SSPC Issue Brief

Cyber Insecurity in South Korea: Decoding Cybersecurity Vulnerabilities

Meghna Pradhan

September 02, 2024

The Issue Brief explores the complex challenges South Korea faces in securing its cyberspace amid rapid digital transformation and escalating geopolitical tensions. Despite being one of the most digitally connected nations, South Korea's cybersecurity framework suffers from significant vulnerabilities, particularly due to persistent cyber threats from North Korea and other state and non-state actors. The study examines South Korea's cybersecurity framework through four distinct phases, each reflecting increased sophistication in policy development. The paper also delves into internal and external factors contributing to these vulnerabilities, including the country's geopolitical situation, technological advancements, and public distrust of government agencies. The paper argues that South Korea lacks a robust legal and institutional framework and a unified strategy to effectively counter and deter cyber threats. The study advocates for a more integrated and transparent approach to cybersecurity to address these persistent challenges.

INTRODUCTION

The cybersecurity apparatus in South Korea seems to be undergoing a gauntlet, as North Korea was allegedly responsible for the recent theft of classified technical data related to two surveillance aircraft. According to the ruling People Power Party, North Korean cyber threat actors could access and steal sensitive information on Baekdu and Geumgang signals intelligence and reconnaissance aircraft, which are important reconnaissance assets deployed by South Korea to monitor its northern neighbour. [1] The theft had emerged at a critical time, as the Baekdu fleet has been undergoing modernization as part of a USD 640 million project, with four additional Dassault Falcon 2000LXS jets being converted into reconnaissance aircraft.[2]

The breach is indicative of a broader pattern of cyber threats that have been targeting the country. In April, for instance, South Korean security services identified North Korean Advanced Persistent Threat (APT) actors Kimsuky, Andariel and Lazarus as responsible for infiltrating 83 defense companies and stealing data from 10 of them between October 2022 and July 2023.[3] Another North Korean cyber threat activity cluster called DEV#POPPER has allegedly targeted software developers by using multiple malware to manipulate the developers into divulging confidential information.

The attack sources aren't limited to North Korea only. Earlier this year, threat intelligence company Cisco Talos identified a suspected Vietnamese threat called CoralRaider, which allegedly targeted several Asian countries, including South Korea, to harvest financial data.[4] Similarly, China-based hacker group CyberDragon had also launched Distributed Denial-of-Service (DDoS) attacks on

---

[1] Saballa, Joe. "North Korean Hackers Breach South Korean Defense Systems, Steal Data on Tanks and Spy Planes." *The Defense Post*, August 13, 2024. Accessible at https://www.thedefensepost.com/2024/08/13/korea-tank-spy-planes/.

[2] Defense News Army. "North Korean Cyberattacks: Theft of Sensitive Data on South Korea's Military Capabilities, Including K2 Black Panther and SIGINT Aircraft." Army Recognition, August 14, 2024. Accessible at https://armyrecognition.com/news/army-news/army-news-2024/north-korean-cyberattacks-theft-of-sensitive-data-on-south-koreas-military-capabilities-including-k2-black-panther-and-sigint-aircraft.

[3] Antoniuk, Daryna. "South Korean Defense Companies Targeted in Cyber Espionage Campaign Attributed to North Korea." The Record, August 18, 2024. Accessible at https://therecord.media/south-korean-defense-companies-cyber-espionage-north-korea.

[4] Raghuprasad, Chetan, and Chen, Joey. "CoralRAT: CoralRaider Targets Social Media Accounts in South Korea." Talos Intelligence, August 16, 2024. Accessible at https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts

government and financial institutions, as well as Incheon airport, over South Korean support of Ukraine.[5]

While the cyberattacks mentioned above have certainly made 2024 an eventful year for South Korean cybersecurity, the country is not a stranger to being a target of such attacks. South Korean economy has been supported by and is now driven by, a highly proliferated digital infrastructure, which also implies cyber-attack vulnerabilities. These vulnerabilities have become especially accentuated due to hostilities with North Korea, which has used its limited resources to develop some of the most notorious APT threats. Of course, North Korea is not the only country which has targeted South Korea; a growing number of cyber-attacks on South Korea have found their origins in countries like China, Russia and Iran, as well as internal sources.

South Korea has also been proactive in its endeavours to secure its cyberspace. The pivot to knowledge-based industries, the spread of online documentation and banking, and the rising threat to digital infrastructure led South Korea to lay the foundation of its cybersecurity framework in the 1980s. They have kept a cybersecurity strategy continuously in place since 2009.[6] Therefore, South Korea has an advanced cybersecurity infrastructure, and the Global Cybersecurity Index by the International Telecommunications Union (ITU) ranked it as the 5th best in the world. Yet, as seen with the reports of successful attacks on the country's critical infrastructure this year alone, the country's cyber capabilities seem to be riddled with severe vulnerabilities. From the socio-economic, political, and national security perspective, the losses incurred due to this virtual siege make it extremely important to study the vulnerabilities posited in cybersecurity in South Korea, despite the efforts to curb them. In this context, this issue brief will attempt to briefly discuss the South Korean cybersecurity framework and provide an overview of its extant issues.

Cybersecurity framework in South Korea: An overview

South Korea's odyssey into securing its digital space started in the 1980s, although it will be overestimated to call it cybersecurity. In 1988, for instance, South Korea developed its first 'computer vaccine' following the attack by the Brain virus (which targeted the boot systems of IBM computers). South Korean government also started leveraging the internet to ease administration and governance through documentation security and online service for issuing

[5] Murthy, Krishna. "CyberDragon Hacking Group Targets South Korean Sites." *The Cyber Express*, August 15, 2024. Accessible at https://thecyberexpress.com/cyberdragon-hacking-group-south-korean-sites/.

[6] Cavanaugh, Luke. "South Korea's 56 Hours of Paralysis Is a Cyber Resilience Cautionary Tale." GovInsider, August 21, 2024. Accessible at https://govinsider.asia/intl-en/article/south-koreas-56-hours-of-paralysis-is-a-cyber-resilience-cautionary-tale.

resident registration documents in 1991. In 1992, the Act on the Promotion of Information and Communications Network Utilization and Information Protection (also known as the Network Act) guaranteed the security of personal information of any consumer using information and communications services.

However, it should be noted that these steps offered limited protection to details of documentation stored ON the network; the network's security did not become a consideration till the 1990s. One of the plausible reasons for this is that cyberspace, around this time, was a limited resource due to high entry barriers in terms of costs and feasibility of establishing networks. This changed in the 1990s due to the advent of the World Wide Web (WWW) in 1991. WWW enabled fragmented networks in academic and strategic institutions to come together and further expand at a level wherein it could be commercialized. For South Korea, this meant being able to make the Internet public in 1994. By 1997, the country had been a forerunner in internet speeds, providing one (1) Mbps broadband speed at the national scale. The push by the state towards growing internet infrastructure led to a boom in the proliferation of the internet and its related services. By 2002, nearly 70 percent of the households and all schools in South Korea had access to the internet.[7]

Coinciding with these developments, North Korea also established its cyber capabilities. In 1986, the administration established Mirim School, aimed at using support from the erstwhile USSR to train 'cyber warriors'.[8] By 1995, South Korea had started honing its offensive capabilities through resources gathered in 'electronic intelligence' by the People's Liberation Army (PLA).

These developments, combined with an increasing number of international cyberattacks, led South Korea to begin taking steps to secure its networks comprehensively. From this point on, the evolution of South Korean cybersecurity can be seen through four general phases, primarily marked by the sophistication in response to an escalation by North Korea.

The First Phase (1995 – 2009): The first phase was marked by the formation of the Korea Internet Safety Commission (KISCOM), with a directive to regulate online content and purge any 'illegal or harmful' content.[9] In 1996, the Korea Information Security Agency developed

[7] Hwang, Jo-Sung. "South Korea." In *Digital Review of Asia Pacific 2003/2004*, 2003, pp. 140–149. Accessible at, https://digital-review.org/uploads/files/pdf/2003-2004/140_149_Korea_Final_May.pdf.

