

Issue Brief

Vol.106, No.3, 2024

ROK's New National Cybersecurity Strategy and Its Implications

So Jeong Kim
(Senior Research Fellow, INSS)

Abstract

Recently, ROK has been actively responding to economic, technological, and cyber security issues. In line with this, on February 1st, the "National Cybersecurity Strategy" was revised to accommodate the evolving cyber landscape and expand its strategic scope. By openly disclosing the nation's cyber security strategy and policies to ensure transparency, safety, openness, and responsible use of cyberspace, this also aims to demonstrate transparency in policies regarding inter-state cyber space usage, as demanded by the UN Group of Governmental Experts (GGE) on Cyber Security. The revised strategy embodies three main features. Firstly, it clearly delineates the threat actors in cyberspace and commits to consider more active stance to counter malicious cyber activities. Secondly, it reaffirms the responsibility of our country as a Global Pivotal State to fulfill obligations and contribute to the international community, while enhancing cooperation as responsible users of cyberspace, specifying the identification, coercion, and joint response to malicious actors. Thirdly, it concretely outlines the domestic cybersecurity governance to enforce these efforts, specifying relevant institutional improvements. To implement the revised strategy, several steps are essential. Firstly, detailed plans for strategy implementation need to be devised. Secondly, our stance on various issues must be clearly communicated to the international community. Thirdly, objective assessment data on the status, strengths, weaknesses of cooperating partner countries must be secured. Fourthly, theoretical and practical foundations to take aggressive strategies need to be developed.

Keywords

National Cybersecurity Strategy, offensive cyber, cyber resilience, cyber capacity building, joint response to cyber threats

ROK's New National Cybersecurity Strategy and Its Implications

So Jeong Kim

(Senior Research Fellow, INSS)

To ensure transparent, secure, open, and responsible use of cyberspace, countries publish national cybersecurity strategies in line with Confidence Building Measures (CBMs) advocated by the United Nations Group of Governmental Experts (GGE) on cybersecurity. For example, South Korea publicly released its first national cybersecurity strategy in 2019 and recently published a revised version under the oversight of the National Security Office.

The new strategy has three main features: Firstly, it underscores the importance of identifying cyber threat actors and acquiring offensive capabilities to counter malicious activities, including hybrid threats, while ensuring the seamless operation of critical IT functions and enhanced resilience. Secondly, South Korea commits to fulfilling its responsibilities by contributing to the international community as a global pivotal state emphasizing cooperation, responsible use, and joint responses to malicious actors. Thirdly, the strategy outlines domestic cybersecurity governance led by the "National Cybersecurity Commission" and the National Intelligence Service, along with specific institutional improvements to support such agencies. In the following sections, the author will examine the features of South Korea's revised National Cybersecurity Strategy and the implications thereof.

Features of the 2024 National Cybersecurity Strategy

The vision presented by ROK's 2024 National Cybersecurity Strategy is to become a "global pivotal state that fulfills its international role and responsibility while defending the values of freedom, human rights, and the rule of law in cyberspace." To fulfill such a vision, the strategy outlines five strategic tasks – bolstering offensive cyber defense operations; building global cooperation mechanisms; enhancing cybersecurity resilience of critical infrastructure; securing a competitive edge in emerging technologies; and strengthening South Korea's integrated response capability.

The new strategy explicitly underscores the importance of identifying cyber threat actors and securing offensive capabilities in responding to malicious cyber activities. One significant change from the 2019 National Cybersecurity Strategy is the recognition of international and state-sponsored hacking organizations as primary threats, and specifying serious national security threats such as advanced technology leakage, election interference, incapacitation of critical infrastructure, ransomware attacks, and growing threats to supply chain security. It underlines North Korean cyberattacks as South Korea's immediate threat, stating, "To effectively respond to the malicious cyber activities, such as the theft of classified information, dissemination of false information, and cryptocurrency theft perpetrated by North Korean threat actors, merely reinforcing defense capabilities has its limitations." By confronting its most significant and practical threat – North Korean cyberattacks – ROK's new cybersecurity strategy clearly defines national security threats and interests, establishing the basis for response measures to security infringements.

In particular, the revised strategy explicitly outlines the goal of

minimizing damage against cyber incidents and ensuring the stable and continuous provision of IT services by securing resilience for the stable operation of critical functions and public protection. This demonstrates a determination to proactively respond to malicious activities while securing resilience to curtail damages and ensure sustainability.

Secondly, the new strategy highlights close collaboration with allies and like-minded nations to secure offensive cybersecurity capabilities against cyber threats and establish global leadership. Building on the U.S.–ROK Strategic Cybersecurity Cooperation Framework, the strategy explicitly declares South Korea's participation and contribution to secure a safe and reliable cyberspace based on universal values shared by the international community, the U.S., Japan, the UK, and like-minded countries in the Indo-Pacific region. South Korea seeks to engage in joint responses with the global society, sharing values of freedom, openness, safety, and peace in cyberspace. As a global pivotal state, South Korea aims to clearly articulate its position in establishing norms regulating responsible behavior in cyberspace, actively participating in multilateral cooperation agreements against cybercrimes, promoting the formation of a norm-based cyberspace order, reaffirming the responsibilities of transit countries in cyberattacks, and actively contributing to global cyber threat responses.

In addition, the strategy stipulates South Korea's response operations against international and state-sponsored hacking organizations, as well as North Korea's malicious cyberattacks. ROK's response against cyberattacks in adherence to its national deterrence strategy includes scientific and reliable investigations, identification of attackers, proportional response, and joint security advisories with like-minded countries. This is in line with the U.S. and EU, which have already established domestic and

international standards and procedures and implemented various response measures such as financial sanctions, prosecutions, and expulsions. It marks the most significant difference from the 2019 National Cybersecurity Strategy, displaying a stronger commitment to international cooperation based on value-based rules and increased collaboration with allies and like-minded countries. Ultimately, it underscores South Korea's determination to block, deter, and prevent North Korea's cyber threats and enhance cybersecurity capabilities.

Furthermore, the strategy demonstrates South Korea's will to fulfill its role and responsibility as a global pivotal state by diversifying channels and targets of international cooperation, promoting Cyber Capacity Building (CCB), expanding its scope, and providing support to other countries, in line with its 2022 Indo-Pacific Strategy.

Thirdly, the strategy has provided a foundation for the national cybersecurity governance scheme by defining the roles and responsibilities of the National Security Office and crisis management agency. The strategy positions the National Security Office at the center, calling for the establishment of the "National Cybersecurity Commission" and an integrated response organization. Subsequently, it specifies the revision of relevant laws and regulations, particularly the enactment of the "Cyber Security Act" to provide a legal basis for securing the institutional foundation for cybersecurity governance. In addition, the strategy proposes measures for capacity-building and public-private cooperation including the development of source and core technologies, effective training of specialized personnel, and information and intelligence sharing of cyber threats.

Implications

First, the strategy needs the support of detailed policies, including a concrete implementation roadmap, designated roles and responsibilities of agents, and specific plans. Considering the evolving threat scenarios and global cooperation dynamics with the heightened threat from North Korea and expanded cooperation between North Korea, