Journal of Social and Political Sciences

Fauzan, F. A., & Juned, M. (2026), South Korea's National Cybersecurity Strategy in Responding to North Korean Cyber Attacks During Moon Jae-in's Administration. *Journal of Social and Political Sciences*, 9(1), 220-229.

ISSN 2615-3718

DOI: 10.31014/aior.1991.09.01.633

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research *Social and Political Sciences* is a peer-reviewed International Journal. The journal covers scholarly articles in the fields of Social and Political Sciences, which include, but are not limited to, Anthropology, Government Studies, Political Sciences, Sociology, International Relations, Public Administration, History, Philosophy, Arts, Education, Linguistics, and Cultural Studies. As the journal is Open Access, it ensures high visibility and the increase of citations for all research articles published. The *Journal of Social and Political Sciences* aims to facilitate scholarly work on recent theoretical and practical aspects of Social and Political Sciences.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Journal of Social and Political Sciences
Vol.9, No.1, 2026: 220-229
ISSN 2615-3718

DOI: 10.31014/aior.1991.09.01.633

South Korea's National Cybersecurity Strategy in Responding to North Korean Cyber Attacks During Moon Jae-in's Administration

Farah Anasti Fauzan[1], Mansur Juned[1]

[1] Universitas Pembangunan Nasional Veteran Jakarta

Correspondence: Farah Anasti Fauzan, anastifarah@gmail.com

Abstract
This study examines the implementation of South Korea's National Cybersecurity Strategy (NCSS) in response to North Korean cyberattacks during President Moon Jae-in's administration (2019–2022). The escalating intensity of North Korean cyber operations, targeting South Korea's government, critical infrastructure, and financial sectors, prompted the state to formulate a comprehensive national cybersecurity policy. Using a descriptive qualitative approach with a case study method grounded in document analysis, this study analyzes how the 2019 NCSS was implemented as a strategic policy response to persistent cyber threats. The findings indicate that the NCSS 2019, through its six main pillars-critical infrastructure protection, enhanced response capacity, collaborative governance, cybersecurity industry innovation, cybersecurity culture development, and global leadership-served as a strategic framework that strengthened institutional coordination and the direction of South Korea's cybersecurity governance in addressing North Korean cyber threats. However, the policy demonstrated effectiveness primarily in threat management and response rather than in threat prevention, as cyberattacks from North Korea will continue into the post-implementation period (2023–2024). This study contributes to cybersecurity policy analysis by demonstrating how securitization theory illuminates the elevation of cyber issues to national security priorities and highlights the gap between normative policy frameworks and operational implementation.

Keywords: Cybersecurity, National Cybersecurity Strategy, South Korea, North Korea, National Security Policy, Moon Jae In, securitization

1. Introduction

1.1 Background

South Korea is one of the world's most advanced nations in information and communication technology (ICT), particularly in the development and deployment of Internet of Things (IoT) infrastructure. Since the post-Korean War period, South Korean governments have consistently prioritized education and technology as engines of national development. Massive investments in broadband and mobile technology infrastructure since the early

1990s facilitated exponential growth in internet penetration, with South Korea becoming one of the world's first countries to launch a 5G network.

However, the advancement of ICT and IoT simultaneously created new vulnerabilities in South Korea's cyberspace. As the number of interconnected devices has multiplied, the risk of cyberattacks intensified significantly, making cybersecurity a critical element in maintaining national stability and security. North Korea has been the primary source of these cyber threats. Since the Korean War, inter-Korean relations have existed under extreme tension. This complexity has extended into the cyber domain, where both states continuously compete to demonstrate cyber capabilities, making the South Korea–North Korea cyber confrontation one of the most prominent examples of escalated conflict in East Asia.