[8] "A Look at Mirim College, Hotbed of Cyber Warfare", *Daily NK*, May 06, 2011, Accessible at, https://www.dailynk.com/english/a-look-at-mirim-college-hotbed-of/

[9] Chung, T. J. "Policing Internet Fraud: A Study of the Tensions between Private and Public Models of Policing Fraudulent Activity in Cyberspace with Particular Focus on South Korea and Special Reference to the United

technologies to protect the internet, evaluate security systems such as commercial firewalls, protect personal data, and raise general awareness regarding internet security. Network Act also saw a significant revision in 2001, with the express purpose of securing the burgeoning digital space within the country. Beyond the mandates on data collection, protection of personal information, user rights, grievance redressal and dispute resolution, the Network Act 2001 also gave the Ministry of Information and Communication the power to establish guidelines for safe and reliable information and communications networks. South Korea also developed its indigenous 128-bit encryption technology called SEED cryptology to secure its online banking system, which later expanded to all other major public websites.[10]

In 2004, following a cyber-attack that led to widespread internet disruption the previous year, the National Cyber Security Centre under the National Intelligence Service (NIS) was established, with a new control tower called Korea National Computer Emergency Response Team (KN-CERT) functioning under it. Reporting of any hacking attempt was made mandatory. The scope of the cybersecurity framework was also divided clearly, with NIS managing the public sector and the Ministry of Science and ICT (MSIT) undertaking private entities. Finally, initiatives like Cyber21 and e-Korea Vision were launched to make South Korea an internet powerhouse to develop cybersecurity. However, these steps did not shape or form a cohesive cyber strategy.[11]

The Second Phase (2009 – 2013): The second phase began with Chinese agents' January 2008 hack of eBay Korea's Auction Co. servers, which led to a data leak of 18.07 million users. The legal apparatus at the time was insufficient to hold companies accountable for improper firewalls and encryptions, which the Supreme Court used as a basis to acquit the company of all charges. This attack was followed by the 2009 DDoS attack, allegedly by the North Korean APT group Lazarus. South Korean and U.S. government and financial websites were systematically crashed by generating millions of requests per second. This further underscored the deficiency in the cybersecurity framework and the need to consolidate and improve it. In pursuance of the ideal of

Kingdom and the United States." Doctoral thesis, School of Law, University of Leeds, December 2008. Accessible at, https://etheses.whiterose.ac.uk/1010/

[10] Yeo, S., A. S. Birch, and H. S. Bengtsson. "The Role of State Actors in Cybersecurity: Can State Actors Find Their Role in Cyberspace?" In *National Security and Counterintelligence in the Era of Cyber Espionage*, edited by E. Silva, Hershey: Information Science Reference, 2016. pp. 217–246.

[11] Kim, So-jeong, and Sunha Bae. "Korean Policies of Cybersecurity and Data Resilience." In *The Korean Way with Data: How the World's Most Wired Country Is Forging a Third Way*, edited by Evan A. Feigenbaum and Michael R. Nelson. Washington, DC: Carnegie Endowment for International Peace, 2021. Pp. 39–60

'micro-government', the incumbent President, Lee Myung-bak, decided to rationalize the multiple governance institutions. Thus, the Ministry of Communications was dissolved, and ICT was integrated across ministries. Additionally, The Korea Internet and Security Agency (KISA) was formed after combining the Korea Information Security Agency (KISA), the National Internet Development Agency (NIDA) and the Korean I.T. International Cooperation Agency (KIICA). His presidency also saw the passing of the Personal Information Protection Act in 2011 and the establishment of the Army Cyber Command under the Ministry of Defense for cyber warfare against North Korea.

