From Hermit Kingdom to Digital Dynasty: North Korea’s Cyber Security Strategies and Artificial Intelligence

Münzevi Krallıktan Dijital Hanedanlığa: Kuzey Kore'nin Siber Güvenlik Stratejileri ve Yapay Zeka

Aybala LALE KAHRAMAN

Asst. Prof. Dr., Bursa Technical University, Faculty of Humanities and Social Sciences, Department of International Relations, ORCID: 0000-0003-3289-5403, Email: aybala.lale@btu.edu.tr

Abstract

This paper analyzes North Korea's cybersecurity policies and their association with artificial intelligence (AI) as it emerges as an asymmetric power in cyberspace. Evidence suggests that state-sponsored cyber groups associated with North Korea have commenced utilizing AI to enhance the efficacy of their cyber activities. It is interesting that North Korea, once a ‘reclusive kingdom’, has become a prominent name in the digital world. Nowadays, numerous cyberattacks linked to North Korea have been identified. These attacks are generally thought to have the characteristics of North Korean hacker organizations. Consequently, the study doesn’t regard North Korea's integration of AI into its cybersecurity plans as only defensive; it perceives them as a survival strategy inside the international order. The study's central claim is that Juche ideology is connected to the nation's endeavors to strengthen its cyber capabilities and make it possible to employ AI as a cyber instrument for this kind of endeavor.

Keywords: Cybersecurity, Cyber Operations, Artificial Intelligence (AI), North Korea, Juche.

Öz

Bu çalışma, siber uzayda asimetrik bir güç olarak varlık kazanan Kuzey Kore’nin siber güvenlik stratejilerini ve yapay zeka ile ilişkisini incelemektedir. Kuzey Kore bağlantılı devlet destekli siber oluşumların, siber operasyonlarını daha etkin hale getirmek için yapay zeka kullanmaya başladığı yönünde tespitler mevcuttur. Kuzey Kore’nin, ‘münzevi bir krallık’ iken, dijital ortamda adından söz ettirir bir duruma gelmesi ilgi çekicidir. Son yıllarda Kuzey Kore’ye atfedilen pek çok siber saldırı faaliyeti tespit edilmiştir. Bu saldırıların Kuzey Koreli hacker gruplarından izler taşıdığı yönünde kanaatler hakimdir. Bu nedenle çalışma, Kuzey Kore’nin siber güvenlik stratejilerini yapay zeka ile bütünleştirme çabalarını, salt savunma amaçlı olarak değerlendirmemekte; uluslararası düzende hayatta kalmaya yönelik bir strateji olarak yorumlamaktadır. Çalışmanın temel argümanı, Juche ideolojisinin, ülkenin siber kapasitesini geliştirme çabalarıyla bağlantılı olduğu ve yapay zekânın bu amaç doğrultusunda bir siber araç olarak kullanılmasına imkân sağladığıdır.

Anahtar Kelimeler: Siber Güvenlik, Siber Saldırılar, Yapay Zeka (YZ), Kuzey Kore, Juche.

Makale Türü / Article Type	**Başvuru Tarihi / Submitted**	**Kabul Tarihi / Accepted**
Araştırma Makalesi/Research Article	22.09.2025	04.11.2025

Bu makaleye atıf için / To cite this article
Lale Kahraman, A. (2025). From Hermit Kingdom to Digital Dynasty: North Korea’s Cyber Security Strategies and Artificial Intelligence. *Bölgesel Araştırmalar Dergisi,* 9(2), 214-230.

Introduction

> *"If you're not concerned about AI safety, you should be. Vastly more risk than North Korea."*
>
> Elon Musk (2017)

As the world moves towards Industry 4.0, the Internet of Things and machine-to-machine interaction are transforming economic and social life. It is impossible for inter-state relations to remain unaffected by this transformation. In the 21st century, digitalization, particularly social media, is an element of diplomacy and foreign policy and has been influenced by new security parameters. Artificial intelligence has an undeniable place in this digitalized world order. In fact, technology not only provides opportunities and benefits, but also creates the most impactful states in terms of risks it harbours and crisis potential.

In the aftermath of the Cold War, states have shifted their areas of competition to space, cyberspace, defense industry driven by the utmost technologies and artificial intelligence. At this point, cyberspace offers opportunities. However, the phenomenon of an anarchic international system reveals the fact that cyberspace cannot be used only for peaceful purposes. This is due to the fact that countries carry out activities in cyberspace in accordance with their own ambitions and interests. Cyberspace and artificial intelligence create an asymmetric power that facilitates not only the development of the world's advanced nations but also those of developing and even the backward countries to enter the power equation.

It is clear that such a system, where machines mimic human behavior, can provide undeniable advantages for countries like North Korea. In recent years, North Korea has created an asymmetric power in cyberspace and launched devastating cyberattacks, posing a threat to cybersecurity. The integration of artificial intelligence into North Korea's cybersecurity strategies has the potential to significantly amplify the scale and sophistication of the threats posed by the regime. It is highly likely that North Korea, which actively employs cyber technologies in the development of its ballistic missile and nuclear programs, will seek to capitalize on the opportunities presented.

A few previous studies have focused on the evidence for the use of artificial intelligence by North Korea (Harold et al., 2022; Kang, 2024; Kang, 2019; Choe et al., 2018). Researchers have not treated how authoritarian regimes such as North Korea use artificial intelligence to improve their abilities in much detail. As a highly closed and totalitarian society, North Korea has limited opportunities to obtain information from primary sources. This constitutes the limitation of the study. This study employs document analysis as its primary research method, given the challenges associated with accessing reliable primary data from North Korea. The document analysis method is particularly effective for investigating closed regimes where field research is constrained. However, North Korean websites and resources with the .kp domain name will be analyzed in this study. Although websites with .kp domain codes are limited, North Korean websites directly shared by the South Korean website kcnawatch.org were also utilized.

