states, enterprises, and individuals. It also acknowledges the consequences on victims and the need for protection and justice.[156] The Convention against Cybercrime will open for signature in Hanoi, Vietnam, in 2025 and will enter into force once ratified by at least 40 states. The drafting process had begun in 2017, led by states such as Russia and, notably, North Korea, both of which were dissatisfied with the Budapest Convention, claiming that the convention was violating state sovereignty. However, these countries view the final Convention as overly restrictive.[157] As a result, it remains uncertain whether North Korea will sign and ratify the Convention. If it does, however, this could represent a significant step

[153] Ibid.
[154] Vibhu Mishra, "UN General Assembly adopts milestone cybercrime treaty", *UN News*, December 2024, https://news.un.org/en/story/2024/12/1158521.
[155] Ibid.
[156] Ibid.
[157] Lisandra Novo, "The UN finally advances a convention on cybercrime… and no one is happy about it", August 2024, *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/the-un-finally-adopts-a-convention-on-cybercrime-and-no-one-is-happy/.

toward regulating the state's illegal cyber activities.

4.2. Enforcement Mechanisms in the ICCPR and the ICESCR

As a signatory to both the ICCPR and the ICESCR, North Korea is legally bound to adhere to and be subject to the provisions of both covenants. The covenants protect different sets of rights, as mentioned in Section 3, and have different enforcement mechanisms. Recognizing that international enforcement of rights and obligations is often complicated and consequential, the ICCPR and ICESCR offer a starting point for highlighting Human Rights violations and beginning the process for a greater structural and systemic shift toward bringing both domestic and international justice.

The ICCPR gives way to meaningful but ultimately limited measures to rectify violations to the right to security (article 9), the right to freedom of expression (article 19), the right to privacy (article 17), and the right to be free from slavery and forced labor (article 8). The ICCPR requires that every member state submit regular reports to the ICCPR Human Rights Committee (HRC), but North Korea has failed to do so since its last report in August 2001.[158] As an alternative, ICCPR allows NGOs and member states to submit inquiries and concerns to the HRC for the Committee to identify violations and to make the appropriate declarations. Additionally, article 41 of the ICCPR allows a member state to bring claims of rights violations against another state to the HRC. Unfortunately, article 41 requires that both the complaining state and the state complained recognize the authority of the HRC to hear these complaints, which North Korea has not done. Finally, the ICCPR First Optional Protocol allows for individuals who have exhausted domestic remedies of violations to bring claims against their States to the HRC. Even if North Korea did ratify the First Optional Protocol, for

[158] Second Periodic Report of the Democratic People's Republic of Korea on its Implementation of the International Covenant on Civil and Political Rights, U.N. Human Rights Committee, U.N. Doc. CCPR/C/PRK/2000/2 (2000), available at https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FPRK%2F2000%2F2&Lang=en.

rather obvious reasons, this measure is typically not viable for North Korean citizens, meaning that the ICCPR provides the framework for demonstrating the relevant Human Rights violations but does not provide adequate enforcement remedies.

The ICESCR, on the other hand, protects the right to just and favorable conditions of work (article 17) and the right to take part in cultural life (article 15), which section 3 has explained how North Korea has violated. ICESCR Articles 16 and 17 require that as a signatory, North Korea is obligated to produce periodic reports on the legal and political measures that the state has taken to comply with the ICESCR. North Korea submitted its last report in April of 2002 and has failed to submit reports since. However, like the ICCPR, the ICESCR is weak in its enforcement power. The treaty does not provide for counteraction, bringing focus and urgency to the international community to build pressure and find solutions elsewhere. In short, neither treaties provide adequate responses to the clear and critical Human Rights violations that North Korea has committed. Greater action is required.

4.3. Further Approaches

4.3.1. South Korea's Response: National Legislation

Based on North Korea broadening its cyber threats and aggressions, South Korea has responded accordingly. In addition to unilateral sanctions against North Korean individuals and entities that raise funds through cyber activities for North Korea's nuclear and missile programs,[159] South Korea has released a revision of its National Cybersecurity Strategy from 2019. While the original 2019 version took a more defensive approach, South Korea's new 2024 framework tends towards a more offensive perspective, outlining five 'strategic tasks.' Compared to the 2019 framework, this updated version takes a more explicit approach naming the North Korean state as their 'main threat', as

[159] Shreyas Reddy, "South Korea issues first-ever cyber sanctions against North Korea", *NK News*, February 2023. https://www.nknews.org/2023/02/south-korea-issues-first-ever-cyber-sanctions-against-north-korea/.

the first strategy calls for "strengthening offensive cyber defense activities". The second strategy hopes to "establish a global cyber cooperation framework" to extend cooperation with other nations to strengthen cybersecurity through multilateral cybercrime agreements and active participation in global discussions surrounding cyber threats.

Furthermore, the third strategy calls for "enhancing cyber resilience of critical infrastructure", looking to strengthen the security of critical information systems to allow for the government to respond and defend itself against cyberattacks efficiently. This strategy further calls for the implementation of the 'Zero Trust' security strategy in order to protect public data on digital government platforms. Next, the fourth strategy aims to "secure a competitive edge in critical and emerging technologies" by encouraging innovation through the collaboration of industry, academia, and research institutions. The fourth strategy also calls for developing a cyber risk management system that promotes collaboration between private technology companies and public research institutions to ensure successful execution. Finally, the fifth strategy hopes to "strengthen the operational foundation" to ensure that cybersecurity tasks are carried out across all sectors and institutions. This strategy calls for more cybersecurity personnel and professionals in both private and public sectors, as well as increasing public awareness and engagement. Through the National Cybersecurity Strategy, it is made clear that South Korea prioritizes combating cybersecurity threats against North Korea through offensive and defensive cyber risk programs, a heightened approach since 2019.

South Korea has also developed bilateral strategies, especially with the United States, its strongest partner in cybersecurity, with close collaboration between President Yoon and President Biden. Together, their administrations launched the Strategic Cybersecurity Cooperation Framework in 2023 on the 70th anniversary of the United States and South Korea alliance. The framework emphasizes mutual agreement and growth in cooperative cybersecurity measures. President Yoon's more offensive approach outlined in the most recent National Cybersecurity Strategy aligns with the US' strategy on preemptive action, creating

grounds for a future of continued close collaboration between the two countries. However, as mentioned by malware Researcher Sebastian Garcia, the US and South Korea could smooth potential bumps in direct institution-to-institution collaboration and capacity-building by having clearer operationalization of cybersecurity governance.[160]

To effectively counter emerging cybersecurity threats, particularly those posed by North Korea, states can draw valuable lessons from South Korea's approach. South Korea's updated National Cybersecurity Strategy provides a model that other nations could adapt to their own domestic frameworks. A key aspect of this strategy is the periodic revision of cybersecurity policies to reflect evolving threats and technological advancements. Establishing mechanisms for continuous threat analysis and consulting with cybersecurity experts can further strengthen national resilience. Additionally, South Korea's implementation of the Zero Trust model offers a valuable blueprint for enhancing the protection of critical infrastructure through advanced security measures.