Since the early 2000s, North Korea has actively invested resources to develop and expand its cyber capabilities (Boo, 2017). The strategic trajectory of North Korean cyberattacks against South Korea evolved in both scale and sophistication over time. An early watershed moment occurred in 2013, when coordinated cyberattacks simultaneously targeted three major broadcasting companies and three financial institutions, disabling more than 57,000 devices and causing substantial operational and financial disruption across the South Korean economy (Pakshad, 2025). The following year, in 2014, North Korean-linked actors infiltrated Korea Hydro and Nuclear Power (KHNP), exfiltrating sensitive nuclear power plant designs, an attack that exposed the vulnerability of South Korea's critical national infrastructure to hostile cyber operations. In 2015, North Korean actors targeted 14 government computers, including three belonging to members of the National Assembly and 11 used by government support staff, demonstrating a direct intrusion into the state's political apparatus. The following year, in April 2016, hackers infiltrated Daewoo Shipbuilding & Marine Engineering (DSME), extracting approximately 40,000 classified documents containing weapons systems data, submarine blueprints, and construction technologies. The breach went undetected for five months and was only revealed in September 2016 after it was discovered that the stolen data included "OPLAN 5015," a classified South Korea–United States operational plan aimed at neutralizing North Korean leadership (C. W. Kim & Polito, 2019).

The period of 2017–2019 marked a qualitative escalation in the character and scope of North Korean cyberattacks. From 2017 onward, North Korean state-affiliated groups, principally Lazarus, Kimsuky, and Andariel, have shifted their significant operational focus toward South Korea's financial sector, executing large-scale cryptocurrency heists and targeting banking institutions as alternative funding mechanisms for the regime. In April 2017, approximately 3,816 bitcoins valued at nearly USD 5 million were stolen from the cryptocurrency exchange YouBit. A second breach in December 2017 resulted in losses of USD 15.6 million and forced the company into bankruptcy after it lost 17 percent of its total assets (Klingner, 2021). During the same year, Bithumb suffered multiple attacks, including two major incidents in February and July that each generated losses exceeding USD 7 million, while other platforms such as Coinis, experienced additional financial damage through hacking and cryptojacking schemes.

Although financially motivated attacks intensified, state-sector targets were not abandoned. In 2018, North Korean-linked actors compromised systems associated with South Korea's Defense Acquisition Program Administration (DAPA) and the Ministry of Unification, exfiltrating sensitive data and personal information of approximately 1,000 North Korean defectors (Ernst & Lee, 2021). That same year, the cryptocurrency exchange Coinrail suffered losses of approximately USD 37 million, while Bithumb recorded an additional USD 40 million loss following a June 2018 cyberattack (C. W. Kim & Polito, 2019). The dual targeting pattern persisted into 2019. North Korean actors attempted to infiltrate the Ministry of Unification through spear-phishing campaigns aimed at gaining access to government systems, reportedly driven by political motives. Concurrently, approximately 58 billion won (roughly USD 49 million at the time) was stolen from Upbit, South Korea's largest cryptocurrency exchange (Klingner, 2021).

Collectively, these incidents produced cascading economic and political consequences. These financial cyberattacks had cascading effects on South Korea's digital economy, undermining public trust in financial infrastructure and exposing the inadequacy of existing sectoral cybersecurity regulations. Simultaneously, North Korean cyber operations intensified espionage operations targeting South Korean defense officials, think tanks,

and diplomatic personnel through sophisticated spear-phishing campaigns, directly threatening national security intelligence.

By this period, North Korean cyberattacks had effectively demonstrated a dual strategic function: generating revenue to sustain the regime's weapons programs while simultaneously destabilizing South Korean society, weakening confidence in state institutions, and probing defense systems without triggering conventional armed conflict. The cumulative impact of these attacks, spanning critical infrastructure, financial systems, defense, and diplomatic sectors, clearly demonstrated that South Korea's fragmented, reactive cybersecurity architecture was no longer adequate to manage the threat environment. Against this backdrop of intensifying and diversifying North Korean cyberattacks, President Moon Jae-in's administration released the National Cybersecurity Strategy (NCSS) in April 2019, representing South Korea's first comprehensive, integrated long-term national cybersecurity policy. Moon Jae-in served as South Korea's 19th president from May 2017 to May 2022, and it was in the third year of his administration that the NCSS was formally adopted, making the period 2019 to 2022 the central timeframe for examining its implementation and effectiveness.

1.2 Research Problem

This study addresses the following research question: How was the National Cybersecurity Strategy (NCSS) implemented in responding to North Korean cyberattacks during the period 2019–2022?

1.3 Research Objectives

This study aims to analyze South Korea's cybersecurity efforts in addressing North Korean cybeattacks through the implementation of NCSS 2019 during the Moon Jae-in administration.

2. Method

This study employs a descriptive qualitative method with a case study approach. Descriptive qualitative research aims to describe and understand phenomena in depth based on narrative descriptive data, with an emphasis on context and the meaning of events studied. The case study approach is suitable for the in-depth analysis of a specific research object, the South Korean National Cybersecurity Strategy (NCSS) 2019, within the context of its implementation in responding to North Korean cyber threats during the Moon Jae-in administration.

Data collection was conducted through document analysis, drawing on official policy documents, government reports, annual cybersecurity reports, and relevant secondary literature. Primary sources include the 2019 NCSS document issued by South Korea's National Security Office, NCSC Annual Reports (2020–2024), and ministerial press releases. Secondary sources include academic journals, books, policy analyses, and scholarly theses. Data analysis followed a three-stage model encompassing data reduction, data presentation, and conclusion drawing. This systematic approach enabled the identification of patterns in policy design and implementation, as well as an assessment of NCSS effectiveness over the study period.

3. Results

3.1 Theoretical Framework: Securitization and Cyber Policy

This study is grounded in securitization theory, developed by the Copenhagen School. Securitization theory provides an analytical framework for understanding how an issue is perceived and constructed as a security threat. In this framework, security is understood as the outcome of a social and political process. An issue becomes a security matter when it is constructed as an existential threat to a valued referent object, such as the state or national stability, requiring emergency measures beyond normal political mechanisms (Buzan et al., 1998). This process, known as a securitizing move, elevates an issue into the security domain (Otukoya, 2024). Securitization emphasizes that the state plays a central role in defining and constructing what is perceived as a threat to national security (Farrahdiba & Juned, 2024).

In South Korea, the securitization of cybersecurity accelerated as North Korean cyberattacks expanded from the government sector to the financial sector from 2017 onward. South Korea has regard North Korean cyber capabilities as equivalent in impact to military operations, since cyberattacks can target vital state sectors without direct armed confrontation (Hwang & Choi, 2021). Therefore, securitization has emerged as a strategic approach to ensure security within South Korea's public cyberspace, given that cyberspace encompasses a broad spectrum of societal interactions and fosters the development of cyberdemocracy within the digital domain (Juned et al., 2024). This perception drove the state to elevate cybersecurity to the level of national security, as reflected in the conceptual design of NCSS 2019. The state must possess the capacity to secure its cyberspace, as such capability directly shapes national security in the physical world, particularly because of the close interconnection between digital systems and conventional information structures (Juned et al., 2023).

The study also employs the cyber policy concept articulated by ENISA (2016) who frame policy as a response to threats that are socially and politically constructed rather than purely technical. This framework further guides the analysis by conceptualizing national cybersecurity strategies as layered, cyclical public policy encompassing strategic, operational, and evaluative dimensions.

3.2 South Korea's Cybersecurity Context

South Korea's cybersecurity ecosystem has been shaped by the synergy of digital infrastructure development, governance reform, multi-sector engagement, and regulatory evolution. The national cybersecurity governance structure is organized across three levels: national, sector, and agency. At the national level, the National Security Office (NSO) serves as the highest authority, with the National Intelligence Service (NIS) providing intelligence support. At the sector level, ministries hold sectoral cybersecurity responsibilities. At the agency level, security monitoring and incident response are directly supported by public institutions and specialized technical bodies operating under the supervision of their respective ministries, such as the Korea Internet & Security Agency (KISA), and the National Cyber Security Center (NCSC) execute operational cybersecurity functions (Park & Kim, 2025).

