DIJEMSS:
Dinasti International Journal of Education Management and Social Science
E-ISSN: 2686-6331
P-ISSN: 2686-6358
https://dinastipub.org/DIJEMSS dinasti.info@gmail.com +62 811 7404 455
DINASTI PUBLISHER

DOI: https://doi.org/10.38035/dijemss.v6i4
https://creativecommons.org/licenses/by/4.0/

North Korean Threat Perceptions in Advanced Persistent Threat (APT) Operations in Global Cyberspace

Dessi Nursari[1]
[1]Universitas Indonesia, Depok, Indonesia, dessi.nursari@ui.ac.id

Corresponding Author: dessi.nursari@ui.ac.id[1]

Abstract: Technological developments have given rise to new threats in the form of cyber attacks, one of which is Advanced Persistent Threat (APT). APT is a campaign of attacks by groups that may or may not be linked to a state (state-sponsored). Based on reports from various sources related to cyber security, data shows that cyber attacks originating from North Korea have targeted several countries in various sectors such as government, finance, and private industry. Therefore, this study aims to understand the perceptions and motives behind cyber attacks, including those carried out by North Korean APT groups in targeting the global cyberspace. This study uses a qualitative-deductive method with the threat perception theory, as well as data from literature and documents from various scientific sources. The results show that North Korea's APT is an asymmetric strategy used to maintain regime stability and mitigate global economic pressures in a hidden way.

Keyword: Cyber Attack, Threat Perception, Advanced Persistent Threats, North Korea

INTRODUCTION

National security is one of the most important aspects of a country's national interests. In today's digital age, protecting sensitive data, critical infrastructure, and the stability and sovereignty of the state has become increasingly crucial. Rapid technological developments have not only brought progress to the lives of people around the world, but have also given rise to new challenges in the form of complex and ever-evolving cyber threats. National security is no longer limited to conventional military power, but has expanded to include asymmetric threats such as terrorism, information warfare, and cyber attacks involving both state and non-state actors (Blank, 2003).

Cyber attacks have become a serious global threat that knows no geographical boundaries. One of the most dangerous forms of cyber attack is the Advanced Persistent Threat (APT). APT is a carefully planned and organized attack against the digital assets of a targeted organization. These cyber attacks are structured, continuous, and covert, with the main objective of stealing sensitive information over a long period of time. APTs are usually carried out by groups with high resources, including those suspected of being state-sponsored, and utilize advanced techniques such as zero-day exploits, spear phishing, and covert network infiltration. These attacks are very difficult to detect and counter by conventional security systems due to their flexible, persistent nature and the use of constantly evolving tools and methods (Ahmad, 2019).

Based on data obtained from NSFOCUS's Fuying Laboratory, in 2024, APT attacks were detected that were characterized by strong political orientation, accelerated technological advancement, and intensified offensive operations. These international APT activities are still closely related to the political dynamics in various regions, with conflict areas such as East Asia, South Asia, Eastern Europe, and the Middle East experiencing high incidents of APT. APT attacks on public network devices in China also continued to increase. The Fuying Laboratory successfully detected various APT attacks originating from East Asia, Southeast Asia, and North America, with the main targets being high-value public network equipment, such as video surveillance systems, alarm systems, security systems, Haiwen systems, and large screen systems (NSFOCUS, 2025).

In 2024, the Fuying NSFOCUS Laboratory successfully detected 296 attacks originating from 67 APT groups. Of these, 47 attacks were first disclosed by the Fuying Laboratory through reports or blogs. 91% of these APT activities originated from 42 known APT groups, while the remaining 9% came from 25 emerging APT groups. Additionally, among the 42 known APT groups, Kimsuky ranked first in APT threat trends based on data from the Fuying NSFOCUS Laboratory.

Kimsuky is an APT group indicated to have ties to North Korea. Besides Kimsuky, North Korea is also frequently associated with other prominent APT groups, such as Lazarus (MITRE, 2025). Based on APT threat trend data from the Fuying Laboratory, it ranks sixth overall. This finding indicates that North Korea is one of the most active and consistent state actors in conducting cyber operations against strategic targets at the global level (NSFOCUS, 2025). Based on the 2023 Indonesian Cyber Security Landscape report published by the National Cyber and Cryptography Agency (BSSN), there were 4,001,905 instances of anomalous traffic in the form of APT activity. Of the five APT groups that most frequently attacked Indonesia, two of them were Lazarus and Kimsuky. The Lazarus group is known to have motives including data theft, financial gain, espionage, and sabotage that could threaten security and political stability. Meanwhile, Kimsuky primarily aims to conduct espionage against government, military, and research institutions. The involvement of the North Korean government in these APT activities adds a complex geopolitical dimension (BSSN, 2024).

On July 25, 2024, the US Federal Bureau of Investigation (FBI) issued a security alert regarding cyber espionage activities carried out by North Korea's 3rd Reconnaissance General Bureau (RGB) based in Pyongyang and Sinuiju. This unit has been identified as a state-sponsored cyber group, operating under various codenames such as Andariel, Onyx Sleet (formerly PLUTONIUM), DarkSeoul, Silent Chollima, and Stonefly/Clasiopa. This group specifically targets strategic sectors such as defense, aerospace, nuclear, and engineering to obtain sensitive technical information and classified intellectual property. The primary objective of these espionage activities is to support the development of North Korea's military and nuclear programs. The existence of this group poses a real threat to various industrial sectors worldwide, including in countries like Japan and India. Additionally, funding for their operations is obtained through ransomware attacks targeting healthcare institutions in the United States (National Cyber Security Centre, 2024).

Mandiant (2025) identified APT45 as a cyber group consistently supporting North Korea's strategic interests. Since 2009, APT45 has carried out various cyber operations in line with the changing geopolitical dynamics of North Korea. Initially focused on espionage activities targeting government agencies and the defense industry, the group later expanded its operational scope to the financial sector with economic gain as its motive, including involvement in ransomware development. Additionally, in 2019, APT45 was directly linked to targeting research facilities and nuclear power plants, including the Kudankulam Nuclear Power Plant in India, marking one of the rare public cases of North Korean cyber operations targeting critical infrastructure (Mandiant, 2025).

Furthermore, one of the threat actors identified in 2024 is Moonstone Sleet from North Korea. This group uses the FakePenny ransomware in a series of cyber espionage operations aimed at supporting the strategic interests of the North Korean government. This strategy indicates a new trend where espionage activities are not only focused on information theft but also leverage criminal techniques, such as ransomware, as a funding source and operational tool. This phenomenon reflects the increasingly complex and adaptive nature of hybrid threats in the global cybersecurity landscape (Verizon Business, 2025). A number of previous studies have proven North Korea's capabilities in conducting cyber attacks against other countries, such as South Korea and the United States, through various methods ranging from *Distributed Denial of Service* (DDoS) to highly sophisticated APTs (Boo, 2017; Hwang & Choi, 2021).

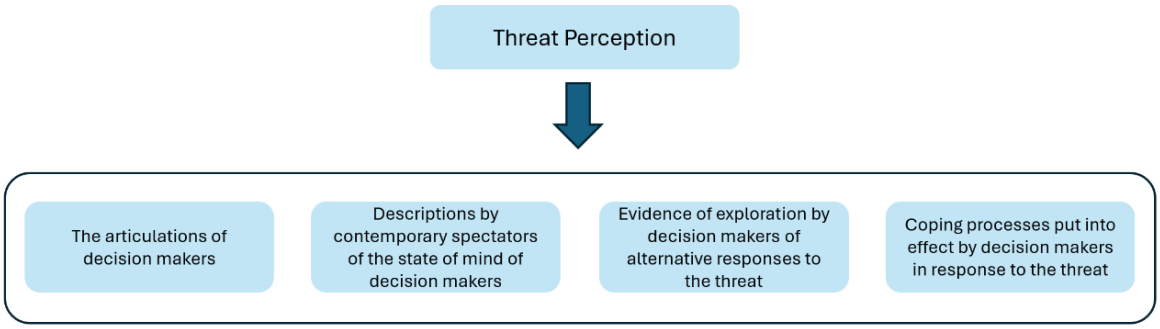
While many studies have examined North Korea's cyber capabilities, very few have examined threat perception as a key driver. This study attempts to fill that gap. Therefore, this study is important to fill the literature gap and contribute to understanding the dynamics of cyber threats from an international relations perspective. Based on this background, this study aims to analyze the threat perception behind APT attacks by North Korean groups in the global cyber space. This study is expected to provide theoretical contributions to the development of cyber security studies in the field of international relations and provide practical input for policymakers in formulating adaptive cyber security strategies to global threat dynamics.

METHOD

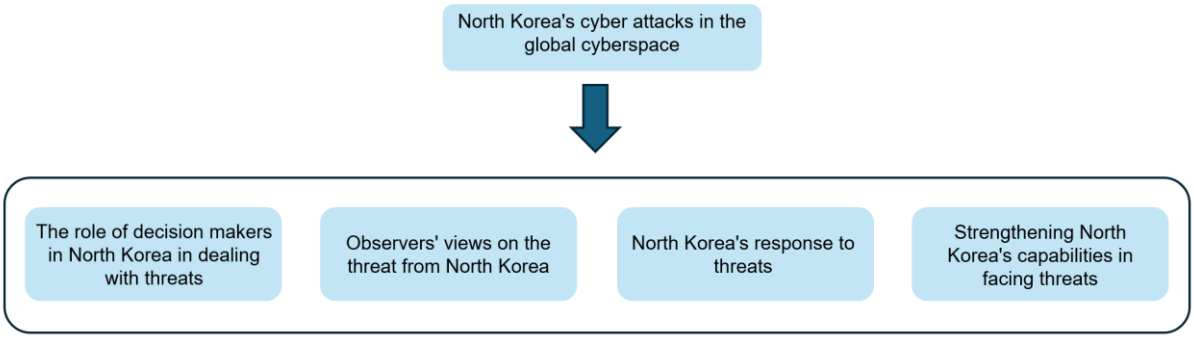
In contemporary international relations, geopolitical tensions resulting from rivalries between major powers create a sense of threat for countries. Conceptually, this condition is known as threat perception, which is the belief that the existence and national interests of a country are at risk due to the actions or presence of other actors. This perception is an intermediate variable that determines actions and reactions in international crises (Cohen, 1978). In international relations studies, threat perception has been approached from various angles. Jervis (1976) highlights the importance of decision-makers' perceptions of their opponents' military intentions and capabilities. The realist approach argues that power imbalances trigger threats and conflicts (Grieco, 1988; Waltz, 1979), while constructivists emphasize the role of shared identities in reducing threat perception (Wendt, 1999).

Cohen (1978) states that threat perception aims to anticipate danger, not impose sanctions. He identifies four main indicators: (1) decision-makers' articulation of threat signals, (2) contemporary observers' views on the psychological state of decision-makers, (3) exploration of alternative responses to threats, and (4) mitigation processes through resource enhancement or diplomatic measures. Furthermore, Cohen distinguishes two stages in threat perception: observation and assessment, which are influenced by psychological tendencies such as distrust and past experiences (Pruitt, 1965; Lazarus, 1966). Based on these concepts, the operationalization of the theory and research analysis model is presented in Figure 1 and Figure 2.The analytical framework used in this study is based on the Threat Perception theory, so the research method used is qualitative research with a deductive approach.

Neuman (2014) explains the orientation of the qualitative research approach. According to him, qualitative data collection is taken from soft data, such as words, sentences, images, and symbols, relying more on interpretive or critical principles of social science in cases and contexts as well as cultural meanings, often resulting in new hypotheses and explaining the details of mechanisms or cause-and-effect processes for a narrow range of cases, and more on logic that emerges from ongoing practice and follows a non-linear research path. Furthermore, the deductive approach represents that the research is conducted using an existing analytical framework and analyzing its relevance to the research topic (Bryman, 2012).