Beyond strategic frameworks, building a highly skilled cybersecurity workforce is crucial for ensuring long-term resilience. Investing in education and training programs can help cultivate the expertise needed to address sophisticated cyber threats. Furthermore, states may consider integrating offensive capabilities into their cybersecurity strategies, not only to respond effectively to cyberattacks but also to serve as a deterrent. Transitioning from a solely defensive approach to a more proactive posture, as demonstrated by South Korea, can significantly enhance a nation's ability to counter malicious cyber operations.[161]

---

[160] Sebastian Garcia, "Facing the North Korean Cyber Threat: United States-South Korea Coordination in Cyberspace", *Wilson Center*, August 2024. https://www.wilsoncenter.org/blog-post/facing-north-korean-cyber-threat-united-states-south-korea-coordination-cyberspace.

[161] Natasha Wood, "South Korea's 2024 Cyber Strategy: A Primer", *CSIS*, August 2024. https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer#:~:text=Ultimately%2C%20the%20strategic%20tasks%20outlined,evolving%20cyber%20threat%20environment%20ROK.

4.3.2. Implementing a Multi-Stakeholder Model

The internet, by fostering global connectivity beyond geographic borders, has both empowered individuals and redistributed power among governments and non-state actors. In contrast, some governments, such as China, advocate for "Internet sovereignty," asserting control over internet infrastructure, data, and content within their borders. To advance human rights in the digital era and combat cybercrime, it is essential to strengthen the existing multi-stakeholder model of internet governance rather than reverting to a state-centric "Westphalian" framework, where sovereign states exclusively control and enforce authority within their recognized territories.[162] As for the multi-stakeholder model, the focus is on the collaboration of various actors, such as governments but also the private sector, civil society, technical experts, and academia. According to a 2015 UN General Assembly Report, cyber security challenges "would benefit from the appropriate participation"[163] of these actors. This collaboration would ensure accountability, transparency, and diverse participation, allowing for more inclusive and representative decision-making[164] on internet governance matters. This also guarantees that the internet remains open, interoperable, and aligned with Human Rights.

Greater stakeholder involvement in public policies has long been advocated across multiple domains. However, the multistakeholder approach to national cybersecurity strategies remains underdeveloped.[165] In 2013, the Seoul Framework, introduced as part of the Global Conference on CyberSpace (GCCS), called for "a trusted, secure and sustainable environment in partnership with multiple stakeholders,

---

[162] Richard Coggins, "Westphalian state system", *Oxford Reference* https://www.oxfordreference.com/display/10.1093/oi/authority.20110803121924198

[163] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (2015).

[164] NRS Team, "The role of multi-stakeholder model in Internet Governance", *Number Resource Society*, July 2024.

[165] Global Partners Digital, "Multistakeholder Approaches to National Cybersecurity Strategy Development" , June 2018, https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf.

including international organizations and the private sector".[166]

Cooperation with the Private Sector

In order to tackle North Korea's cyber crimes and mitigate risks, cooperation with the private sector using public-private partnerships is essential.[167] This includes the creation of a public-private data-sharing platform aimed at unifying the national response to cyberattacks.[168] Key stakeholders include technology firms, cybersecurity companies, and business associations, all of which possess the technical expertise necessary to counter evolving threats. Given that the majority of the technical expertise in cybersecurity resides within the private sector and technical community, these actors, which own and operate much of the internet infrastructure, play a crucial role in developing national cybersecurity strategies that can adapt to evolving threats.[169] Their role as decision-makers at all layers of cyberspace governance also provides states with access to advanced technology and services necessary to combat cyber threats effectively.[170] By operationalizing information sharing and promoting trust, partnerships between governments and private-sector representatives not only enhance resilience against cyber threats but also help safeguard Human Rights. Adopting similar collaborative models globally could strengthen the collective defense against state-sponsored cyber threats, including those from North

[166] GCCS, *Seoul Framework for and Commitment to Open and Secure Cyberspace*, 2013

[167] "National Cybersecurity Strategy," *Office of the President of the Republic of Korea*, Office of National Security in the Office of the President, Republic of Korea, 2024, https://www.president.go.kr/newsroom/press/gdXzwtKB.

[168] Natasha Wood, "South Korea's 2024 Cyber Strategy: A Primer", CSIS, August 2, 2024, https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer#:~:text=Ultimately%2C%20the%20strategic%20tasks%20outlined,evolving%20cyber%20threat%20environment%20ROK.

[169] Eric Rosenbach, Shu Min Chong, "Governing Cyberspace: State Control vs. The Multistakeholder Model", *Belfer Center for Science and International Affairs*, Harvard Kennedy School, August 2019 https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model.

[170] Ibid.

Korea.[171]

Cooperation with Civil Society

In contrast to a state-centric and militarized approach to digital security, experts advocate for a human-centered cybersecurity policy and a whole-of-society approach. This model recognizes citizens and civil society as active participants in cybersecurity policymaking, fostering a more inclusive and comprehensive response to cyber threats and cybercrime.[172] Integrating diverse stakeholders, enhances resilience and ensures that cybersecurity measures align with fundamental rights and democratic values. This co-production must involve the design and implementation of cybersecurity strategies and policies, notably within the framework of the United Nations, in order to protect Human Rights. Despite the mobilisation of numerous civil society organisations, along with tech firms and cybersecurity experts, pushing for changes in the draft to the 2024 UN Convention against Cybercrime, concerns have been expressed as states could use it to justify Human Rights violations or extraterritorial surveillance.[173] Therefore, the international community must remain cautious and ensure that the fight against cybercrime does not drift in a harmful direction.

Besides, effective cooperation should also include the active participation of civil society, such as raising public awareness on cybersecurity risks or setting up cybercrime and online violence smart support networks.[174] The non-governmental organisation Access Now offers emergency assistance in the event of cyberattacks, especially supporting civil society organisations, activists, and journalists through its "Digital Security Helpline".