The study aims to analyze North Korea's cyber security strategy in the context of the Juche, which has become the dominant philosophy in the country, and to reveal the relationship between these strategies and artificial intelligence. The study also aims to find out how North Korea integrates artificial intelligence into the process when conducting cyberattacks. The importance of this study is to assess the capability of authoritarian regimes to integrate artificial intelligence into cyber security strategies. In this context, artificial intelligence in international relations may create power asymmetries between states and reshape power relations. Thus, the fundamental question of the study is how Juche's ideology influenced North Korea's adoption of artificial intelligence in its cybersecurity strategy. In addition, it seeks to present North Korea as an example of how the authoritarian regime shapes its strategic behaviour in the digital age.

Understanding a Hermit Country: Juche Ideology (주체 사상)

North Korea, often described as a ‘closed box’, is steeped in a long history of isolation. The term ‘Hermit Kingdom’ traces back to the Joseon Dynasty (1392-1897), a period marked by strictly limited external interactions. During this era, Korean citizens were prohibited from traveling abroad, and the Peninsula maintained minimal contact with foreign entities. The few permitted interactions were restricted to controlled trade with Japan in select border towns and a walled compound in Busan. Apart from diplomacy with China and Japan, Korea remained closed to foreigners (Seth, 2008: 28). This isolationist stance, which originally characterized Joseon Korea, eventually came to define the North Korea (DPRK)[1], founded as a separate state in 1948. Today, North Korea represents a rare example of a closed socialist society.

North Korea is characterized by an ideology that permeates every aspect of life. It is important to analyze and understand the main outlines of this ideology in order to understand North Korea's overall activities and current situation. In fact, there is almost no area in the country where the Juche ideology does not find a place. The word Juche is a combination of two Chinese characters, Ju and Che. Ju means master, subject, actor, while Che means object, thing, material (Helgesen, 1991: 188-189). According to “Juche Idea: Answers to Hundred Questions,” published by the Pyongyang Foreign Languages Publishing House, *“The Juche idea is, in a word, an ideology that the masses of the people are the masters of the revolution and construction and they have the strength to push them. In other words, it is an ideology that man is the master of his destiny and he has the power to carve out his destiny”* (Foreign Languages Publishing House, 2012: 1). Therefore, Juche emphasizes that the Korean people are the masters and determinants of their own destiny, highlights the Korean nation's ability to be ‘self-sufficient’.

The idea of Juche, first announced by founding leader Kim Il Sung in 1955 (Kim, 1973), was influenced by Marxism-Leninism and Maoism, but Kim made no reference to Karl Marx, Frederick Engels or Vladimir Lenin in his Juche speech (David-West, 2011: 93). In 1983, Kim Jong Il claimed that the communist movement, which is considered as a struggle to free people from all forms of dependence and constraints, is fully in line with the principles of Juche. However, Kim emphasized that it is the interpretation of

[1] The official name of the state known as North Korea in the literature is the Democratic People's Republic of Korea (DPRK). In the study, this state will be referred to as 'North Korea'.

Marxism-Leninism from a Juche perspective that provides the ideological and theoretical basis for the Korean revolution (Kim J.I., 1983). Juche is seen as a creative adaptation of Marxist-Leninist principles to the political realities in North Korea (Yuk, 1972: 157). At this point, Kim Il Sung was in fact a mass-oriented leader like Mao Zedong and was heavily influenced by China. The similarity of the historical experiences and current conditions of both countries led to the adoption of Maoism to some extent. In particular, the emphasis on the mobilization of the masses and the establishment of a people's army to wage people's war were shaped by Maoism (Kakışım, 2017: 75). However, since the 1960s, when the Sino-Soviet split began, Juche has completely broken away from these ideologies as a separate path. Shaped by Confucian thought and Korean nationalism, Juche aimed to develop collective revolutionary consciousness and socialism by uniting the Korean proletarian and peasant masses (Lerner, 2001: 655).

Before the basic principles of Juche, the only concept that cannot be considered independent of Juche is the principle of Songun (선군-army first). Songun is based on the principles of Juche. For North Korea, the army is not an abstract authority but a practical performer. Its most important task is to respond directly and effectively to the needs and aspirations of the people. The Songun-centered society believes that the military has the resources, knowledge and skills to solve the problems people face. In this way, the doctrine requires people to be completely dependent on the military. The popular belief propagated under the Songun banner is that "there is no problem too big or too small for the military to solve" (Park, 2007: 2). At this point, controlling and prioritizing the military has paved the way for North Korea to become a country focused on military doctrines. In the background of this situation, there is the need to establish the independent line of a country that was enemies and declared an axis of evil both during and after the Cold War. Indeed, after the loss of the Soviet Union's support, the necessity of building a unique path for North Korea increased.

Juche is an ideology of self-sufficiency and self-reliance that permeates every aspect of life. The system, reinforced by a dynastic succession from father to son, consists of three basic elements: chaju (자주-political independence), charip (자립-an independent economy) and chawi (자위-confidence in national defense). Simply put, the military-first line guarantees political independence, which in turn provides the conditions for economic self-reliance (French, 2007: 31). Political independence (chaju), the most fundamental principle of Juche ideology, emphasizes full equality and mutual respect between nations. It asserts that each state has the right to self-determination in order to secure the happiness and well-being of its people in the way it deems most appropriate. In the North Korean interpretation, Juche entails non-submission to foreign oppression. Kim Jong Il predicted that dependence on foreign powers would lead to the failure of the socialist revolution in Korea (Lee, 2003: 106). In the sense of economic independence, charip means that the Korean Peninsula, which was devastated after the war, should develop according to its own means and build a national economy based on its own strength. Charip set as a goal the creation of an industrial infrastructure capable of autonomous development and prioritized a strict central planning policy to support economic and political independence (Gills, 1992: 128). Chawi, on the other hand, envisages a self-sufficient defense system and aims to mobilize the entire country and fully instill the ideology in the armed forces (Lee, 2003: 107). In this context, the importance of chawi is reflected in the efforts to advance North Korea's nuclear armament efforts and ballistic missile tests, which resonated in the global context.

As a result, in the light of Juche principles, a socialist-based dynastic order unique to North Korea was built in the country. The Juche ideology was constructed to facilitate the establishment of a monolithic system and presented as a people-oriented philosophy, transforming it into a system where one must submit to the guidance of the Suryeong, the leader (Park Y.S., 2014: 6). By building Juche as a religious and state ideology, it serves as a mechanism for maintaining the dictatorship of North Korea and shows the appearance of a socialist monarchy.