Source: Result has been processed (based on Cohen, 1978)
Figure 1. Operationalization of Threat Perception Theory



Source: Result has been processed (based on Cohen, 1978)
Figure 2. Threat Perception Theory Analysis Model

The analysis stage in this study begins with data collection from various relevant documents, including cybersecurity reports, academic publications, international news, and open online data sources containing information about cyberattacks, especially those related to North Korea. The data were selected based on their substantial relevance to threat perceptions at the state level. These documents were then systematically classified using the threat perception analysis model: 1) The role of decision makers in North Korea in dealing with threats; 2) Observer's views on the threat from North Korea; 3) North Korea's response to threats; and 4) Strengthening North Korea's capabilities in facing threats. Furthermore, the analysis was carried out thematically to identify how the threat narrative is constructed, and how the form of the state response reflects the process of forming threat perceptions.

RESULTS AND DISCUSSION

Threat Perception by Decision Makers

North Korea is a country known for its centralized, authoritarian, and personalistic dictatorship under the third generation of the Kim dynasty. North Korean policy places great emphasis on the political interests of the founding family of North Korea, Kim Il-sung, rather than the interests of North Korea as a whole. Security dilemmas and an obsession with succession have been the main causes of its provocative behavior. When Kim Il-sung and his family felt threatened, they took aggressive measures (Yongho Kim, 2013).

Kim Il-sung inherited a provocative policy influenced by his experience as a partisan fighting against Japan in the 1930s and 1940s. Guerrilla tactics such as ambushes and surprise attacks became a hallmark of North Korea's foreign policy. The Korean War influenced Kim Il-sung's perception of threats. Additionally, the Vietnam War in the late 1960s heightened Kim Il-sung's sense of threat, as he feared a potential U.S. attack on North Korea. Kim's statements at the time revealed his concern that the war in Vietnam could trigger similar actions against North Korea. Ronald Reagan's policy in the early 1980s to enhance trilateral security

cooperation with South Korea and Japan also posed a threat to North Korea, as it was perceived as a military alliance against North Korea (Yongho Kim, 2013).

Kim Il-sung and Kim Jong-il employed different strategies to maintain their political power. Kim Jong-il consolidated his power through internal power struggles, facing off against his stepmother, Kim Song-ae, and his uncle, Kim Yong-ju. Kim Jong-il utilized military power as his primary source of power, implementing a military-first policy (son'gun chongch'i). He argued that military power was more important than the economy for maintaining the survival of the state. This policy included efforts to build nuclear weapons to strengthen the military and his regime. After Kim Il-sung's death, Kim Jong-il successfully maintained power and strengthened his position through military policies and by maintaining the political stability of North Korea's founding family. North Korea's socialist system, based on the Juche ideology, was considered essential for maintaining control over the people and preserving the Kim family's power (Yongho Kim, 2013).

In the 1990s, Kim Jong-il began to recognize the importance of cyber capabilities, which gave North Korea sufficient time to recruit and train human resources and invest in institutions to develop and maintain the country's presence in cyberspace. North Korea's focus on Information and Communication Technology (ICT) is reflected in its national strategy, which encompasses national security and economic development (Pinkston, 2020). Byman and Lind (2010) also mention that Kim Jong-il's methodical use of authoritarian instruments shows that he was a skilled strategic player. The instruments used included restrictive social policies, manipulation of ideas and information, use of violence, co-optation, manipulation of foreign governments, and institutionalized coup prevention (Byman and Lind, 2010).

This statement is in line with Kim Jong-il's directive to the North Korean People's Army to develop cyber warfare capabilities after the Iraq War. He emphasized that “In the 20th century, war was about bullets and oil. However, in the 21st century, war will be [a form of] information warfare.” Therefore, “War is won or lost by the side that has greater access to the enemy's military technical information during peacetime” (Kim, 2022). Advances in ICT in North Korea are exploited by its authoritarian leaders as instruments of surveillance and repression to maintain power. With its continuously developing ICT infrastructure, various institutions such as the Department of Organization and Guidance of the Workers' Party of Korea, the Ministry of State Security, the Ministry of People's Security, the General Political Bureau, and the Military Security Bureau can communicate, store data, and maintain social control more efficiently. In this regard, the North Korean regime has an incentive to conceal its cyber capabilities and institutions (Pinkston, 2020).