This phase is also the first time we see South Korea developing its first cybersecurity strategy. The 'National Cyber Crisis Comprehensive Countermeasures' in 2009, as well as the National Cyber Security Master Plan in 2011 (formed after a North Korean attack on Nonghyup Bank), were formulated as a roadmap for the country to respond against cyber-attacks by North Korea. The National Cybersecurity Masterplan, in particular, attempted to clarify the roles of cybersecurity agencies while boosting national defense measures. However, these were not comprehensive enough to be called 'strategic policy visions', as they had a limited mandate.

The Third Phase (2013 – 2019): This phase marked the launch of policy measures in response to the March 20 and the June 25 cyber-attacks. The June 25 cyber-attack, which saw North Korea use the malware known as DarkSeoul, followed a different pattern from the previous attacks. Firstly, they had not just targeted government offices, telecom companies and banks but had hacked into the Presidential Office website itself, leaking data of political party members, military personnel, and other users. Secondly, this attack obfuscated its origins, with South Korea earlier presuming it to be the work of hacktivists. The correction in attribution was possible only after similarities were found in Darkseoul with other known North Korean malware.

The attack led to the announcement of the second iteration of Comprehensive Countermeasures, aimed at developing the ROK's cybersecurity workforce, governance, and market and improving critical infrastructure protection (CIP) information sharing.[12] Under the new system, the Presidential Office undertook a central role in all cybersecurity efforts, with the Chief of Future Strategy responsible for day-to-day activities and the National Security Office responsible for crisis events. It should be noted that the attacks on Sony Pictures in June 2013 also marked the usage of

[12] Ebert, Hannes, and Laura Groenendaal. *Cyber Resilience and Diplomacy in the Republic of Korea: Prospects for EU Cooperation.* EU Cyber Direct, 2020.

economic penalization as a response to cyberattacks for the first time, as the U.S. put sanctions on North Korea due to the latter's alleged role as being 'centrally involved' in the cyber-attack.

In 2014, following an attack on Korea Hydro & Nuclear Power Co., Ltd. (KNHP), South Korean efforts to protect their cyberspace were revitalized. Cyber-attacks were a serious threat in the National Security Strategy 2014. The NIS announced that its third department will undertake "monitoring of cyberspace and telecommunications" to protect networks in the country. They also attempted to create better coordination regarding cybersecurity responses by appointing a dedicated officer in the National Security Council, which functions directly under the President of South Korea.[13]

At the same time, the period saw a strategic shift in the outlook towards cyber-capabilities. The Ministry of Defense specifically articulated the need to develop cyber-offensive capabilities, recognize cyberspace as a future battlefield, and integrate cyber warfare functions within the military to counter North Korean nuclear facilities.

While the policy announcements were made post-haste for cybersecurity, response efforts faced delays and political hurdles. Political disputes repeatedly stalled legislative efforts to strengthen cybersecurity. For instance, the bill for the National Cyber Terrorism Prevention Act introduced during the 19th National Assembly lapsed with the expiration of the term of office. Similar attempts in 2016 and 2017 also saw bipartisan favour for creating cybersecurity law but opposition to what that would entail.

The Fourth Phase (2019 – Ongoing): The ongoing fourth phase has been marked with continuities and discontinuities. The evolving nature of cyberattacks, targeting financial theft and intellectual property, necessitated a shift from reactionary policies to comprehensive strategies in South Korea. Attacks on cryptocurrency exchanges and intellectual property, such as those on CoinRail, Bitthumb, and Samsung, highlighted the need for this change.

The first sign of the changing nature of the cybersecurity framework was seen in the 2019 Defense Task Report, which skipped mentioning North Korea as the enemy for the first time. It called for diversifying its foreign policy beyond focusing on one country and blamed strong-arm diplomacy

[13] Kim, So-jeong, and Sunha Bae. "Korean Policies of Cybersecurity and Data Resilience." In *The Korean Way with Data: How the World's Most Wired Country Is Forging a Third Way*, edited by Evan A. Feigenbaum and Michael R. Nelson. Washington, DC: Carnegie Endowment for International Peace, 2021. Pp. 39–60

for instability. It also recognized the dangers of transnational and non-military threats, including cyber threats. This prefaced the fourth phase's initial character, further solidified as South Korea launched its first National Cybersecurity Strategy in April 2019.