North Korea's Cybersecurity Strategies Within the Framework of Juche Ideology

North Korea represents one of the world's most challenging intelligence targets. Despite its limited technological infrastructure and economic constraints, the regime has invested significantly in cyber capabilities. North Korea's domestic intranet is accessible only to an elite few, leaving the general population largely disconnected from the global internet. In 2013, Eric Schmidt reported only a few thousand internet-connected computers in the country, underscoring North Korea's digital isolation (Boo, 2017: 98). Nonetheless, North Korea has increasingly conducted cyber operations against various states, particularly South Korea, signaling its growing ambitions in cyberspace.

Since the Korean War, North Korea has consistently developed asymmetric tactics and capabilities aimed at exploiting its adversaries' vulnerabilities and offsetting its own limitations in conventional military power (Metz and Johnson, 2001: 1). Offensive cyber capabilities offer the regime a means to project power beyond its geographic limitations. Starting in the 1990s, North Korea's political-military strategy has increasingly prioritized asymmetric tactics that can harm or destabilize neighboring states and adversaries (Harold et al., 2022: 3). Kim Jong Un, the current leader, has described cyber warfare as an "all-purpose sword" which, alongside nuclear weapons and missiles, ensures the military's unyielding offensive capabilities. This notion has roots in the 1980s when North Korea, acutely aware of its conventional weapons inferiority relative to the United States and South Korea, focused on developing nuclear, chemical, and biological weapons of mass destruction. In Pyongyang's strategic framework, it is precisely these asymmetric capabilities that safeguard the regime's survival. Cyber operations have now emerged as a key component of this asymmetric strategy.

With outdated conventional military resources and limited means for modernization, North Korea finds cyber capabilities a cost-effective alternative. Cyberattacks, especially those aimed at a technologically advanced state like South Korea, serve as a mechanism to disrupt social stability and foster unrest. Economic incentives are also a primary driver of North Korea's cyber operations, as these activities generate revenue through hacking, online bank heists, and cryptocurrency theft. Thus, North Korea leverages cyber strategies not only to destabilize adversaries but also to secure illicit financial flows into the country.

Internet access in North Korea is strictly limited to a select group of government officials and a small number of foreign nationals. Within this elite group, only the highest-ranking leaders, ruling elites, and their families receive direct access to the global internet, making up an even smaller subset (Recorded Future, 2017: 19). Despite these restricted connections, the country’s computer hardware remains limited, although efforts have been made to develop a domestic information technology sector (Lee and Hwang, 2004). In 1995, North Korea installed its first fiber-optic cables along the Pyongyang-Hamhung route through the Wonsan port (Warf, 2015: 113). By 1996, the country’s initial internet connection to the outside world was established via the United Nations Development Program office in Pyongyang (Pinkston, 2016: 62). North Korea’s domestic intranet, Kwangmyong, links key scientific agencies, research institutions, academic centers, libraries, select businesses, and distinguished citizens. Additionally, the country has developed its own Linux-based operating system, Red Star, to ensure digital practices align with national values (Ko et al., 2008). In 2007, North Korea officially obtained its “.kp” domain name (Warf, 2015: 114).

The groundwork for North Korea’s cyber capabilities was laid in the early 1980s. In 1983, North Korea established its first computer assembly plant, followed by the founding of the Pyongyang Information Center (PIC) in 1986, aimed at producing software and automotive systems. North Korea’s focus on cyber technologies grew with global advancements in technology and the fall of the Soviet Union, during a time when the regime faced significant existential challenges. During this period, Kim Jong Il prioritized national security, envisioning North Korea’s strength to rest on three pillars: ideological-political unity, military power, and economic stability (Pinkston, 2020: 77). To sustain the socialist system, all three components were deemed essential. However, economic hardships, exacerbated by food shortages, posed a significant threat to this vision, pushing North Korea toward an intensified focus on information technology.

Recognizing cyberspace's potential to bring strategic benefits, Kim Jong Il designated 1999 as the “Year of Science,” advocating for software development as a cornerstone of a resilient and prosperous nation (Sung, 2020: 268-269). His son, Kim Jong Un, continues to emphasize the role of science and technology, particularly through the byungjin policy, which simultaneously pursues nuclear and economic advancement. Reflecting this dual focus, North Korea’s 2016-2020 five-year economic plan identifies science and information technology as central to bolstering strategic industry production (Pinkston, 2020: 78).

In North Korea, cyber warfare is regarded as a national mission, embedded within the country’s military strategy and overseen by the Workers' Party and the Central Military Commission, North Korea’s highest authorities (Jense and Lies, 2013). The country's hacking operations are divided primarily between the General Staff of the Korean People's Army and the General Bureau of Reconnaissance, which is responsible for intelligence gathering and covert actions against South Korea. Each organization has specialized units tasked with software development, network protection, and offensive cyber operations. Cybersecurity analysts have identified several North Korean hacking groups, including Lazarus Group, Bluenoroff, Andariel, and Stardust Chollima, among others. Bureau 121, established in 1998 under the General Bureau of Reconnaissance, is one of the regime's primary cyber units. Initially estimated to have 500-1,000 members, this unit focuses on researching cyberattack techniques, software engineering, cryptography, and networking. Members often receive training at leading computer science institutions in China and Russia (Pinkston, 2016: 60).