Kim Jong-un shares the same threat perception as his father, Kim Jong-il, but with some important differences, namely that he was younger when he ascended to the throne and did not have much experience in the party and military. The threats perceived by Kim Jong-un are also more related to his political survival (Yungho Kim, 2013). Quoting The New York Post, Kim Jung-un once stated that “cyber warfare, along with nuclear weapons and missiles, is a ‘multi-purpose weapon’ that guarantees the military's ability to attack relentlessly” (Kim and Polito, 2019; Kim, 2022).

Based on the historical role of North Korean decision-makers, it can be concluded that the authoritarian, dynastic, and highly personalistic leadership characteristics of North Korea shape a pattern of response to external threats that tends to be aggressive, strategic, and focused on regime survival. Threats are not merely understood as risks to the state but rather as threats to the political stability of the Kim family. Therefore, when combined with the utilization of its cyber capabilities, North Korean leaders can leverage cyber power as an ideal tool and strategy to implement aggressive foreign policies without triggering open conflict, while simultaneously maintaining security and defense against external pressures.

Observer's Views on Threats

Cyber terrorism experts in South Korea agree that North Korea's conventional motivation is the accumulation of power and wealth, which is now driving the country to develop its activities in cyberspace. Technological developments are seen as a new opportunity for North Korea to expand its illegal activities, which have previously been part of the regime's strategy. The initial motive of gradually obtaining confidential information has shifted to a focus on financial gain. These experts state that the drive for economic gain is the main factor behind North Korea's cyber aggression (Hwang & Choi, 2021)

In April 2014, General Curtfis M. Scaparrotti, then-Commander of the United Nations Command and the Republic of Korea Combined Forces, stated that North Korea possesses advanced hacking capabilities in open-source intelligence collection, cyber espionage, and disruptive cyber attacks. A number of attacks on South Korea's banking sector in recent years have been linked to North Korean cyber activities. He emphasized that cyber warfare is a strategic asymmetric instrument relied upon by North Korea because it is difficult to trace and relatively inexpensive to operate (Avery, 2017).

In 2015, Professor Kim Heung-Kwang, who teaches computer science at Hamheung Computer Technology University in North Korea, told BBC News that he estimated "between 10% and 20% of the regime's military budget is spent on cyber operations" and that "attacking other countries is to demonstrate that North Korea has cyber warfare capabilities," which could ultimately lead to "military attacks, killing people, and destroying cities (Avery, 2017).

According to observers, North Korea's cyber activities indicate that the country is exploiting cyberspace as a strategic instrument to achieve two main objectives: power accumulation and wealth acquisition. The focus on information gathering has now been supplemented by a focus on economic gain. The use of cyber as a tool of asymmetric warfare allows North Korea to act aggressively without incurring high costs or the risk of detection, making it an efficient option for a regime with limited resources.

Statements from other observers further reinforce that North Korea is seriously developing its cyber capabilities as part of its national military strategy and allocating a portion of its military budget to cyber operations. Thus, North Korea's cyber aggression is not only a tool for espionage or sabotage but also a form of power projection aimed at demonstrating the country's capabilities in modern conflicts, while posing a challenge to the international security order.

North Korea's Response

In the 1990s, North Korea faced an economic threat in the form of a famine. In response, North Korea implemented market reforms and a centralized economy, as well as investing in development. North Korea also pursued a program to develop weapons of mass destruction (nuclear and missile). Some experts argue that the motivation behind developing weapons of mass destruction was to deter foreign enemies and control their domestic system, including the military and internal security forces. However, the weapons of mass destruction program also led to economic sanctions against North Korea. In response to these economic threats, it is said that North Korea has carried out bank robberies and other crimes in cyberspace to help balance its critical trade deficit and avoid economic sanctions (Pinkston, 2020).

North Korea's foreign policy priorities in cyberspace include developing the following: 1) Cyber weapons that can be integrated with electronic warfare and other asymmetric capabilities; 2) Cyber tools for espionage in military security, industrial technology, and diplomatic information; 3) Cyber revenue sources, including legitimate (albeit small-scale) internet commerce and illicit cash sources; 4) Defense against cyber espionage and cyber attacks from enemies, particularly South Korea and the United States; and 5) More sophisticated and widespread information operations (Pinkston, 2020).