Despite this structured architecture, South Korea's pre-2019 cybersecurity posture was characterized as largely reactive. The absence of a single comprehensive cybersecurity law led to fragmented sectoral regulations and inter-agency coordination challenges (Do, 2022). The 2009 National Cyber Crisis Comprehensive Countermeasures and 2011 National Cyber Security Master Plan addressed immediate threats but remained insufficient as long-term strategic visions.

3.3 North Korean Cyber Attack Architecture

North Korea's cyber capability development has evolved from rudimentary espionage into sophisticated, multi-sector offensive operations. The strategic direction of North Korean cyber operations is determined at the level of Supreme Leadership and coordinated through the Reconnaissance General Bureau (RGB), which oversees cyber espionage, attacks against external targets, and illicit financial operations as alternative regime funding sources. State-affiliated hacker groups, including Kimsuky, Lazarus, and Andariel, serve as operational extensions of the regime with specific mission profiles. Lazarus is associated with large-scale financial theft; Kimsuky specializes in spear-phishing and intelligence collection targeting diplomats and policy experts; and Andariel focuses on industrial and defense sector infiltration. North Korean cyber operations against South Korea can be classified into three categories: cyber espionage targeting strategic information and defense data; financial attacks on cryptocurrency exchanges and banking institutions as alternative funding mechanisms; and system disruption targeting digital infrastructure stability. These operations are not incidental but are designed to support long-term strategic objectives, allowing North Korea to conduct intelligence activities, disrupt systems, and generate economic gains without direct armed confrontation, with minimal effective international legal consequences (Klingner, 2021).

4. Discussion

4.1 NCSS 2019 and the Moon Jae-in Administration

President Moon Jae-in, South Korea's 19th president (May 2017–May 2022), assumed office in the aftermath of a major political crisis that eroded public trust in state institutions. A former human rights lawyer and pro-democracy advocate affiliated with the progressive Democratic Party, Moon emphasizing inclusivity, transparency, and innovation-driven growth. Upon taking office, however, he inherited two simultaneous cybersecurity challenges: escalating North Korean cyber threats and a fragmented national cybersecurity system. His administration also navigated complex geopolitical dynamics, balancing relationships with both the United States and China while managing domestic economic priorities. Moon's approach to North Korea, reconciliatory yet pragmatic, shaped the character of NCSS 2019 (Ku, 2021).

As noted by Meghna Pradhan (personal communication, 2025), rather than adopting a purely confrontational posture, the administration adopted a reconciliatory and de-escalatory approach toward North Korea, seeking to reduce inter-Korean tensions. Moon recognized that cyber threats, especially those originating from North Korea, could not be disregarded, given their expanding impact on critical infrastructure, financial systems, and national defense. His approach therefore evolved into a pragmatic synthesis: engagement with North Korea did not imply strategic leniency, but rather coexistence with strengthened institutional preparedness. Within this context, the adoption of the National Cybersecurity Strategy (NCSS) in 2019 marked a decisive consolidation of national cyber policy under Moon’s leadership, the administration expanded the roles of key institutions such as NIS, MSIT, and MoIS to strengthen inter-agency coordination and response capacity (Pradhan, 2024).

NCSS 2019, officially approved by the National Security Office on April 3, 2019, represented the culmination of South Korea's cybersecurity reform process. The strategy marked a decisive policy shift from sectoral and technical approaches toward a comprehensive, nationally integrated strategic framework encompassing defense, diplomacy, industry, and civil society. The strategy aligned with Moon's broader vision of a "Just Republic of Korea," framing digital security as a component of public welfare and a prerequisite for innovation-driven economic growth.

4.2 Implementation of the Six Pillars of NCSS 2019

Pillar 1 — Critical Infrastructure Protection. The first pillar focused on protecting the core national infrastructure, including energy, transportation, health, finance, and communications. Implementation was characterized by incremental strengthening of existing systems rather than wholesale policy transformation. Key actions included support for the world's first commercial 5G network launch in 2019, with over 4.5 million subscribers. In the energy sector, Korea Electric Power Corporation (KEPCO) & Korea Hydro & Nuclear Power (KHNP) implemented mandatory 24-hour cyber incident reporting and "security by design" for nuclear industrial control systems (ICS). For financial infrastructure, KISA conducted annual information security management system (ISMS) audits of cryptocurrency exchanges, while Financial Services Commission (FSC), via Financial Intelligence Unit (FIU), monitored suspicious transactions and anti-money laundering (AML) compliance in digital assets. In transportation and healthcare, institutions such as the Korea Railroad Corporation (KORAIL) and the National Health Insurance Service (NHIS) participated in annual attack simulations organized by KISA.