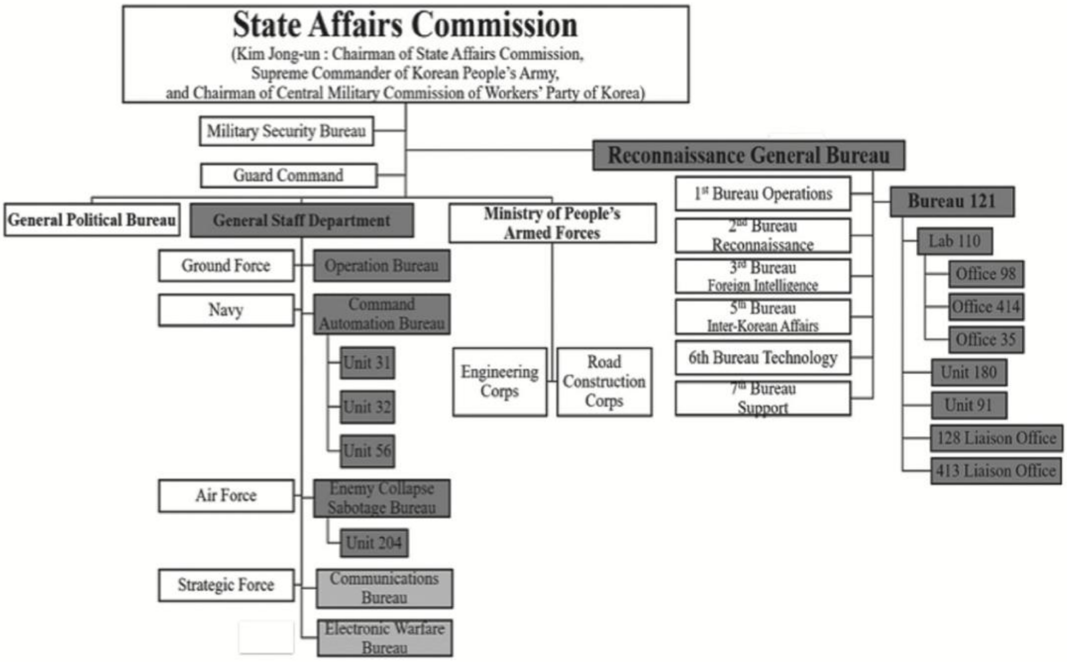

Table 1: North Korean Cyber Organization Structure (Kong and Lim, 2019: 4)

North Korea also has seven key research institutions dedicated to information technology. Among them, the Korea Computer Center (KCC)—a joint venture with Samsung that began operations in Pyongyang’s Mangyongdae district in 2000—is particularly prominent. Other notable institutions include the Pyongyang Informatics Center, the DPRK Academy of Sciences, and Silver Star Laboratories. The Ministry of Education has also introduced computer science curricula from primary school through university levels to support this cyber infrastructure (Warf, 2015: 113). The limited development of these institutions and their organizational structures, however, is shaped by the guiding principles of Juche, North Korea's self-reliance ideology.

North Korea’s cyber priorities are as follows: (1) development of cyber weapons that complement electronic warfare and other asymmetric capabilities; (2) espionage tools targeting military security, industrial technologies, and diplomatic information; (3) revenue generation from both legitimate internet commerce and criminal sources; (4) defense mechanisms against cyber espionage and attacks, particularly from South Korea and the United States; and (5) advanced information operations (Pinkston 2020, 81-82). North Korean cyberattacks likely began around 2004, but South Korean concerns surged after the 7.7 DDoS attack in 2009. Prior to this incident, North Korean cyber activities mainly involved basic email hacks (Boo, 2017: 100).

The Lazarus Group, a state-backed entity with North Korean origins, has reportedly conducted cyber operations since 2009. Some of its most significant attacks include the 2013 DarkSeoul incident and the 2014 Sony Pictures breach. In the DarkSeoul attack, malware was deployed against major South Korean broadcasters and financial institutions, resulting in the disabling of thousands of computers and critical servers. The Sony Pictures attack, executed in 2014, included anonymous ransom notes directed at executives, followed by targeted system breaches and data leaks (Whyte, 2016: 99-100). This operation aimed to prevent the release of The Interview, a satirical film depicting a fictional plot against North Korea's leader. The attack was notable for including threats reminiscent of 9/11 and escalated the level of physical intimidation involved in cyber operations. A more recent example includes the 2022 cryptocurrency heist, in which North Korean hackers allegedly stole a record $1.7 billion, adding to an estimated $3 billion in cryptocurrency thefts since 2017. In 2022 alone, funds from these activities are thought to have covered approximately 45% of North Korea's military budget, allowing the regime to circumvent economic sanctions through illicit digital finance channels.

North Korea, which utilizes third-country networks and information technologies while conducting cyber operations, prefers networks in countries such as China and Russia to compensate for its limited internet infrastructure. The country also engages in indirect technology transfers and cyber collaborations with China and Russia, which it considers friendly nations in cyberspace. China, in particular, is directly linked to North Korea's cyber activities and provides infrastructure support. North Korean hackers operate in some Chinese cities near the North Korean border. IP addresses originating in China have been used in significant attacks, including the 2014 Korea Hydro and Nuclear Power attack and the 2016 attack on South Korea's cyber command center. It is also known that Park Jin Hyok, a member of the Lazarus Group, worked at Chosun Expo, a China-based front company. Russia enabled North Korea's internet access by laying fiber optic cables along the border in 2017. Russian IP addresses are also used in North Korean cyberattacks. It has been determined that BlockNovas, a fake company recently established in the United States by North Korea, also uses a Russian IP address. The depth brought to relations by the Ukraine War has also increased North Korea's dependence on Russian infrastructure (Bae, 2025). On the other hand, recent studies show that countries such as Russia, China, North Korea, and Iran are increasing their use of artificial intelligence to carry out cyberattacks against the US and spread manipulation and disinformation online. For example, North Korea is making progress in developing digital profiles that use artificial intelligence to create fake American identities (The Korea Times, 2025). Although the US has imposed sanctions on Chinese and Russian individuals and entities supporting North Korea's cyber operations, these measures remain limited (Bae, 2025).

North Korea's cyber strategy aligns closely with the economic principles of Juche, aiming to reinforce the nation's nuclear and military capabilities while securing unauthorized financial resources. The regime maintains a doctrine of political independence, grounded in the Juche ideals of national defense and economic self-sufficiency. North Korea's cyber activities are not restricted to attacks against South Korea; rather, they represent an adaptive approach that leverages the evolving asymmetries of cyberspace to diversify and refine its attack methods continually.