Since 2011, the country has begun directing its hacking capabilities toward the private sector for economic gain. The targets of these attacks have expanded geographically from the Korean Peninsula to a global scale, as seen in major incidents such as the hacking of Sony Pictures in 2014, the theft of funds from the Bangladesh Central Bank in 2016, and the WannaCry ransomware attack in 2017 (Hwang 7 Choi, 2021; Sharp, 2017).

Based on this, North Korea's response to economic and security threats shows how it strategically utilizes cyberspace as an instrument in responding to external pressures such as economic sanctions and diplomatic isolation. North Korea has developed offensive cyber capabilities to achieve political and economic goals that are difficult to achieve through conventional means. Cyber activities such as theft, espionage, and sabotage have become asymmetric tools to create strategic effects on other countries, particularly South Korea and the United States, without triggering open military confrontation. These cyber attacks serve as a relatively inexpensive yet highly destructive medium for conflict, while also providing North Korea with an opportunity to demonstrate its strength and respond to threats against its nation.

Strengthening Cyber Capabilities

Since the mid-1980s, North Korea has made significant efforts to strengthen its cyber capabilities. Recognizing its relative inferiority in conventional weaponry compared to the United States and South Korea, North Korea has invested in asymmetric military capabilities, such as nuclear weapons, ballistic missiles, and cyber capabilities. Within Pyongyang's strategic thinking, asymmetric warfare capabilities are considered the main guarantee for national survival. North Korea views cyber capabilities as a strategic weapon. Thus, the strengthening of cyber capabilities is a product of Pyongyang's strategic thinking in preparing for a new era. Specifically, this strategy serves three main strategic objectives: to offset North Korea's conventional military limitations, to cause social disruption in enemy territory at minimal cost and risk of retaliation, and to generate revenue amid international sanctions (Kim, 2022).

The US Department of Defense has expressed the view that North Korea's cyber capabilities pose a serious threat that extends beyond the regional sphere. Given North Korea's bleak economic prospects, offensive cyber operations are seen as a cost-effective way to develop deniable asymmetric military options (Siers, 2014).

North Korea is determined to build offensive cyber capabilities, and given its previous successes involving sabotage and even theft from foreign central banks, any potential cyber espionage, sabotage, or infiltration in cyberspace that facilitates violence in the real world must be handled with extreme caution (Nah, 2023). North Korea's offensive cyber capabilities are becoming more sophisticated and destructive. Initially, its cyber attacks consisted of website defacement or DDoS (Distributed-Denial-of-Service) attacks against servers. However, following the Sony attack in November 2014, North Korean hackers focused on larger crimes such as bank heists and ransomware to generate profits for the regime (Berghel, 2015; Chung, 2016).

Given the regime's characteristics and its need for cash, these efforts are expected to continue unless there is a fundamental change in the government. North Korean hackers are highly skilled and very difficult to prevent effectively. Methods for identifying the source of attacks are improving, but attribution still requires a significant amount of time. This makes it difficult for targets to respond, while North Korean attackers continue to learn and strengthen their computer network defenses (Pinkston, 2020). The implementation of North Korea's cybersecurity capabilities will be heavily influenced by sovereign government policies, as previously discussed in the indicators related to the role of decision-makers.

Judging from the cyber attacks carried out, Lazarus or Hidden Cobra is one of the biggest cyber threats to international security, originating from North Korea, which has disabled millions of computers and caused financial losses because, in addition to stealing data, they also target cryptocurrency and vaccine intellectual property. Little is known about the Lazarus

Group, except that they are a group of cybercriminals from North Korea. The US intelligence community states that Lazarus primarily engages in espionage and hacking financial institutions to obtain much-needed funds to finance the heavily sanctioned country and its nuclear program. By the end of 2019, Lazarus had successfully disabled hundreds of thousands, even millions, of computers and stolen up to US$2 billion. Despite the mystery surrounding the Lazarus Group, one thing is clear: they are one of the biggest cyber threats to international security (Park, 2021).