Pillar 2 — Response Capacity. The NCSC, operating under the NIS, served as the primary national response actor. Key mechanisms included the System for Sharing National Cyber Threat Information, upgraded and extended to the private sector in 2020; 91 security monitoring centers, 13 of which were newly established post-NCSS 2019; and the development of digital network analysis (DNA) for each hacker organization through malware pattern analysis, producing detection rules shared across government and public sector monitoring centers. The NCSC issues cyber emergency warnings across four risk levels: moderate, substantial, severe, and critical, based on hack incident patterns and impact potential. Training exercises in 2020 covered 57 ICS-managing organizations encompassing 128 ICS systems, including Email Hacking Response Training and Virtual Network Real-Time Defense Training (NCSC, 2020).

Pillar 3 — Collaborative Governance. The governance structure integrated government, military, private sector, and civil society. The NSO assumed a whole-of-government coordination role, with the NIS providing intelligence support. The policy framework was developed by nine government organizations and ratified by presidential signature. From the military side, the Military Cyber Command (MCC) conducted offensive and defensive cyber operations (Park & Kim, 2025) while the Defense Counterintelligence Command (DCC) handled internal security and investigation. Private sector partners including AhnLab, SK Shieldus, and Samsung SDS collaborated with the NCSC and KISA through formalized public–private partnership schemes. Notably, South Korea does not possess a single comprehensive cybersecurity law; regulation operates through sectorally dispersed legislation, creating persistent challenges in cross-sector incident coordination.

Pillar 4 — Industry Innovation. The government acted as an "enabler" of cybersecurity ecosystem growth. Support mechanisms included the Scale-up TIPS program under the Ministry of SMEs and Startups, which provided intensive state-backed funding support to support research and development (R&D) and business expansion, thereby accelerating technological commercialization and strengthening market competitiveness. This financial mechanism reflected a broader strategy to cultivate a sustainable cybersecurity industry capable of competing at the global level.

The National Cyber Security Research Institute (NSRI) under KISA received 70 billion KRW within MSIT's total 190.4 billion KRW cybersecurity budget for national R&D (Ministry of Science and ICT, 2024). The NCSC, in collaboration with NSRI, also organized the Cyber Conflict Exercise (CCE) to cultivate operational-level and student talent. These measures demonstrate that the state did not merely regulate the cybersecurity sector but actively shaped its innovation trajectory through coordinated financing, research consolidation, and workforce development.

Pillar 5 — Cybersecurity Culture. The state positioned society as a primary actor in the national cybersecurity ecosystem. Programs spanning education, awareness campaigns, academic competition, and industry exhibitions have been deployed, including the JCSC Workshop, the annual Eulji Exercise (national emergency drills across provinces), Korea Cyber Security Week, the Cyber Security Thesis Contest and Academy, the National Cryptography Contest, and international conferences ISEC and SECON & EGISEC. These initiatives reflected an approach that integrated fundamental rights including the right to access a safe and free digital space into cybersecurity education strategy, fostering civic responsibility for digital security.

Pillar 6 — Global Leadership. South Korea pursued bilateral and multilateral cybersecurity partnerships to position itself as an influential actor in global cyber governance. The K-Cybersecurity Promotion Strategy (2021) targeted a top-five global ranking through 670 billion KRW investment by 2023, encompassing real-time threat sharing through a Cybersecurity Alliance, annual assessment of 110,000 PCs, and development of 3,000 digital experts and 100 AI-based startups. Through the Ministry of Foreign Affairs (MOFA), South Korea transferred capacity-building programs for developing nations. As a leading nation in this field, it has actively participated in multilateral forums including the UN Group of Governmental Experts (GGE), the Open-Ended Working Group (OEWG, 2019–2022), the Global Forum on Cyber Expertise (GFCE), and the ASEAN Regional Forum (ARF), contributing to the promotion of responsible state behavior norms in cyberspace.