The concept of strategic culture has the potential to shed light on North Korea's cybersecurity strategies. Snyder (1977: 8) defines strategic culture as *"the sum-total of ideas, conditioned emotional responses, and patterns of habitual behavior that members of the national strategic community have acquired through instruction or imitation."* Following this logic, strategic culture in North Korea is shaped by the country's totalitarian political structure, Juche ideology, and historical traumas. Both Japanese colonial rule and the devastating effects of the Korean War drove the North Korean regime to “survival” and “develop self-defense,” and the major power politics on the Peninsula fueled this. Therefore, increasing military capacity, the cult of leadership, and the propaganda apparatus are necessary for the regime's survival (Husenicova, 2018). The traumas of the twentieth century and its military culture continue to this day for North Korea, which is surrounded by enemies such as the United States, South Korea and its allies (Stratford, 2025: 127-128). In this context, cyber activities, like nuclear weapons, guide the regime's security strategies and form part of its strategic culture. The pursuit of developing independent technologies linked to Juche encourages North Korea to use artificial intelligence.

The Role and Future of Artificial Intelligence in North Korea’s Cyber Security Strategies

The Juche ideology, central to North Korea's efforts to bolster its cybersecurity infrastructure and cyberattack capabilities, is intrinsically linked to advancements in science and technology. In its quest to mitigate security challenges, North Korea increasingly relies on asymmetric warfare tactics. Notably, the nation has demonstrated an active engagement with developments in artificial intelligence (AI) over recent years.

As AI continues to integrate into various sectors, cybersecurity has become indispensable to its safe and systematic application. Conversely, AI is also essential for achieving robust cybersecurity. Major technology firms, including Google, Microsoft, and IBM, exemplify AI's potential in enhancing cybersecurity through capabilities such as detection, prediction, analysis, and threat mitigation. These AI systems swiftly identify vulnerabilities, supporting cybersecurity professionals in scaling their threat detection efforts. However, the proliferation of AI raises critical questions regarding its role as both a technological and economic resource for North Korea, especially in the context of cyber fraud. Under the Kim Jong Un regime, cyber tools have evolved into pivotal instruments for attaining policy objectives (Chanlett-Avery et al., 2017). Despite advancing its cyberattack sophistication, North Korea struggles to develop the skilled human capital necessary for the field. Consequently, AI has gained prominence as a potential substitute, aiming to address this shortfall and augment cyberattack capabilities.

In 2020, Japan's Ministry of Defense reported that North Korea maintains large-scale cyber units as part of its asymmetric military strategy. These units engage in espionage to acquire sensitive military information and develop capabilities to target critical foreign infrastructures (Ministry of Defense of Japan, 2020: 91). Similarly, South Korea's Ministry of National Defense stated in its 2020 Defense White Paper that North Korea operates a specialized cyber warfare unit, comprising approximately 6,800 trained experts. This unit is reportedly focused on advancing cyber capabilities by investing in the latest technologies, particularly AI (Ministry of National Defense of the Republic of Korea, 2020: 30). AI stands out among these technologies as a tool to optimize and accelerate cyberattack operations. Through AI-driven algorithms, North Korea could potentially enhance its attack precision and efficacy, thereby significantly elevating its cyber threat posture.

The North Korean regime’s approach to the Fourth Industrial Revolution emphasizes the advancement of artificial intelligence (AI) capabilities. In this context, the Fourth

Industrial Revolution represents North Korea's efforts to modernize its economy, with a focus on mass communications, internet infrastructure, and AI technology. The economic principles of Juche thus increasingly depend on technological advancements. Notably, the implementation of the Mirae Wi-Fi system alongside other cellular networks within North Korea marks a significant step toward establishing Industry 4.0 technologies based on wireless connectivity (Lim T.W., 2019: 100). Mirae, a wireless intranet system designed for mobile devices, restricts North Korean households' access to global information through the Mirae SIM card, thereby shielding citizens from foreign propaganda, economic alternatives, communication avenues, entertainment, and potential espionage (HanVoice SFU, 2022).

Some North Korean websites and media outlets occasionally refer to artificial intelligence, with one of the earliest mentions dating back to 2004. A 2004 article titled "Artificial Intelligence Program Developed" noted that the Koryo Academy of Medical Sciences in the DPRK had created an AI program called "Koryo Medicine." Additionally, Kim Il Sung University has been publishing a quarterly series on Information Science since 2018. Between 2018 and 2020, this series featured 48 articles on machine learning and deep learning techniques. The majority of these articles addressed Natural Language Processing (NLP), exploring topics like English-to-Korean machine translation, database development, and detection of prohibited words in text (Harold et al., 2022: 7). An August 11, 2019 article in the Pyongyang Times highlighted the expanding role of AI worldwide. This article provided an overview of AI's historical development and included examples of AI applications in China and Russia. It also suggested that AI would be integrated with education, signaling a shift from traditional teaching methods. Furthermore, a 2019 report detailed a competition held during the "2019 IT Achievements Exhibition" to showcase advancements in North Korea's AI technology. Kim Il Sung University was again mentioned in a 2021 article, underscoring AI's prominent position in North Korea's technological agenda (Pyongyang Times, 2021). In addition, Naenara has published news about the ideals of allied countries such as Russia and Iran to develop their own artificial intelligence technology, both by presenting parallel policies with these countries and by emphasizing the right to self-determination (Naenara, 2024; Naenara, 2025).

According to North Korean sources, AI has become a required subject for undergraduate students at Kim Il Sung University, illustrating its growing importance in recent years. The United Nations Panel of Experts reported that North Korea employs over a thousand IT professionals abroad who generate foreign income for the regime (Yoshida and Oshima, 2020). Recognizing data as more valuable than gold or oil in the AI era, North Korean leaders likely benefit from information these IT workers collect abroad, which informs domestic AI research at various universities. A 2018 study published in "KSII Transactions on Internet and Information Systems" involving five North Korean researchers reflects ongoing efforts to enhance the nation's computing infrastructure, particularly in cloud services (Choe et al., 2018).

North Korean artificial intelligence (AI) research has its origins in the algorithm-based program Eunbyul, developed by the Korea Computer Center for the traditional game of Go (Lim, 2019: 101). First created in 1997, Eunbyul achieved its inaugural victory in 1998 and continued to perform impressively in the World Computer Go Championship until 2009 (Kang S.W., 2017). Although Google DeepMind's AlphaGo gained worldwide fame as the first AI program to defeat a professional human Go champion, Eunbyul had previously secured six international titles and established dominance in the digital Go arena (HanVoice SFU, 2022). Eunbyul's development is closely linked to machine learning. Furthermore, Pyongyang's programs, while limited in resources, demonstrate efficiency and effectiveness. North Korea's AI initiatives exemplify how single-minded focus can achieve notable outcomes through maximum resource mobilization and determination (Lim, 2019: 101).