Since 2013, the Kimsuky hacking group has been attempting to gather important information from public institutions through phishing attacks. Since 2018, investigations into the Kimsuky group's attack techniques have been conducted. The results show that the phishing pages used in the attacks were not only sophisticated enough to be difficult to distinguish by security experts, but also used various disguises such as customer centers and emails. The phishing was disguised as defense and government agencies using typical social engineering attack techniques. Technically, it is difficult for ordinary email users to respond only according to their interests because the emails use advanced attack techniques such as exploiting vulnerabilities in email attachments (Lee, 2021).

In cases of remote control using leaked account information or the sending of phishing emails, it is very difficult to take action because it is impossible to immediately confirm that the account has actually been stolen. Lee (2021) also mentions that Kimsuky continues to develop phishing email attack techniques to collect important information related to defense, security, and diplomacy. According to Lee, the goal of the Kimsuky group is to collect intelligence data because it focuses on phishing attacks targeting diplomatic and defense institutions of target countries and related foreign institutions. This is reinforced by findings in January 2022 of a hacking attack allegedly carried out by Kimsuky with the aim of stealing COVID-19-related research data (Youn, 2022).

Although North Koreans generally have limited access to advanced Internet infrastructure, the country has highly trained cyber capabilities to carry out its cyber operations. North Korea continues to increase its resources and budget. This increased capability enables North Korea to respond to external threats more effectively and efficiently. Through cyber operations, North Korea can have strategic impacts not only on security but also on strengthening the country's position in the face of international pressure. Thus, cyberspace has become a domain for North Korea to carry out its defense strategy.

CONCLUSION

Based on the analysis of the data obtained, it can be concluded that North Korea's threat perception is greatly influenced by the characteristics of its authoritarian regime and dynastic power system, with the main emphasis on the regime's political stability being prioritized over the country's institutional security. North Korea shows a pattern of centralized, aggressive, and interpretation-based response to external pressure, especially from Western countries. The strategy of using cyber power carried out by North Korea reflects a stage of observation and assessment influenced by historical experience, deep distrust of the outside world, and the need to maintain internal power without having to engage in conventional conflict.

The practical implications of these findings indicate that cyber power has become a primary tool for North Korea in dealing with international isolation and sanctions. Cyber operations are not only used as a tool of espionage and sabotage, but also as an instrument for seeking foreign exchange through digital theft and as a form of coercive diplomacy. North Korea's ability to exploit gaps in global governance in cyberspace makes it a difficult actor to deal with in the international system. This can increase the risk of cyber conflict and also complicates the international community's efforts to create transparent, stable, and accountable cyber governance.

Therefore, further research is recommended to further explore the relationship between threat perception and asymmetric strategies in cyberspace, especially in the context of state actors operating outside international norms. Further studies can also deepen the understanding of the effectiveness of diplomatic responses and collective mechanisms of international or states in dealing with transnational cyber threats. In terms of policy, the international community or states also need to accelerate the formulation of stronger and more inclusive cyber legal norms, as well as build verification and accountability mechanisms that are able to face challenges from states that use cyberspace as a tool for geopolitical contestation.

Acknowledgement

The author wishes to extend sincere appreciation to Dr. phil. Yandry Kurniawan who has provided valuable direction and insightful consultation in the writing process of this article.

REFERENCE

Ahmad, Atif., et al. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Elsevier: Computers & Security, 86*, 402-418. https://doi.org/10.1016/j.cose.2019.07.001

Avery, Emma C., et.al. (2017). North Korean Cyber Capabilities: In Brief. *Congressional Research Service*. https://sgp.fas.org/crs/row/R44912.pdf

Badan Siber dan Sandi Negara. (2024). *Lanskap Keamanan Siber Indonesia Tahun 2023*. Jakarta: BSSN.

Berghel, Hal. (2015). *Cyber Chutzpah: The Sony Hack and the Celebration of Hyperbole*. The IEEE Computer Society.

Blank, S. J. (2003). *Rethinking Asymmetric Threat*. Strategic Studies Institute.

Blatter, Joachim & Haverland, Markus. (2014). *Case Studies and Causal Process Tracing*. Palgrave Macmillan.

Boo, Hyeong-wook. (2017). *An Assessment of North Korean Cyber Threats*. *The Journal of East Asian Affairs, 31(1)*, 97–117. https://www.jstor.org/stable/44321274

Bryman, Alan. (2012). *Social Research Methods* (4th ed.). Oxford University Press.