4.3 Policy Continuity Assessment: 2023–2024

The post-Moon administration period provides a critical lens for evaluating the long-term impact of NCSS 2019. Hacking incidents detected throughout 2023 were attributed to state-sponsored hacker groups, confirming that cyber threats from North Korea remained structurally entrenched. The Kimsuky group consistently conducted spear-phishing campaigns in 2023, impersonating South Korean and U.S. think tanks to target experts in politics, diplomacy, and national security. In June 2023, an advanced phishing campaign exploited real-time website cloning technology to replicate the Naver portal, targeting user credentials. These attacks demonstrated that even the nation's most critical digital infrastructure remained vulnerable to social engineering.

In 2024, the Andariel group intensified espionage targeting semiconductor equipment companies using Living off the Land (LotL) techniques, stealing product design images and facility location photographs, data with high strategic value given North Korea's semiconductor needs for satellite and missile programs. The Lazarus group was confirmed to have stolen nearly 1 TB of internal data from South Korean court computer networks, indicating that long-term infiltration had continued into the post-NCSS implementation period. In response to continued threats, South Korea issued four joint international cybersecurity warnings with the United States, United Kingdom, and Germany in 2023, launched the National Cyber Risk Management Unit (NCRMU) for enhanced cross-sector coordination, and expanded National Cyber Threat Intelligence (NCTI) sharing mechanisms.

4.4 Evaluating NCSS 2019 Effectiveness

Conceptualizing securitization in the field of cyber security policy illuminates the strategic, operational, and evaluative dimensions of NCSS 2019. At the strategic layer, the six pillars comprehensively articulated South Korea's cybersecurity vision, priorities, and governance structure. At the operational layer, the policy was translated into concrete actions including infrastructure hardening, expanded monitoring centers, cross-sector training, startup ecosystem support, and international partnerships. At the evaluative layer, post-2022 evidence reveals that while institutional and operational capacity improved considerably, cyber threat intensity from North Korea did not decline.

This finding aligns with the securitization framework's implication that once an issue is securitized, it becomes structurally embedded in national security discourse; however securitization does not inherently guarantee the elimination of the threat (ENISA, 2016) NCSS 2019 effectively institutionalized South Korea's cyber response architecture but remained limited in its preventive capacity. The preventive limitations of NCSS 2019 are further illuminated through this assesment.

South Korea’s cybersecurity governance faces the fundamental challenge not in the absence of strategic vision, but in the structural gap between policy formulation and ground-level implementation, a gap that allows persistent state-sponsored actors, such as North Korea, to continue operating with relative impunity despite institutional improvements. National cybersecurity strategies operating in asymmetric threat environments must be accompanied by adaptive operational mechanisms, particularly given that state-sponsored cyber actors continuously recalibrate their techniques in response to defensive countermeasures. The primary impact of NCSS 2019 lies in threat management and mitigation rather than threat prevention. The policy strengthened the state's ability to detect, respond to, and recover from cyberattacks. In this sense, NCSS 2019 is institutionally sustainable but preventively constrained. It succeeded in building a solid long-term institutional and operational foundation through a combination of domestic technical strengthening, multi-actor collaboration, and international leadership, but could not halt or significantly reduce the intensity of North Korean cyber operations.

4.5 Enabling and Constraining Factors in the Implementation of NCSS 2019

An analysis of NCSS 2019's implementation cannot be separated from identifying the factors that supported or constrained its effectiveness during the 2019–2022 period. Understanding these factors provides a more comprehensive context for evaluating the gap between normative policy design and operational execution on the ground.