With a vision of creating a 'free and safe cyberspace to support national security', promoting economic prosperity, and contributing to international peace, the National Cybersecurity Strategy was a marked departure from previous Countermeasures as it focused not on response against North Korea, but instead on strengthening its internal capabilities. It recognized several pitfalls of the previous approach, particularly in inculcating cybersecurity behaviour (businesses, for instance, did not view cybersecurity as an asset but as a cost, which changed how investments were made in it). The actors it considered in its purview were not limited to one entity but expanded to include state-sponsored criminal and terrorist groups along with malicious actors, thereby broadening its scope.[14] In particular, the National Cybersecurity Strategy was followed by a Basic Plan, which laid a comprehensive roadmap to strengthen the cybersecurity framework across policy and technical goals.

The focus on internal capacity building continued throughout the COVID-19 years, especially since the pandemic had led to an escalation in cyberattacks. The Korean New Deal, brought in response to the COVID-19 pandemic, refers to growing dependency on ICT technology. Its components, the Digital New Deal (2020) and Digital New Deal 2.0 (2021) have weighed heavily on more robust cyber secure systems. The Digital New Deal as a policy aims at "stronger integration of DNA (data, networks, and artificial intelligence) throughout the economy", while Digital New Deal 2.0 expanded the scope of cybersecurity to include other emerging computational technologies such as Metaverse, 6G and others.

The Yoon Seok-yeol government has continued highlighting cybersecurity as an important aspect of national security, deeming it a 'strategic industry'. However, the administration has forgone the neutrality shown towards North Korea in the initial part of the fourth phase. The Defense White Paper, published in 2023, explicitly mentioned North Korea as the 'enemy'.[15] Regarding

[14] Republic of Korea. *National Cybersecurity Strategy*. National Security Office, 2019. Accessible at, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf

[15] Kim, Hyun-jin. "South Korea Defense Report Revives 'Enemy' Label for North." *The Diplomat*, February 2023. https://thediplomat.com/2023/02/south-korea-defense-report-revives-enemy-label-for-north/.

cybersecurity, the paper highlights the need for cooperation with the U.S. to oppose North Korea, which is a significant departure from the previous approach.

This was further underscored with the launch of the 2024 National Cybersecurity Strategy. Although the document does acknowledge other sources of cyber threats, North Korea was mentioned in adversarial terms twelve times throughout the document.[16] The new strategy specifies the need for offensive cyber capabilities and enhanced resilience. Another departure from the 2019 National Cybersecurity Strategy is the recognition of international and state-sponsored hacking organizations as primary threats.

The strategy highlights issues such as advanced technology leakage, election interference, attacks on critical infrastructure and ransomware attacks as serious threats to national security. The strategy also explicitly underscores the need for collaboration with like-minded nations and allies to identify threats and raise cyber capabilities to counter them. This is especially relevant, as South Korea will soon join the ranks of non-permanent members of the U.N. Security Council. Finally, it specifies the creation of a separate "National Cybersecurity Commission" for cybersecurity governance, which will function alongside the National Intelligence Service to ensure a seamless integrated response.

Evaluating Major Issues in Cybersecurity Governance

Despite the various policy measures taken for cyber security and the focus on increasing cyber capabilities, the South Korean cyber security framework has not been able to ward off attacks successfully. Perhaps the most prolific reason South Korea is victim to cyberattacks is its geography and geopolitics. South Korea's antagonistic relationship with its northern counterpart has lasted for decades, and cyberspace has become an avenue for rivalry. A factor against South Korea is its unique geographic position bordering North Korea, making it especially vulnerable to some types of cyber-attacks. For instance, regarding numerous GPS attacks against the South allegedly carried out by the North, geography has a vital role to play. In the 2012 GPS attacks, the jamming signals were identified as coming from Kaesong in North Korea, about 10 km from the border and 50 km from the Incheon International Airport. Additionally, North Korea has leveraged its lack of internet networks against South Korea's ubiquitous connectivity, as while it

[16] Republic of Korea. *National Cybersecurity Strategy*. National Security Office, 2024. Accessible at https://www.president.go.kr/newsroom/press/gdXzwtKB.

can use its undercover cells spread across China, Russia, Southeast Asia and Europe to attack through their server, there is little in the way of target within North Korea itself.