Byman, Daniel & Jennifer Lind. (2010). Pyongyang's Survival Strategy: Tools of Authoritarian Control in North Korea. *International Security, 35(1)*, 44–74. https://www.jstor.org/stable/40784646

Chung, Min Kyung., et.al. (2016). A Study on North Korea's Cyber Attacks and Countermeasures. *Journal of Information Technology Services*, *Journal of Information Technology Services, 15*(*1),* 67–79. https://doi.org/10.9716/KITS.2016.15.1.067

Cohen, Raymond. (1978). *Threat Perception in International Crisis*. *Political Science Quarterly, 93(1)*, 93–107. https://doi.org/10.2307/2149052

Hwang, Jeeseon. & Choi, Kyung-Shick. (2021). North Korean cyber attacks and policy responses: An Interdisciplinary Theoretical Framework. *International Journal of Cybersecurity Intelligence and Cybercrime*, *4(2),* 4–24. https://www.doi.org/10.52306/04020221NHPZ9033

Jervis, R. (1976). *Perception and Misperception in International Politics*. Princeton University Press.

Kim, Chong Woo & Carolina Polito. (2019). The Evolution of North Korean Cyber Threats. *Asan Institute for Policy Studies*.

Kim, Min-hyung. (2022). North Korea's Cyber Capabilities and Their Implications for International Security. *Sustainability*, *14*, 1744. https://doi.org/10.3390/su14031744

Kim, Yongho. (2013). North Korea's Threat Perception and Provocation Under Kim Jong-un. *North Korean Review, 9(1)*, 6-19. DOI: 10.3172/NKR.9.1.6

Kim, Yu-Kyung., et al. (2020). Analysis of the Asymmetrical Relationships between State Actors and APT Threat Groups. *2020 International Conference on Information and*

Communication Technology Convergence (ICTC), 695-700, DOI: 10.1109/ICTC49870.2020.9289506

Lee, Jaeil, et al. (2021). Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups. *IEEE Access, 9*. DOI: 10.1109/ACCESS.2021.3084897

Mandiant. (2025). M-Trends 2025 Report. Google Cloud Security. https://cloud.google.com/security/resources/m-trends

MITRE. (2025). Kimsuky. https://attack.mitre.org/groups/G0094/

MITRE. (2025). Lazarous Group. https://attack.mitre.org/groups/G0032/

Nah, Liang Tuang. (2023). North Korean Hackers. *North Korean Review*, *19(1*), 91–98. DOI: 10.2307/NKR/19.1./NKR.19.1.91

National Cyber Security Centre. (2024). Joint Cybersecurity Adisory: North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs. https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/0/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches* (7th ed.). Pearson Education.

NSFOCUS. (2025). APT Annual Lanscape Report. Beijing: NSFOCUS's Fuying Lab. https://nsfocusglobal.com/company-overview/resources/2024-apt-annual-landscape-report/

Park, Joshua. (2021). The Lazarus Group: The Cybercrime Syndicate Financing The North Korea State. *Harvard International Review, 42(2),* 34-39.

Pinkston, Daniel A. (2020). North Korea's Objectives and Activities in Cyberspace. *Asia Policy*, *15(2)*. https://www.jstor.org/stable/27023903

Sharp, Travis. (2017). Theorizing cyber coercion. *Journal of Strategic Studies, 40(7),* 898–926. DOI:10.1080/01402390.2017.1307741

Siers, Rhea. (2014). North Korea The Cyber Wild Card. *Journal of Law & Cyber Warfare, 4(1),* 1–12. http://www.jstor.org/stable/26441246

Verizone Business. (2025). 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

Waltz, K. N. (1979). *Theory of International Politics*. Random House.

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge University Press.

Youn, Jaepil, et al. (2022). Research on Cyber ISR Visualization Method. *Electronics, 11,* 4142. https://doi.org/10.3390/electronics11244142

Youn, Jaepil, et al. (2023). Correction: Research on Cyber ISR Visualization Method *Electronics, 12,* 4975. https://doi.org/10.3390/electronics12244975