---

[171] Eugenia Lostri, James Andrew Lewis, Georgia Wood, "A Shared Responsibility: Public-Private Cooperation for Cybersecurity", *CSIS*, March 2022, https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

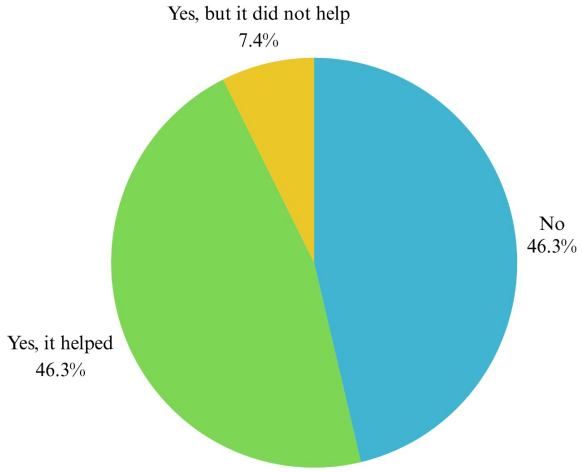
[172] Julia-Silvana Hofstetter, "The future of cybersecurity policy lies in civil society", ICT4Peace Foundation, 2024.

[173] Jonathan Greig, "UN General Assembly approves cybercrime treaty despite industry backlash", *The Record*, December 27th 2024.

[174] Ibid.

This type of initiative needs to be further developed to support victims, especially in the North Korean context, in light of the frequent and aggressive nature of their cyberattacks. Indeed, many victims have felt let down by their government when seeking help after being hacked. They have reported a lack of adequate support mechanisms, which exacerbates the situation for those advocating for Human Rights. One interviewee expressed frustration, stating that "*there is nothing that the government gave us*", highlighting the perceived absence of assistance for activists despite the significant risks they face in their advocacy roles.[175] Despite educational workshops and advisory services for North Korean defectors and members of Human Rights NGOs, interviewees reported that these initiatives were infrequent and insufficiently detailed to provide meaningful help. According to them, cybersecurity education is a fundamental step to combat North Korean threats and cyberattacks effectively.

Fig. 11: PRESENCE OF GOVERNMENT SUPPORT



Additionally, they emphasized the need for further assistance and personalized support in cases of actual hacking incidents to ensure that viruses are immediately contained and prevented from spreading to a broader community. Overall, the issue takes root at the top, with

[175] Jeong-Yoon Heo, interview by Nam Bada, PSCORE, 15th December 2024.

government officials and employees of the Ministry of Unification lacking proper cybersecurity training, leaving them vulnerable to hacking attempts and making them victims of North Korean hacking. Due to this lack of knowledge, they often simply delete suspicious files. While government officials might be expected to receive adequate training on cyber threats, Human Rights Organization leaders, who are often more exposed, tend to be better informed on this issue. It is essential for government officials to receive sufficient training to protect both themselves and the people they work with. Furthermore, our survey revealed that while some people did receive help from the government, 7.4% of the participants said it was not helpful and, 46% of people did not receive any assistance at all. The leader of a Human Rights organisation corroborates this, as he explained that the only help he receives comes in the form of reaching out to personal contacts like "friends in the community who are tech-savvy" or friends who have advanced knowledge on hacking and North Korean cyber strategies. He noted, however, that he had never received any official assistance or a reliable contact to whom he could send suspicious emails to verify whether they contained North Korean malware.

5. Conclusion

North Korea's cyberattack strategies pose an increasing threat, encompassing espionage, cyber terrorism, and financial warfare. These operations target governments, private organizations, Human Rights groups, and individuals, including defectors and activists. North Korea's cyber capabilities rely on a rigid training program for IT workers and hackers, selecting individuals with advanced mathematics and science skills for domestic and international training at specialized centers. The Reconnaissance General Bureau (RGB) leads North Korea's cyber operations, employing advanced techniques like identity laundering and foreign team-based attacks to expand its global cybercrime reach. The RGB's third and fifth departments direct groups like APT38 and Kimsuky, which specialize in financial crimes, espionage, and propaganda. Beyond institutional damage, these operations violate Human Rights, targeting defectors and activists with privacy breaches and intimidation. Combating North Korea's cyber capabilities requires sustained attention to mitigate institutional and personal consequences.

North Korean cyberattacks violate Human Rights across three generations: civil and political liberties, economic and social rights, and collective rights. North Korea employs increasingly sophisticated hacking methods such as phishing emails, fake messages on social media, and malicious files. Cyberattacks, particularly those targeting individuals and NGO members, have been recorded as leading to psychological harm, including anxiety, PTSD, and paranoia. North Korean defectors are particularly vulnerable due to existing trauma and precarious social conditions. Victims report disrupted work, fear for safety, and compromised trust. Additionally, North Korean IT workers suffer from Human Rights violations, as they endure severe exploitation, including forced labor, harsh quotas, and limited personal freedom. They receive minimal pay, face constant surveillance, and suffer from sleep deprivation and mental health issues. This environment fosters isolation,

stress, and extreme pressure, with some workers reportedly resorting to suicide. North Korean cyberattacks inflict far-reaching damage, violating multiple Human Rights and creating an atmosphere of fear and instability. Addressing these violations will require global cooperation, robust cybersecurity policies, and support systems for victims and affected communities.

North Korea's cyber operations, which violate international treaties like the ICCPR, pose significant threats to global stability and Human Rights. International responses include U.S. sanctions and EU regulations targeting North Korea's resources and cyber activities. Broader frameworks, such as the Budapest Convention on Cybercrime (2001), NATO's Tallinn Manual (2013), and the UN Convention against Cybercrime (2024), provide legal guidance for addressing cybercrime but have yet to be ratified by North Korea. Domestically, South Korea's 2024 National Cybersecurity Strategy adopts an offensive stance against North Korea. Its measures focus on strengthening defense systems, enhancing global cooperation, protecting critical infrastructure, and fostering cybersecurity innovation. However, victims of cyberattacks often report insufficient support, with limited government training and resources for activists and officials, leaving many vulnerable to threats.

North Korea's cyber operations have emerged as a global security challenge, combining sophisticated technology and human exploitation to disrupt international systems and violate fundamental human rights. While international institutions and the global community have taken steps to address these threats, there is an urgent need for coordinated action to prevent North Korea from spreading insecurity in cyberspace.

The alarming findings highlighted in recent reports underscore North Korea's persistent human rights violations through its aggressive and malicious cyber activities, both domestically and globally. These operations not only threaten the security of nations and individuals worldwide but also directly undermine the fundamental freedoms of the North Korean people.

As an organization dedicated to advocating for North Korean defectors and global human rights, PSCORE emphasizes the critical need to document these violations and calls for decisive international measures. Strengthening cyber resilience, holding perpetrators accountable, and safeguarding victims—both in North Korea and around the world—are essential steps toward ensuring global peace and security in the digital age.

6. Recommendations From PSCORE

6.1. Recommendations to the International Community

To put an end to these violations, PSCORE calls on the global community to take decisive action against these cybercrimes and to uphold the Human Rights of the North Korean population, as well as all victims of North Korea's malicious cyber activities worldwide.