Regarding enabling factors, at least three key elements contributed to the relative success of NCSS 2019. First, South Korea's highly advanced digital infrastructure, including extensive internet penetration and the world's first commercially launched 5G network which created an ecosystem conducive to the deployment of high-technology cybersecurity solutions. Dunn Cavelty (2022) emphasize that the maturity of a nation's digital infrastructure directly influences its capacity to implement effective cybersecurity policies. Second, substantial budgetary commitment, reflected in MSIT's allocation of 190.4 billion KRW for national cybersecurity R&D, provided the financial foundation for industry innovation and human resource development. Third, South Korea's active participation in multilateral forums, such as the UN GGE and OEWG, reinforced the international legitimacy of its cybersecurity strategy while enabling real-time cyber threat intelligence exchange.

Conversely, several structural factors constrained the effectiveness of NCSS 2019. The absence of a single comprehensive cybersecurity law was fundamental. Sectorally dispersed regulation created inter-agency jurisdictional ambiguity and slowed cross-sector incident response coordination (Y. Kim, 2021). The second constraining factor was the inherent capability asymmetry in the South Korea–North Korea cyber confrontation. As argued by (Klingner, 2021), state actors operating outside international norms with minimal legal consequences hold a structural advantage in the cyber domain, since the cost of attack is far lower than the cost of defense. North Korea, unconstrained by effective international cyber legal regimes, can continue to launch offensive operations without bearing meaningful sanctions. The third factor was the human resource challenge. Despite the launch of digital talent development programs, the gap between demand for cybersecurity professionals and the availability of trained experts remained a significant bottleneck in the operationalization of NCSS 2019, particularly in critical sectors operating Industrial Control Systems (ICS).

5. Conclusion

South Korea's experience under the Moon Jae-in administration illustrates both the possibilities and the inherent limits of national cybersecurity strategy in the face of persistent, state-sponsored aggression. The NCSS, formally adopted in April 2019, was not simply a policy document; it was a structural response to years of escalating North Korean cyberattacks that had exposed critical vulnerabilities across South Korea's government, financial, and infrastructure sectors. By consolidating cybersecurity governance under a coherent six-pillar framework, the strategy succeeded in transforming what had been a fragmented, reactive national posture into a more coordinated and institutionally grounded one.

Across the 2019–2022 implementation period, tangible progress was achieved in several dimensions: the expansion of security monitoring infrastructure, the deepening of public-private collaboration, the cultivation of a domestic cybersecurity industry, and the strengthening of South Korea's engagement in multilateral cyber governance forums. These developments collectively raised the country's baseline resilience and positioned cybersecurity firmly within the national security agenda. The securitization process, once set in motion, became institutionally self-reinforcing.

However, the evidence from the post-implementation period makes clear that institutional progress and threat reduction are not the same. North Korean cyber operations did not diminish, they continued to evolve, with attacks in 2023 and 2024 targeting semiconductor companies, judicial systems, and diplomatic institutions using increasingly sophisticated techniques. This trajectory confirms that the primary contribution of NCSS 2019 lies in enhancing South Korea's capacity to manage and respond to cyberattacks, rather than preventing or deterring them at their source. Therefore, the gap between strategic design and operational effectiveness remains the central challenge in cybersecurity governance, particularly where the adversary operates outside international legal constraints.

Taken together, these findings point to an enduring tension in national cybersecurity policy: the more comprehensive the strategy, the greater the expectations placed upon it. However, the asymmetric nature of state-sponsored cyber conflict means that even well-resourced, well-designed frameworks cannot fully neutralize a determined and adaptive adversary. Future policy development in South Korea must therefore focus not only on institutional consolidation, but on closing the legislative gaps that persist across sectors, investing in proactive deterrence capabilities, and building the human capital necessary to sustain long-term operational effectiveness. Research into how subsequent South Korean administrations have adapted, or departed, from the NCSS legacy would further enrich our understanding of the relationship between political transition and national security continuity in the cyber domain.

Author Contributions: Conceptualization, methodology, investigation, data curation, writing original draft preparation, and writing review and editing were conducted by the authors.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Informed Consent Statement/Ethics approval: Not applicable.