Another issue South Korea faces is the lack of a reasonable ground against North Korea to create deterrence. North Korea has been conducting 'psychological operations' since 2000, with cyberattacks as a component.[17] For North Korea, each cyberattack does not just serve the obvious purpose of data or currency theft but also leads to the destabilization of public opinion and trust in South Korea's institutions. South Korea's tendency to immediately point fingers at North Korea as soon as a cyberattack occurs is also an issue, as there is no threat of a bilateral repercussion. After all, since North Korea is isolated and will be implicated in an attack anyway, not to mention South Korea is a lucrative source of both income and technology. There exists no disincentive for them not to attack South Korean infrastructures.

Compounding this issue, While North Korea is the first to receive suspicion for cyberattacks, it is difficult to blame them or hold the attackers accountable officially. This is due to two major reasons. One, cyberattacks are easy to deny and difficult to attribute. Unless a state finds decisive evidence or accurate proof of the attack, it must rely heavily on circumstantial evidence to assign blame. Secondly, North Korean cyber-attacks generally come through other countries' servers, particularly Russia and China. Yet, the two countries (especially the latter) have been uncooperative with South Korean investigations and have been actively involved as a cyber threat.[18] Thirdly, while the South Korean National Cybersecurity Strategy (2019 and 2024 iteration) outlines detecting and countering threats, they have not mentioned any legal or institutional mechanism to enforce accountability and create deterrence. The government-led investigations evaluate the reason and background of attacks, and if the culprit is North Korea, ROK goes only as far as publicly attributing it. Yet, there has been no prosecution or separate sanctions on perpetrators. While the 2024 document does talk about coopting international standards, this will not be possible unless substantive mechanisms are in place to enforce them.

While numerous external pressures exist, South Korean cyber security is also plagued by internal issues. The most prolific cyber security governance in South Korea is its fragmented nature.

---

[17] Hewlett-Packard Security Research. *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape.* Hewlett-Packard Development Company, 2014. Accessible at, https://www.slideshare.net/slideshow/profiling-an-enigma-the-mystery-of-north-koreas-cyber-threat-landscape/73358820

[18] Park, Donghui. *Cybersecurity Spotlight: South Korea.* 2016. Accessible at https://jsis.washington.edu/news/cybersecurity-spotlight-south-korea

Multiple agencies deal with different aspects of cybersecurity and the constellation of different laws for each domain and industry. While the creation of nodal agencies and a single cybersecurity law has been attempted (the 2024 National Cybersecurity Strategy also explicitly mentions a dedicated law), it has been unsuccessful due to power contestations regarding each agency's domain.

A key reason for this deadlock is the widespread distrust in the government, rooted in historical factors. Past authoritarian regimes in South Korea misused the National Intelligence Service (NIS) and the military, leading to public concern over the concentration of power in these institutions. This distrust is exacerbated by allegations that the NIS has used social media to promote the ruling party and has a history of acquiring hacking tools potentially used for illicit surveillance. This lack of trust is further deepened by the government's inconsistent approach to the NIS's powers. The current system is proving impractical as cyberspace increasingly integrates public, private, and military domains.