Therefore, PSCORE:

- Urges the global community to hold North Korea accountable for its unlawful cyber activities.

- Appeals to international actors to amend or update existing international legal documents on Human Rights that reflect modern issues. While current documents include some provisions on victim protection, additional measures must be adopted to ensure it becomes a core principle of international efforts to combat cybercrime.

- Requests the international community to impose stronger sanctions on North Korea and to hold the regime accountable, particularly relating to cybercrime.

- Urges the international community to foster stronger multilateral collaboration with both the private sector and civil society when developing cybersecurity strategies.

- Encourages NGOs to continue raising awareness on cyber threats by actively informing governments, corporations, and individuals about the risks posed by cyber activities and providing resources

for protection.

- Strongly requests governments and policy-makers to consider investing in public awareness campaigns like educational programs and workshops, which can equip individuals with tools to navigate the threat of cyberattacks.

- Appeals to the United Nations to ensure that the Convention on Cybercrime will not be used ill-intendedly by states to justify abusive surveillance of individuals, especially activists and journalists, in light of the worries expressed by civil society organizations.

- Asks the international community to provide practical support for the affected individuals, including mental health professionals for counseling or therapy, to manage the emotional burden and health impacts of the cyber threats and attacks.

6.2. Recommendations to North Korea

In light of the evidence presented in this report, PSCORE urges North Korea to immediately cease its involvement in cyber operations that violate international law and infringe upon Human Rights. These actions are necessary to ensure the well-being of North Korean citizens and other cybercrime victims. North Korea must uphold its responsibilities as a member of the international community and act accordingly.

Therefore, PSCORE:

- Encourages North Korea to uphold its international commitments through the covenants it has ratified, such as the ICCPR and the ICESCR.

- Urges North Korea to cease state-sponsored cybercrime and dismantle cyber units involved in illicit activities such as financial theft, ransomware attacks, espionage, and cyber-enabled Human Rights violations.

- Calls upon North Korea to put an end to grave Human Rights violations by ensuring ethical and lawful employment conditions for its IT workforce, including fair wages, safe working environments, and freedom from coercion.

- Asks North Korea to adopt international Human Rights standards in cyberspace as a crucial step toward integration into the global community.

- Recommends North Korea to cooperate with the UN to combat cybercrime and establish transparency regarding its cyber operations. Constructive engagement with the international community can facilitate pathways toward responsible cyber governance.

- Urges North Korea to adopt a system that allows its citizens to access global online data. This may be a difficult feat owing to its extensive censorship measures, but it should be done to respect the state's compliance with international statutes, which they, themselves, are a part of. The right to access information is fundamental to human dignity and development.

Bibliography

Aboujaoude, Elias. “Protecting Privacy to Protect Mental Health: The New Ethical Imperative.” *Journal of Medical Ethics* 45, no. 9 (2019): 604–606. https://jme.bmj.com/content/45/9/604.full.

Barnhart Michael, Cantos Michelle, Johnson Jeffery, Fox Elias, Freas Gary, and Scott Dan. “Not So Lazarus: Mapping North Korea Cyber Threat Groups to Government Organizations.” *Google Blog*, March 23, 2022. https://cloud.google.com/blog/topics/threat-intelligence/mapping-North Korea-groups-to-government/?hl=en.

Bartlett, Jason. *Exposing the Financial Footprints of North Korea’s Hackers.* Washington, DC: Center for a New American Security, 2020.

Brooks, Tyson. “The Professionalization of the Hacker Industry.” *International Journal of Computer Science & Information Technology (IJCSIT)* 14, no. 3 (2022): 87–95. https://doi.org/10.5121/ijcsit.2022.14307.

Budimir Sanja, Fontaine Johnny, Huijts Nicole, Haans Antal, Loukas George, and Roesch Etienne. “Emotional Reactions to Cybersecurity Breach Situations: Scenario-Based Survey Study.” *Journal of Medical Internet Research* 23, no. 5 (2021): e24879. https://doi.org/10.2196/24879.

Burkadze, Khatuna. “International Legal Definition of a Cyberattack”. *Journal Iustitia*, 2022.

Center of Excellence Defence Against Terror. *Responses to Cyber Terrorism (NATO Science for Peace and Security).*Texas: IOS Press, 2008.

Chun, Chaesung. *Knowledge State in the Era of Generative AI and the Future of the Korean Peninsula.* EAI Issue Briefing. Seoul: East Asia Institute, 2024. Accessed January 15, 2025. https://www.eai.or.kr.

CISA. “North Korea Cyber Threat Overview and Advisories.” *Cybersecurity and Infrastructure Security Agency (CISA)*. Accessed September 23, 2024. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea.

Coggins, Richard. “Westphalian State System.” *Oxford Reference.* Accessed February 3, 2025. https://www.oxfordreference.com/display/10.1093/oi/authority.20110803121924198.

Cohen, Gary. “Throwback Attack: Korea Hydro and Nuclear Power Highlights the Vulnerability of Critical Systems.” *Industrial Cybersecurity Pulse*, March 16, 2023.

Collins English Dictionary. s.v. “PROGRAMMER.” Accessed 2025. https://www.collinsdictionary.com/dictionary/english/programmer.

Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms.* Rome, November 4, 1950. https://www.echr.coe.int/Documents/Convention_eng.pdf.

Council of Europe. *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols*. Accessed February 3, 2025. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Council Regulation (EU) 2017/1509 of 30 August 2017 Concerning Restrictive Measures Against the Democratic People’s Republic of Korea and Repealing Regulation (EC) No 329/2007, 224 OJ L § (2017). http://data.europa.eu/eli/reg/2017/1509/oj/eng.

Daily NK. “Anti-Reactionary Thought Law: Bans on External Culture in North Korea (English Translation).” *Daily NK*, March 2023.

Daily NK Reporter. Interview by Nam Bada, Elma Duval, Yunah Jang, PSCORE, October 23, 2024.

Fischer, Eric A. *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options.* Congressional Research Service Report RL32777, February 22, 2005. https://sgp.fas.org/crs/natsec/RL32777.pdf.

Fischer, Eric A. “Cybersecurity Issues and Challenges: In Brief.” *Congressional Research Service*, August 12, 2016.

Garcia, Sebastian. “Facing the North Korean Cyber Threat: United States-South Korea Coordination in Cyberspace”. *Wilson Center*. August 2024. https://www.wilsoncenter.org/blog-post/facing-north-korean-cyber-threat-united-states-south-korea-coordination-cyberspace.

GCCS. *Seoul Framework for and Commitment to Open and Secure Cyberspace*, 2013.