In addition to Eunbyul, North Korea has developed Ryongnamsan, a voice-assistance software comparable to Siri or Alexa (Kang S.W., 2017). Ryongnamsan functions as a translation tool for social science texts from English to Korean and supports over 30 specialized fields, including physics, biology, chemistry, mathematics, information technology, geography, and medicine. According to North Korean researchers, the software incorporates a large-scale circular neural network language model, achieving a speech recognition accuracy of 98% (Kang J., 2019: 23). Furthermore, Kim Il Sung University has developed fingerprint and facial recognition systems, while Kim Chaek University of Technology has created a multilingual translation program (Kim M., 2021: 32).

Access to hardware necessary for AI advancement remains challenging for North Korea, primarily due to sanctions that restrict the export of luxury goods and advanced technologies to the country. However, nations such as China and Russia often interpret these restrictions differently (Harold et al., 2022: 8). The 2019 United Nations Panel of Experts report noted that a company associated with the DPRK National Academy of Defense Science signed an agreement with a Chinese firm to employ three North Korean programmers and two hardware developers for the design of AI products, encompassing both software and hardware. AI practitioners in North Korea use terminology that aligns closely with language used in Western AI research (Lim, 2019: 102).

Linking scientific and technological advancements with leadership aligns with North Korea's concept of the Suryeong, or "guiding leader." This leader-focused ideology presents the head of state as the visionary transforming the nation from an agricultural society into a technologically advanced one. In North Korea, where titles like "Supreme Leader" and "Eternal Leader" are used, AI development is similarly influenced by the leader's vision. Under Kim Jong Un, North Korea has initiated a push toward the Fourth Industrial Revolution, emphasizing science and technology policies (Kang J., 2019: 22). However, this technology-driven ambition faces challenges due to the country's isolationist stance, which hampers North Korea's AI efforts. The isolation limits the accessibility, sharing, and integration of large data repositories essential for AI applications (Lim, 2019: 102). Nevertheless, North Korea prioritizes state control over AI, aligns its initiatives with global economic trends, and focuses on commercializing its technological achievements (Lim, 2022: 90).

North Korea is considered part of a "cyber axis" alongside Iran, Russia, and China, strategically leveraging cyberspace to exert destabilizing influence (Fabio, 2018: 8). Militarization of AI in North Korea will likely center on cyberspace. Given that nations North Korea considers adversaries—such as the United States, South Korea, and Japan—increasingly deploy AI in military contexts, North Korea is likely interested in exploring how cyber operations could target AI systems. Currently, North Korean cyberattacks still rely primarily on human operatives, with limited integration of advanced AI technologies. However, the regime's commitment to AI research is evident. Statements from the Leader, official media reports, studies at major universities, and expert analyses collectively indicate North Korea’s investment in AI and its attention to international technological advancements. These signs suggest that North Korea may soon adopt AI-driven cyber offensive or defensive strategies.

North Korea’s focus on AI for cyber operations holds significant advantages, particularly in minimizing the costs associated with cultivating human expertise. For the regime, AI offers an ideal tool: unlike human operatives, AI requires no loyalty or resources to remain dependable. Consequently, the North Korean government may consider deploying AI for surveillance, sentiment analysis, loyalty verification, and censorship (Harold et al., 2022: 15-16).

Recent reports suggest that North Korea is actively enhancing its cyber capabilities through the integration of artificial intelligence. U.S. Deputy National Security Advisor Anne Neuberger has highlighted that certain North Korean cybercriminals are attempting to leverage AI models to develop malware and exploit vulnerable systems, posing a substantial threat to global cybersecurity. North Korea's previous cyberattacks, including the 2014 Sony Pictures breach, the 2017 WannaCry ransomware attack, and various cryptocurrency theft operations, exemplify its existing cyber proficiency. The integration of AI into such attacks could significantly escalate the level of risk and instability in cyberspace. For North Korea, utilizing artificial intelligence as a strategic tool—both for offensive and defensive cyber operations—appears to be an inevitable progression.

Here we can raise the following question for discussion: Will AI increase strategic predictability in authoritarian regimes? It is clear that countries such as China, North Korea and Russia restrict access to the Internet strictly or partially in order to prevent the dissemination of ideas. These trends manifest themselves in the form of access restrictions, surveillance, suppression of freedom of expression and the establishment of digital firewalls, all aimed at controlling information and people. This is because artificial intelligence is one of the easily accessible tools that authoritarian leaders can use to maintain their power (Acevedo, 2023). Therefore, the difficulty of attributing blame for crimes already existing in cyberspace further reinforces unpredictability with artificial intelligence.

Conclusion

The influence of Juche ideology, which promotes self-sufficiency, is evident across all aspects of the North Korean regime. North Korea’s recent transformation from a hermit dynasty to a digital power underscores its potential as an assertive and global threat within its region. This shift is particularly visible in the regime’s cyberattacks and operations over the past decade. Despite restricted internet access for the general population, North Korea’s ability to conduct effective cyberattacks not only sustains the regime but also enhances the strategic use of military assets that the nation prioritizes. Although North Korea’s systems may appear rudimentary, they nonetheless exhibit asymmetric power in cyberspace.

In the era of artificial intelligence, it is almost inevitable that North Korea will exploit emerging opportunities to advance its cyber operations. Integrating artificial intelligence into cybersecurity strategies as a means to stabilize the regime would likely intensify North Korea’s threat level. The country’s pursuit of AI-enhanced cybersecurity is not limited to defensive strategies; rather, it serves its broader goal of survival in an international order it perceives as a direct threat. Juche ideology, therefore, aligns closely with North Korea’s endeavors to expand its cyber capabilities. The financial gains from cyber operations contribute to sustaining the regime's economic independence, while AI integration further enhances its digital strategy. This advancement allows for more sophisticated activities, including data manipulation, surveillance, and high-level cyberattacks. North Korea’s efforts reflect a broader trend among authoritarian regimes that leverage technology as a geopolitical tool.