The policies in South Korea have also been relatively laggard in keeping up with the technological advancements in the country. The National Cybersecurity Strategy documents of South Korea have come several years later compared to similarly digitally connected countries. More than that, it fails to address several core issues plaguing cybersecurity governance. Both documents had also established major goals for themselves in terms of cybersecurity policy. The 2019 document had come with a Basic Plan that, while riddled with a consistent legal foundation to be followed by the institutions, did create a framework for a comprehensive cybersecurity policy. The 2024 document, on the other hand, has yet to provide any such framework.

Finally, South Korean cybersecurity practices are still largely dominated by military and government perspectives. The recent attacks on Coinrail (2018), Bithumb (2018), and Upbit (2019) for financial profits, Universities for patent and intellectual property, and even hospitals (Seoul National University Hospital, 2021) for patient information have underscored the need for South Korean government to increase the scope of cybersecurity to the economy as well. However, there is a disconnect between the economic sector and government/military, so firefighting seems to be the only response the country can muster against attacks on private and civilian infrastructure.

CONCLUSIONS

The sheer magnitude of cyberspace's role in the country's developmental story has meant that cybersecurity is imperative for South Koreans' perception of security. South Korea's ROK economy experienced remarkable growth over the past decades - from a GDP per capita of around $160 in 1960 to over $30,000 in 2018 – with the knowledge industry as the focus of its production since the 1990s. This success in ICT is not random but primarily driven by the country's push in the knowledge industry, particularly based on hardware such as semiconductors, flat panel displays, etc. Heavy reliance on ICT in a wide range of sectors, especially critical infrastructure, has painted a large target on the country for cyberattacks that may disturb their normal functioning. South Korea is mindful of this reality and has instituted countermeasures to secure cyberspace.

While, in theory, South Korea's attempt at creating a robust cybersecurity framework has been successful, the country has also been victim to several attacks on its critical infrastructure. Structural problems internally due to fragmented policy, political differences, and in-silos approaches to public, private and military cybersecurity aspects constitute internal shortfalls in the framework. At the same time, the hyper-focus on North Korea (while slightly justified, given the quantum of attacks coming from the country) has led to tunnel vision in policy approaches as new cyber threats emerge from other States (China, Iran, Pakistan, Russia), as well as Non-State Actors.

Cybersecurity in South Korea requires balancing several critical factors: organizational roles against public trust, the rapid spread of the internet against increased vulnerability, geopolitical tensions against globalized threats, evolving threat landscapes, and the need for self-reliance versus dependence on U.S. involvement. While initial efforts to secure servers have led to ongoing cybersecurity initiatives, these efforts have been hindered by fragmented laws, policies, institutions, trust deficits, power struggles, and an overemphasis on North Korea. The absence of comprehensive legal frameworks and persistent external threats, mainly focusing on North Korea, has undermined the effectiveness of the National Cybersecurity Strategy.

MEGHNA PRADHAN is a PhD scholar in East Asian Studies at the University of Delhi. She holds a Master's in East Asian Studies from the same university and an MPhil in Korean Studies from Jawaharlal Nehru University, where she researched South Korea's cybersecurity governance. Her interests include emerging computational technologies, tech artifacts in global politics, governance, and non-traditional security. She is a NASC fellow (2024-25) at the Takshashila Institution and a Research Assistant at the Manohar Parrikar Institute for Defense Studies and Analysis (MP-IDSA).

The views expressed in this article are personal.

The Society for the Study of Peace and Conflict (SSPC) is an independent, non-profit, nonpartisan research organization based in New Delhi, dedicated to conduct rigorous and comprehensive research and work towards disseminating information through commentaries and analyses on a broad spectrum of issues relating to peace, conflict and human development. SSPC has been registered under the Societies Registration Act (XXI) of 1860. The SSPC came into being as a platform to exchange ideas, undertake quality research, and ensure a fruitful dialogue.

Published by:
Society for the Study of Peace and Conflict.
Post Box: 10560,
JNU Old Campus, New Delhi-110067.
Website: www.sspconline.org
https://x.com/sspconline
https://www.facebook.com/sspconline

We welcome your feedback. Email your comments at "sspconline@gmail.com"

Designed and typeset by Excel Solutions