Genians Security Center. *Kimsuky APT* 그룹의 *Storm* 작전과 *BabyShark Family* 연관 분석. October 30, 2023.

Genians Security Center. *K* 메신저로 유포된 *'APT37'* 그룹의 악성 *HWP* 사례 분석. February 7, 2025.
https://www.genians.co.kr/blog/threat_intelligence/k-messenger.

Global Partners Digital. *Multistakeholder Approaches to National Cybersecurity Strategy Development*, June 2018.
https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf.

Gregory Jules, de Lepinau Jean, de Buyer Ariane, Delanoy Nicolas, Mir Olivier, and Gaillard Raphaël. "The Impact of the Paris Terrorist Attacks on the Mental Health of Resident Physicians." *BMC Psychiatry* 19, no. 1 (2019).
https://doi.org/10.1186/s12888-019-2058-y.

Greig, Jonathan. "UN General Assembly Approves Cybercrime Treaty Despite Industry Backlash." *The Record*, December 27, 2024.

Guterres, António. "Secretary-General's Remarks to the Security Council's High-Level Debate on 'Maintenance of International Peace and Security: Addressing Evolving Threats in Cyberspace.'" United Nations, June 20, 2024.
https://www.un.org/sg/en/content/sg/speeches/2024-06-20/secretary-generals-remarks-the-security-council's-high-level-debate-"maintenance-of-international-peace-and-security-addressing-evolving-threats-cyberspace".

Guynn, Jessica. "Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes." *USA Today*, February 24, 2020.

Haggard Stephan, and Jon R. Lindsay. *North Korea and the Sony Hack: Exporting Instability Through Cyberspace.*Honolulu: East-West Center, 2015.

Heo, Jeong-Yoon. Interview by Nam Bada, PSCORE, December 15, 2024.

Hofstetter, Julia-Silvana. "The Future of Cybersecurity Policy Lies in Civil Society." *ICT4Peace Foundation*, 2024.

Hollifield Michael, Hewage Chandanie, Gunawardena Charlotte, Kodituwakky Piyadasa, Bopagoda Kalum, and Weerarathnege Krishantha. "Symptoms and Coping in Sri Lanka 20–21 Months After the 2004 Tsunami." *The British Journal of Psychiatry* 192, no. 1 (2008): 39–44. https://doi.org/10.1192/bjp.bp.107.038422.

Human Rights Watch. “Upcoming Cybercrime Treaty Will Be Nothing but Trouble.” August 7, 2024. https://www.hrw.org/news/2024/08/07/upcoming-cybercrime-treaty-will-be-nothing-trouble.

Iancu Niculae, Fortuna Andrei, Barna Cristian, and Mihaela Teodor. *Countering Hybrid Threats: Lessons Learned from Ukraine.* Amsterdam: IOS Press, 2016.

International Business Machines Corporation, “Types of Cyberthreat”, March 2024. https://www.ibm.com/think/topics/cyberthreats-types.

International Telecommunication Union, “Recommendation X.1205”, 2008.

IT Workers. Kim, Ju-Won and Bom-Seok Kim. Interview by Nam Bada, PSCORE, October 6, 2024.

Jensen, Eric Talbot. “The Tallinn Manual 2.0: Highlights and Insights.” *Georgetown Journal of International Law* 48 (n.d.). https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

Jung, Yuna. Interview by Nam Bada, Elma Duval, Yunah Jang, PSCORE, November 13, 2024.

Joint Cybersecurity Advisory. “North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media.” 2023.

Kang, Shin-Sam. Interview by Nam Bada, Elma Duval, Yunah Jang, PSCORE, October 24, 2024.

Kilovaty, Ido. “Psychological Data Breach Harms.” *SSRN Electronic Journal*, 2021. http://dx.doi.org/10.2139/ssrn.3785734.

Kim, Chong Woo, and Carolina Polito. “The Evolution of North Korean Cyber Threats.” *The Asan Institute for Policy Studies*, August 2019. https://www.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/.

Kim, Dongwook, Seulgi Lee, Taewoo Lee, and JaeKwang Lee. *TTPs#9:* 개인의 일상을 감시하는 공격전략 분석. Korea, 2021.

Kim, Hyun-Seong. Interview by Nam Bada, Eunhye Kim, and Clara Omer, PSCORE, September 2, 2022.

Kim, Ji-Min. “Lecture on North Korean IT Workforce.” 2024.

Kim, Yoo-Hyang. “North Korea’s Cyberpath.” *Asian Perspective* 28, no. 3 (2004): 191–209. https://doi.org/10.1353/apr.2004.0018.

Klingner, Bruce. “North Korean Cyberattacks: A Dangerous and Evolving Threat.” *The Heritage Foundation*, September 2, 2021.

Kong Ji-Young, Lim Jong-In, and Kim Kyoung-Gon. “The All-Purpose Sword: North Korea’s Cyber Operations and Strategies.” 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2019: 1–20. https://doi.org/10.23919/CYCON.2019.8756954.

Kulka, Richard. “Trauma and the Vietnam War Generation: Report of Findings from the National Vietnam Veterans Readjustment Study”.*Choice Reviews Online* 27, no. 11 (1990): 27–6366. https://doi.org/10.4324/9781315803753.

Lankov, Andrei. “On the Great Leader’s Secret Service: North Korea’s Intelligence Agencies.” *NK News*, May 1, 2017. https://www.nknews.org/2017/05/on-the-great-leaders-secret-service-north-koreas-intelligence-agencies/.

La Rue, Frank. “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.” *United Nations Document* A/HRC/17/27, May 16, 2011.

Lostri, Eugenia, James Andrew Lewis, and Georgia Wood. *A Shared Responsibility: Public-Private Cooperation for Cybersecurity*. CSIS, March 2022. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

Louie, Ryan K., MD, PhD. “Quick Look: #Psybersecurity: Mental Health Impact of Cyberattacks.” YouTube, February 17, 2020. https://youtu.be/JxGar7_2KLA.

Martin, David. “Tracing the Lineage of Dark Seoul.” *SANS Institute*, 2021. https://www.giac.org/paper/gsec/31524/tracing-lineage-darkseoul/126346.

Mishra, Vibhu. “UN General Assembly Adopts Milestone Cybercrime Treaty.” *UN News*, December 2024. https://news.un.org/en/story/2024/12/1158521.

Na, Jeong-Seok. Interview by Nam Bada, PSCORE, December 15, 2024.

Nanto, Dick K. *North Korea: Chronology of Provocations, 1950–2003.* Washington, DC: Congressional Research Service, 2003.

"N. Korea Boosting Cyber Warfare Capabilities." *The Chosun Daily*, November 5, 2013. https://www.chosun.com/english/north-korea-en/2013/11/05/nwrskrxuwgkjnc42nmtelcniny/.