This study argues that the integration of North Korea's artificial intelligence into its cyber-security strategies reflects a broader survival strategy guided by the Juche ideology. North Korea uses Artificial Intelligence for both defence and offensive cyber operations to strengthen its regime stability, ensure economic independence and maintain strategic deterrence in an adversarial international environment.

Currently, no definitive evidence indicates that North Korea actively employs AI in its cyber operations. However, the country’s ongoing adaptation to technological progress since the 1980s has increasingly brought AI into the spotlight in media and academic discussions, particularly since the early 2000s. Given this trajectory, it is probable that North Korea will adopt AI-driven offensive capabilities in the near future, thereby elevating the sophistication and impact of its cyber operations. Such advancements are expected to enhance North Korea’s ability to conduct sophisticated attacks, manipulate data, and expand its cyber surveillance mechanisms — thereby amplifying its asymmetric power. By leveraging artificial intelligence to enhance its cyber capabilities, North Korea illustrates its dedication to Juche principles—securing safety and strategic advantage through technological advancements while remaining independent of external assistance. To sum up, Juche is not just an ideology, but a strategic driver, enabling the integration of AI into cybersecurity strategies so that authoritarian regimes can more easily adapt to the digital age.

References

Acevedo, M. (2023). Artificial Intelligence and Authoritarian Governments. https://democratic-erosion.org/2023/11/17/artificial-intelligence-and-authoritarian-governments/.

Bae, S. (2025). Hidden Enablers: Third Countries in North Korea’s Cyber Playbook. https://www.csis.org/analysis/hidden-enablers-third-countries-north-koreas-cyber-playbook.

Boo, H. W. (2017). An assesment of North Korean cyber threats. *The Journal of East Asian Affairs,* 31(1), 97-117.

Boulanin, V., Saalman, L., Topychkanov, P., Su, F. and Carlsson, M.P. (2020). Artificial intelligence, strategic stability and nuclear risk. SIPRI.

CFR. (2022, June 28). North Korea’s Military Capabilities. 7 September 2024, https://www.cfr.org/backgrounder/north-korea-nuclear-weapons-missile-tests-military-capabilities.

Chainalysis. (2023, February 1). 2022 Biggest year ever for crypto hacking with $3.8 billion stolen, primarily from defi protocols and by North Korea-linked attackers. 7 September 2024, https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/ .

Chanlett-Avery, E., Rosen, L. W., Rollins, J. W. and Theohary, C. A (2017). *North Korean cyber capabilities: in brief.* Congressional Research Service.

Choe, S., Li, B., Ri, I., Paek, C.S., Rim, J.S.and Yun, S.B. (2018). Improved hybrid symbiotic organism search task-scheduling algorithm for cloud computing. *KSII Transactions on Internet and Information Systems,* 12(8), 3516-3541.

David-West, A. (2011). Between confucianism and Marxism-Leninism: Juche and the case of chŏng tasan. *Korean Studies,* 35, 93-121.

Encylopedia of Korean Culture. (2024). 9 September 2024, https://encykorea.aks.ac.kr.

European Parliament. (2024). Artificial intelligence and cybersecurity. https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA(2024)762292_EN.pdf.

Fabio, R. (2018). *Confronting an “axis of cyber”?—China, Iran, North Korea, Russia in cyberspace*. Ledizioni Ledi Publishing.

Foreign Languages Publishing House. (2012). *Juche idea: answers to hundred questions*. Foreign Languages Publishing House.

French, P. (2007). *North Korea the paranoid peninsula*. Zed Books.

Gills, B. (1992). North Korea and the crisis of socialism: the historical ironies of national division. *Third World Quarterly,* 13(1), 107-130.

Ha, M. and Maxwell, D. (2018). *Kim Jong Un’s ‘all-purpose sword’ North Korean cyber-enabled economic warfare*. FDD Press.

HanVoice SFU. (2022). The past, present, and the future of North Korea’s artificial intelligence. https://sfuhanvoice.medium.com/the-past-present-and-the-future-of-north-koreas-artificial-intelligence-12eb959d3507.

Harold, S. W., Beauchamp-Mustafaga, N., Jun, J. and Myers, D. (2022). *Will artificial intelligence hone North Korea's cyber "all-purpose sword?*. KEI.

Hayes, P. (2005). DPRK information strategy – does it exist?. In A.Y. Mansourov (Ed.), *Bytes and bullets: information technology revolution and national security on the korean peninsula*, (pp. 70-99). Asia Pacific Center for Strategic Studies.

Helgesen, G. (1991). Political revolution in a cultural continuum: preliminary observation on the North Korean "juche" ideology with its intrinsic cult of personality. *Asian Perspective,* 15(1), 187-213.

Husenicova, L. (2018). North Korean Strategic Culture: Survival and Security. *Scientific Bulletin*, 45(1), 26-35.

Jense, T. and Liles, S. (2013). *Open-source analysis of the cyber warfare capability of North Korea.* Proceedings of The 14th Annual Information Security.

Kakışım, C. (2017). Kuzey Kore'nin resmi ideolojisi olarak cuçe öğretisi ve Kuzey Kore dış politikasına etkileri. *Uluslararası İlişkiler,* 14(56), 73-88.

Kang, J. (2019). The 4th industrial revolution and education in North Korea. *ICAICTSEE* (Sofia), 22-27.

Kang, J.G. (2019, November 1). 북한 "인공지능 시대 데이터가 금, 원유보다 중요. http://www.nkeconomy.com/news/articleView.html?idxno=2158.

Kang, J.G. (2024, May 21). North Korea's Kim Il Sung university information technology institute is the center of North Korea's AI research and development. http://www.nkeconomy.com/news/articleView.html?idxno=13357.

Kang, S.W. (2017, October 17). North Korea was once AI powerhouse. https://www.koreatimes.co.kr/www/tech/2024/09/129_237814.html.

KCNA. (2004, May 20). Artificial intelligence program developed. http://kcna.co.jp/item/2004/200405/news05/21.htm#10.

Kim, I.S. (1973). *On eliminating dogmatism and formalism and establishing juche in ideological work - speech to party propaganda and agitation workers, December 28, 1955*. Foreign Languages Publishing House.