Data Availability Statement: Data supporting the reported results are derived primarily from official government documents, institutional reports, and expert interviews. Due to the nature of some primary sources, not all data are publicly accessible. Relevant data may be available upon request from the corresponding author, subject to applicable access restrictions.

Declaration of Generative AI and AI-assisted Technologies: This study has not used any generative AI tools or technologies in the preparation of this manuscript.

References

Boo, H.-W. (2017). *An Assessment of North Korean Cyber Threats and the Republic of Korea's Policy Responses: An Update*. 31(1), 97–117.

Buzan, B., Waever, O., & Wilde, J. de. (1998). *Security: A new framework for analysis* (Nachdr.). Rienner.

Do, G. (2022). *A STUDY ON EFFECTIVE COUNTERMEASURES AGAINST CYBER ATTACKS IN SOUTH KOREA*.

Dunn Cavelty, M. (with Wenger, A.). (2022). *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*. Taylor & Francis Group.

ENISA. (2016). *NCSS good practice guide: Designing and implementing national cyber security strategies.* Publications Office. https://doi.org/10.2824/48036

Ernst, M., & Lee, S. (2021). *Countering Cyber Asymmetry on the Korean Peninsula: South Korea's Defense against Cyber Attacks from Authoritarian Sates*.

Farrahdiba, & Juned, M. (2024). South Korea's Environmental Securitization Process in Facing the Impact of China's Fine Dust. *Journal of Social and Political Sciences*, *7*(1). https://doi.org/10.31014/aior.1991.07.01.480

Hwang, J., & Choi, K.-S. (2021). North Korean Cyber Attacks and Policy Responses: An Interdisciplinary Theoretical Framework. *The International Journal of Cybersecurity Intelligence and Cybercrime*, 4–24. https://doi.org/10.52306/04020221NHPZ9033

Juned, M., Martin, A., & Pratama, N. (2024). Bjorka's Hacktivism in Indonesia: The Intercourse Paradox of Cyberdemocracy, Cyberactivism, and Cybersecurity. *Academic Journal of Interdisciplinary Studies*, *13*(5), 369. https://doi.org/10.36941/ajis-2024-0171

Juned, M., Maryam, S., Salam, S., & Utami, R. A. A. (2023). TikTok's Conflict of Interest with the US Government: Between Big Data Security and Economics (2017-2023). *European Journal of Communication and Media Studies*, *2*(4), 1–8. https://doi.org/10.24018/ejmedia.2023.2.4.23

Kim, C. W., & Polito, C. (2019). *The Evolution of North Korean Cyber Threats*. https://www.jstor.org/stable/resrep20679

Kim, Y. (2021). Evolution of political parties and the party system in South Korea. In S. Lim & N. J. P. Alsford, *Routledge Handbook of Contemporary South Korea* (1st ed., pp. 65–81). Routledge. https://doi.org/10.4324/9781003026150-5

Klingner, B. (2021). *North Korean Cyberattacks: A Dangerous and Evolving Threat*.

Ku, Y. (2021). *An effective shield? Analyzing South Korea's cybersecurity strategy* (S. N. Romaniuk & M. Manjikian, Eds.; 1st ed.). Routledge. https://doi.org/10.4324/9780429399718

Ministry of Science and ICT. (2024). *2024 R&D Budget to Focus on CETs to Aim for Global Technological Dominance*. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&bbsSeqNo=42&nttSeqNo=956

NCSC. (2020). *(Annual Report) NCSC Annual Report 2020*.

Otukoya, T. A. (2024). *The securitization theory*.

Pakshad, P. (2025). *An In-depth Analysis of a Cyber Attack: Case Study and Security Insights*. In RAIS Conference Proceedings 2022-2025 (No. 0561).

Park, J., & Kim, D. (2025). *South Korea's Proactive Cyber Defense and Strategic Cooperation with the United States*.

Pradhan, M. (2024). *Cyber Insecurity in South Korea: Decoding Cybersecurity Vulnerabilities*. Society for the Study of Peace and Conflict (SSPC). https://www.sspconline.org/issue-brief/cyber-insecurity-south-korea-

decoding-cybersecurity-vulnerabilities