"North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector." *Cybersecurity and Infrastructure Security Agency (CISA)*, July 6, 2022. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea.

Novo, Lisandra. "The UN Finally Advances a Convention on Cybercrime… and No One Is Happy About It." *Atlantic Council*, August 2024. https://www.atlanticcouncil.org/blogs/new-atlanticist/the-un-finally-adopts-a-convention-on-cybercrime-and-no-one-is-happy/.

NRS Team. "The Role of Multi-Stakeholder Model in Internet Governance." *Number Resource Society*, July 2024.

Office of the President of the Republic of Korea, Office of National Security. *National Cybersecurity Strategy*. Republic of Korea, 2024. https://www.president.go.kr/newsroom/press/gdXzwtKB.

Padmavathi G., and Uma M. "A Survey on Various Cyberattacks and Their Classification". *International Journal of Network Security*, *15*(5), 390-396 (2013).

Palassis Alexia, Speelman Craig P., and Pooley Julie A. "An Exploration of the Psychological Impact of Hacking Victimization." *SAGE Open* 11, no. 4 (2021): 215824402110615. https://doi.org/10.1177/21582440211061556.

Park, Seong-Min. Interview by Nam Bada, PSCORE, December 17, 2024.

Perkins, Ria C. "The Application of Forensic Linguistics in Cybercrime Investigations." *Policing: A Journal of Policy and Practice* 15, no. 1 (2021): 68–78.

Prioux Clémentine, Marillier Maude, Vuillermoz Cécile, Vandentorren Stéphanie, Rabbit Gabrielle, Petitclerc Matthieu, Baubet Thierry, Stene Lise Eilin, Pirard Philippe, and Motreff Yvon. "PTSD and Partial PTSD Among First Responders One and Five Years After the Paris Terror Attacks in November 2015." *International Journal of*

Environmental Research and Public Health 20, no. 5 (2023): 4160. https://doi.org/10.3390/ijerph20054160.

Ramkumar, Balu. *Bangladesh Bank Cyber Heist: Incident Analysis.* Georgia Institute of Technology, 2022.

Reddy, Shreyas. "South Korea Issues First-Ever Cyber Sanctions Against North Korea." *NK News*, February 2023. https://www.nknews.org/2023/02/south-korea-issues-first-ever-cyber-sanctions-against-north-korea/.

Rosenbach, Eric, and Shu Min-Chong. *Governing Cyberspace: State Control vs. the Multistakeholder Model*. Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2019. https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model.

Sa, Hye-Jun. Interview by Nam Bada, PSCORE, October 24, 2024.

Schmitt, Michael N. "International Human Rights Law", *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*", Cambridge University Press, 2017. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/international-human-rights-law/B5CD88C7C704F5D1CE10294578B5BC9A.

Second Periodic Report of the Democratic People's Republic of Korea on Its Implementation of the International Covenant on Civil and Political Rights. U.N. Human Rights Committee, U.N. Doc. CCPR/C/PRK/2000/2 (2000). https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FPRK%2F2000%2F2&Lang=en.

Singh, Rakesh Kumar. "Right to Peace as a Human Right." *Uttarakhand Judicial & Legal Review* 3, no. 2 : 40–47. https://ujala.uk.gov.in/files/vol_3_iss_2.pdf.

SIRIUS. "The Second Additional Protocol to the Budapest Convention on Cybercrime." *European Union Agency for Criminal Justice Cooperation*, January 23, 2024. https://www.eurojust.europa.eu/sites/default/files/assets/the-second-additional-protocol-to-the-budapest-convention-on-cybercrime-23-01-2024.pdf.

Sonkar, K. Santosh and Rai, V.K. *Why it is Time to Start Treating Cybersecurity Like a Human Rights Issue*. IJFMR Volume 5, Issue 3, May - June 2023.

DOI
10.36948/ijfmr.2023.v05i03.3071.https://www.ijfmr.com/research-paper.php?id=3071.

Song, Tae-Eun. “North Korea’s Illicit Cyber Activities: Latest Developments and ROK’s Responses.” *Institute of Foreign Affairs and National Security (IFANS), Korea National Diplomatic Academy*, 2024.

“#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund North Korea Malicious Cyber Activities.” *Cybersecurity and Infrastructure Security Agency (CISA)*, 2023.
https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_North Korea_ACTIVITIES.PDF.

Stent, Dylan. “The Great Cyber Game.” *New Zealand International Review* 43, no. 5 (2018): 6–9.

Suh, Elisabeth. *North Korea’s Cyber Capabilities and Strategy.* German Council on Foreign Relations, 2022.
https://dgap.org/en/research/publications/north-koreas-cyber-capabilities-and-strategy-0

Suriastini Ni Wayan, Sikoki Bondan, Sumantri Cecep, Umaroh Rodhiah, “Longitudinal Outcomes of Post-Traumatic Stress Disorder Among the Indian Ocean Tsunami Survivors in Indonesia.” *International Journal of Disaster Risk Reduction* 82 (2022): 103358. https://doi.org/10.1016/j.ijdrr.2022.103358.

The Danish Institute for Human Rights. *Human Rights and the 2030 Agenda for Sustainable Development: Leaving No One Behind.* 2018. Accessed January 15, 2025.
https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/sdg/hr_and_2030_agenda-web_2018.pdf.

“The Interview.” IMDb, December 24, 2014.
https://www.imdb.com/title/tt2788710/.

TRM Labs. *TRM 2025 Crypto Crime Report*. 2025.
https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/67a66929a076faf602d64b4c_TRM%202025%20Crypto%20Crime%20Report.pdf.

Turan, Tuba. “The 2016 UN General Assembly Declaration on the Right to Peace: A Step towards Sustainable Positive Peace within Societies?” *Human Rights Law Review* 23, no. 2 (March 10, 2023): ngad007. https://doi.org/10.1093/hrlr/ngad007.

UK Parliament, *Human Rights Act 1998*.
https://www.legislation.gov.uk/ukpga/1998/42/contents.

UNESCO and International Bioethics Committee. *Venice Statement on the Right to Enjoy the Benefits of Scientific Progress and its Applications*. Venice, 2009.

United Nations General Assembly. *United Nations Convention against Cybercrime*. A/RES/79/243. December 24, 2024.

United Nations General Assembly. *Universal Declaration of Human Rights.* 217 A (III), December 10, 1948.
https://www.un.org/en/about-us/universal-declaration-of-human-rights.

United Nations General Assembly. "Declaration on the Right of Peoples to Peace." A/RES/39/11. Adopted November 12, 1984. https://digitallibrary.un.org/record/74608.