Kim, J.I. (1983). *Let us advance under the banner of Marxism-Leninism and the Juche idea.* Foreign Languages.

Kim, M.H. (2021). 북한 인공지능 기술의 군사화와 우리 군의 대응 무기체계 발전방향 연구. *Journal of Information Technology Services,* 20(1): 29-40.

Ko, L. (2018, June 6). North Korea as a geopolitical and cyber actor. https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/north-korea-geopolitical-cyber-incidents-timeline/.

Ko, K., Jang, S. and Lee, H. (2008). *.Kp North Korea. digital review of asia/pacific.* Sage Publications India.

Kong, J., Lim, J.I and Kim, K.G. (2019). *The all-purpose sword: North Korea's cyber operations and strategies* IEEE.

Lee, G. (2003). The political philosophy of Juche. *Stanford Journal of East Asian Affairs,* 3(1), 105-112.

Lee, H. and Hwang, J. (2004). ICT development in North Korea: changes and challenges. *The Massachusetts Institute of Technology Information Technologies and International Development,* 2(1), 75-87.

Lerner, M. (2001). A failure of perception: Lyndon Johnson, North Korean ideology, and the pueblo incident. *Diplomatic History*, 25(4), 647-675.

Lim, E.C. (2019). 북한의 4차 산업혁명 : 대응전략, 추진방식과 성과. *Donga Research Institute*, 1-35.

Lim, T.W. (2019). North Korea's artificial intelligence (A.I.) program. *North Korean Review,* 15(2), 97-103.

Mansourov, A. Y. (2011). *North Korea on the cusp of digital transformation.* The Nautilus Institute.

Masse, B. (2023, October 18). North Korea experiments with AI in cyber warfare: US official. https://venturebeat.com/ai/north-korea-experiments-with-ai-in-cyber-warfare-us-official/.

Metz, S. and Johnson, D. V. (2001). *Asymmetry and U.S. military strategy, definition, background, and strategic concepts.* U.S. Army War College.

Meyers, A. (2018, April 6). Meet crowdstrike’s adversary of the month for april: stardust chollima. https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-april-stardust-chollima/.

Ministry of Defense of Japan. (2020). *Defense of Japan 2020.* Tokyo.

Ministry of National Defense of the Republic of Korea. (2020). *Defense White Paper 2020.* Seoul.

Musk, E. [@elonmusk] (2017, August 12). If you're not concerned about AI safety, you should be. Vastly more risk than North Korea. https://x.com/elonmusk/status/896166762361704450.

Naenara. (2024, December 15). 로씨야대통령 인공지능기술개발문제에 대해 언급. http://naenara.com.kp/main/search_first?sVal=인공지능&csrf_test_name=bdcab409386d0d9aa7ed32712e9f67fc.

Naenara. (2025, January 11). 이란대통령 인공지능개발사업의 중요성을 강조. http://naenara.com.kp/main/search_first?sVal=인공지능&csrf_test_name=bdcab409386d0d9aa7ed32712e9f67fc.

Park, H. S. (2007). Military-first politics (songun): understanding Kim Jong-il’s North Korea. *Korea Economic Institute,* 2(7), 1-9.

Park, Y.S. (2014). Policies and ideologies of the Kim Jong-un regime in North Korea: theoretical implications. *Asian Studies Review,* 38(1), 1-14.

Pinkston, D. A. (2016). Inter-Korean rivalry in the cyber domain: the North Korean cyber threat in the son’gun era. *Georgetown Journal of International Affairs,* 27(3), 60-76.

Pinkston, D. A. (2020). North Korea's objectives and activities in cyberspace. *Asia Policy,* 15(2), 76-83.

Pyongyang Times. (2019, August 11). Artificial intelligence brought into wide application. https://kcnawatch.org/newstream/1566470856-959824495/artificial-intelligence-brought-into-wide-application/.

Pyongyang Times. (2021, March 12). Institute wins top ten IT enterprise title for the third time. http://www.pyongyangtimes.com.kp/?bbs=39864.

Recorded Future. (2023, November 30). Crypto country: North Korea’s targeting of cryptocurrency. https://www.recordedfuture.com/research/crypto-country-north-koreas-targeting-cryptocurrency.

Recorded Future. (2017). *North Korea cyber activity*. Recorded Future Insikt Group.

Rodong Sinmun. (2019, August 11). National exhibition of IT successes 2019 closes. https://kcnawatch.org/newstream/1573186825-553240718/national-exhibition-of-it-successes-2019-closes/.

Seth, M. J. (2008). Korea: from hermit kingdom to colony. *World History: 1750-1914,* 13(2), 28-33.

Stratford, J.D. (2005). Strategic Culture and the North Korean Nuclear Crisis: Conceptual Challenges and Policy Opportunities. *Security Challenges*, 1(1), 123-133.

Snyder, J. (1977). *The Soviet strategic culture: Implications for limited nuclear operations*. Santa Monica: Rand

Sung, Y.E. (2020). 북한 사이버 테러의 특성 분석 및 시사점. *Korean Journal of Convergence Science,* 9(3), 265-279.

The Korea Times. (2025). Russia, N. Korea, China upping AI use to escalate cyberattacks on US., https://www.koreatimes.co.kr/world/20251017/russia-n-korea-china-upping-ai-use-to-escalate-cyberattacks-on-us.

UN Panel of Experts. (2019). Final report of the panel of experts submitted pursuant to resolution 2464, https://undocs.org/Home/Mobile?FinalSymbol=S%2F2020%2F151&Language=E&DeviceType=Desktop&LangRequested=False.

Warf, B. (2015). The hermit kingdom in cyberspace: unveiling the North Korean internet. *Communication & Society, 18*(1), 109-120.

Whyte, C. (2016). Ending cyber coercion: computer network attack, exploitation and the case of North Korea. *Comparative Strategy,* 35(2), 93-102.

Yoshida, K. and Oshima, Y. (2020, April 18). "North Korea sent 1,000 IT specialists across the world: UN report", https://asia.nikkei.com/Spotlight/N-Korea-at-crossroads/North-Korea-sent-1-000-IT-specialists-across-the-world-UN-report.

Yuk, S. L. (1972). *Juche! the speeches and writings of Kim Il Sung*. Grossman Publishers.