United Nations General Assembly. "Declaration on the Right to Peace." A/RES/71/189. Adopted December 19, 2016.
https://digitallibrary.un.org/record/858594.

United Nations. "International Covenant on Civil and Political Rights." Adopted by the General Assembly of the United Nations on December 16, 1966. Reference C.N.467.1997.TREATIES-10 (Depositary Notification).
https://treaties.un.org/doc/publication/cn/1997/cn.467.1997-eng.pdf.

United Nations General Assembly. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174 (2015).

United Nations. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." A/HRC/48/31, 2021. Accessed January 10, 2025.
https://documents.un.org/doc/undoc/gen/g21/249/21/pdf/g2124921.pdf.

United Nations Security Council. *Report of the Panel of Experts Pursuant to Resolution 2397 (2017)*, March 2024. S/2024/215.
https://documents.un.org/doc/undoc/gen/n24/032/68/pdf/n2403268.pdf.

United Nations Security Council. *Resolution 2270 (2016), Adopted at the 7638th Meeting on March 2, 2016.* S/RES/2270 (2016).
https://main.un.org/securitycouncil/en/s/res/2270-%282016%29

United Nations Security Council. *Resolution 2397 (2017), Adopted at the 8151st Meeting on December 22, 2017*. S/RES/2397 (2017).
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/25/PDF/N1746025.pdf?OpenElement.

United Nations Security Council. *Resolutions and Decisions of the Security Council: 1 August 2009 – 31 July 2010*. In *Security Council Official Records*, ISSN 0257-1455. 2010. https://digitallibrary.un.org/record/697781/files/S_INF_65-EN.pdf.

United States. Office of the Federal Register. "Amendments to the Federal Acquisition Regulation: Fair Pay and Safe Workplaces." *Federal Register*, March 18, 2016. https://www.govinfo.gov/content/pkg/FR-2016-03-18/pdf/2016-06355.pdf.

U.S. Department of Justice. "Arizona Woman Pleads Guilty to Fraud Scheme that Illegally Generated $17 Million in Revenue for North Korea." *United States Attorney's Office, District of Columbia*, February 7, 2024. https://www.justice.gov/usao-dc/pr/arizona-woman-pleads-guilty-fraud-scheme-illegally-generated-17-million-revenue-north.

Vasak, Karel. "Three Generations of Human Rights." 1977.

Willett, Marcus. "Lessons of the SolarWinds Hack." *International Institute for Strategic Studies (IISS)*. Accessed January 15, 2025. https://www.iiss.org/blogs/survival-blog/2021/04/lessons-of-the-solarwinds-hack.

Wood, Natasha. "South Korea's 2024 Cyber Strategy: A Primer." *CSIS*, August 2, 2024. https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer#:~:text=Ultimately%2C%20the%20strategic%20tasks%20outlined,evolving%20cyber%20threat%20environment%20ROK.

World Conference on Human Rights. *United Nations, Vienna Declaration and Programme of Action.* Vienna, June 25, 1993. https://www.ohchr.org/en/instruments-mechanisms/instruments/vienna-declaration-and-programme-action

Appendix

This table compiles a significant number of cyber attacks carried out by North Korea. These attacks are among the most commonly covered by the media. While not exhaustive, it provides a clear understanding of the number of attacks conducted by North Korea.

Type of attack	Date	Attack description	Sector	Country
Cyberterrorism (sabotage and retaliation)	2012	South Korean conservative JoongAng Ilbo newspaper was attacked and article databases destroyed	Private sectors companies and banks	South Korea
Cyberterrorism (sabotage and retaliation)	2013	Dark Seoul Attack	Private sectors companies and banks	South Korea
Cyberterrorism (sabotage and retaliation)	2014	Sony Pictures Entertainment attack : DPRK state-sponsored cyber actors allegedly launched a cyber-attack on Sony Pictures Entertainment (SPE) in retaliation for the 2014 film “The Interview.” Confidential data has been stolen. Operation Blockbuster.	Private sectors companies and banks	US
Cyberterrorism (sabotage and retaliation)	2018	PyeongChang Winter Olympics : CyberAttack during the Opening ceremony of the PyeongChang 2018 Winter Olympics against the Organizing Committee and related companies.	Governmental agencies and international organizations	South Korea
Cyberterrorism (sabotage and retaliation)	2023	According to a new report, North Korean hackers breached computer systems at a Russian missile developer for five months in 2022. Analysts could not determine what information may have been taken or viewed.	Private sectors companies and banks	Russia
Financial warfare	2011	DPRK state-sponsored cyber actors attacked the Nonghyup computer network, a South Korean farm cooperative. The attacks destroyed 273 of the bank’s 587 servers.	Private sectors companies and banks	South Korea

Type of attack	Date	Attack description	Sector	Country
Financial warfare	2016	DPRK state-sponsored cyber actors have employed a fraudulent ATM cash withdrawal scheme known as “FASTCash” to steal tens of millions of dollars from ATMs in Asia and Africa.	Private sectors companies and banks	Cross countries
Financial warfare	2016	Bangladesh Bank Heist : DPRK state-sponsored cyber actors allegedly attempted to steal at least $1 billion from financial institutions across the world and allegedly stole $81 million from the Bangladesh Bank through unauthorized transactions on the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network.	Private sectors companies and banks	Bangladesh
Financial warfare	2017	YouBit, a South Korean crypto-currency exchange was attacked by Blunenoroff.	Private sectors companies and banks	South Korea
Financial warfare	2018	Digital Currency Exchange Hack : DPRK state-sponsored cyber actors hacked into a digital currency exchange and stole nearly $250 million worth of digital currency.	Private sectors companies and banks	Cross countries
Financial warfare	2018	South Korea’s cryptocurrency exchange institutions were under attack.	Private sectors companies and banks	South Korea
Information espionnage (phishing)	2005	Operation Flame : North Korea’s first DDoS attack.		South Korea
Information espionnage (phishing)	2005	Large-scale cyber attacks in South Korea which shut down 400 computers at the transition office of President Lee Myung-bak.	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2005	North Korean hackers targeted phishing attacks against the French, South African and Slovak ministries of foreign affairs, the UK’s Royal United Services Institute think tank and the US Congressional Research Service.	Governmental agencies and international organizations	France, South Africa, Slovakia, UK, US

Type of attack	Date	Attack description	Sector	Country
Information espionnage (phishing)	2005	North Korean hackers attacked Israel's Ministry of Defense. The government claimed the intrusion was thwarted, but cyber security firm ClearSky assessed that the hackers penetrated the ministry's computer system and stole a large amount of classified information in Israel and around the globe.	Governmental agencies and international organizations	Israel
Information espionnage (phishing)	2005	The Lazarus group defense targeted defense industry organizations in at least a dozen countries through spear-phishing emails with malware attachments or links. The malware gathered sensitive information and gained access to the organization's restricted networks, which contained mission-critical assets as well as computers with highly sensitive data with no Internet access.	Governmental agencies and international organizations	Cross countries
Information espionnage (phishing)	2005	The Kimsuky group engaged in spear phishing campaigns against 28 UN officials, including six members of the U.N Security Council. The emails contained malicious attachments or a link redirecting the victims to steal usernames and passwords.	Governmental agencies and international organizations	Cross countries
Information espionnage (phishing)	2009	The 4th of July's campaign : Series of coordinated cyber attacks that targeted South Korea and the United States. The sites of the South Korean Presidential Office, the Ministry of National Defense and the National Assembly were attacked by malicious software, while the White House, the Pentagon, and the Washington Post were targeted in the US.	Governmental agencies and international organizations	US, South Korea
Information espionnage (phishing)	2010	Cyberattacks jammed GPS signals at Seoul's Incheon airport.	Governmental agencies and international organizations	South Korea

Type of attack	Date	Attack description	Sector	Country
Information espionnage (phishing)	2011	The Ten Days of Rain attack targeted the South Korea's Presidential Office, the Foreign Ministry, the National Intelligence Service and some major South Korean financial institutions.	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2012	Large-scale cyber attacks jammed GPS navigation signals for at least 674 commercial air flights and 122 ships, as well as in-car navigation for a week.	Private sectors companies and banks	Cross countries
Information espionnage (phishing)	2013	the presidential office website, and several other official and media sites	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2013	The Kimsuky attack targeted South Korean think tanks including the Sejong Institute, the Korea Institute for Defense Analyses, the Ministry of Reunification and the Hyundai Merchant Marine shipping company.	Private sectors companies and banks	South Korea
Information espionnage (phishing)	2014	Hack of Seoul National University Hospital's computer network	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2014	Hacking of Korea Hydro & Nuclear Power by the cyber group Kimsuky	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2015	One espionage operation targeted three computers belonging to National Assembly members and eleven computers belonging to government aides occurred	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2015	Hacking of Seoul Metro : the computer server of one of Seoul City's subway operators has been allegedly hacked by North Korea.	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2016	Forty South Korean officials' smartphones were hacked, accessing their phone conversations, text messages and other sensitive information (expansion of North	Governmental agencies and international organizations	South Korea

Type of attack	Date	Attack description	Sector	Country
		Korea's operations to mobile technology).		
Information espionnage (phishing)	2016	Daewoo Shipbuilding and Marine Engineering Co., Ltd was targeted. Nearly 40 000 documents including 60 classified files were leaked during this attack.	Private sectors companies and banks	South Korea
Information espionnage (phishing)	2016	13 million pieces of customer information compromised from Interpark platform.	Private sectors companies and banks	South Korea
Information espionnage (phishing)	2017	Ransomware developed by DPRK state-sponsored cyber actors: WannaCry 2.0 has infected hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries.	Private sectors companies and banks	Cross countries
Information espionnage (phishing)	2018	Operation Kabar Cobra against the Ministry of Unification press corps.	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2018	Operation Kitty Phishing against the Ministry of Unification press corps.	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2018	Operation Red Salt against retired South Korean diplomatic, government and military officials.	Governmental agencies and international organizations	South Korea
Information espionnage (phishing)	2018	Operation Baby Shark by Kimsuky against U.S national security think tanks for information related to Northeast Asia's national security issues.	Private sectors companies and banks	US
Information espionnage (phishing)	2018	Operation Smoke Screen against U.S experts on North Korea	Governmental agencies and international organizations	US
Information espionnage (phishing)	2018	Operation Stealth Power against U.S and South Korean experts on North Korea.	Governmental agencies and international organizations	US, South Korea
Information espionnage (phishing)	2018	Operation Stolen Pencil against academic institutions	Private sectors companies and banks	Cross countries

Type of attack	Date	Attack description	Sector	Country
Information espionnage (phishing)	2019	North Korean hackers breached the nuclear power plant in Kudankulam, India. The Kimsuky group was seeking proprietary information on thorium-based reactors.The hackers also targeted several Indian nuclear physicists and scholars around the world who had published papers on thorium energy.	Private sectors companies and banks	India
Information espionnage (phishing)	2020	North Korean cyber groups impersonated journalists and news outlets to seed false stories with other reporters to spread disinformation. The hackers used real emails gleaned from experts on North Korea to gain access to the computers of other foreign policy experts, North Korean defectors and people interested in North Korean refugees. The attacks gained access to contact lists for surveillance and follow on cyber attacks	Private sectors companies and banks	Cross countries
Information espionnage (phishing)	2021	Hacking of the Korea Atomic Energy Research Institute and Korea Aerospace Industries by Kimsuky: the Institute was exposed for 12 days to the attacks.	Private sectors companies and banks	South Korea
Information espionnage (phishing)	2023	North Korean hackers targeted U.S.-based cybersecurity research firms in a phishing campaign. The campaign was meant to deliver malware for cyberespionage.	Private sectors companies and banks	US
Information espionnage (phishing)	2023	Hackers posed as journalists requesting interviews from targets, inviting them to use embedded links for scheduling and stealing their login credentials. The amount of information stolen and number of targets are unclear.	Private sectors companies and banks	Cross countries
Information espionnage (phishing)	2023	Attack of a Russian missile developer	Private sectors companies and banks	Russia
Information espionnage (phishing)	2023	Attempt to compromise a joint US-South Korean military exercise	Governmental agencies and	US, South Korea

Type of attack	Date	Attack description	Sector	Country
		on countering nuclear threats from North Korea.	international organizations	
Information espionnage (phishing)	2023	Suspected North Korean hackers attempted to compromise a joint U.S.-South Korean military exercise on countering nuclear threats from North Korea. Hackers launched several spear phishing email attacks at the exercise's war simulation center.	Governmental agencies and international organizations	US, South Korea
Information espionnage (phishing)	2023	North Korean hackers sent malware phishing emails to employees of South Korea's shipbuilding sector. South Korea's National Intelligence Service suggested that the attacks were intended to gather key naval intelligence that could help North Korea build larger ships.	Private sectors companies and banks	South Korea

"The very quality of seamless, instant connectivity that powers the enormous benefits of cyberspace can also leave people, institutions and entire countries deeply vulnerable. The perils of weaponizing digital technologies are growing by the year."

- UN Secretary-General António Guterres
20 June 2024

PSCORE (People for Successful COrean REunification)
6F, 29, Yonsei-ro, Seodaemun-gu, Seoul, Republic of Korea
pscore@pscore.org
+82-2-6497-5035
www.pscore.org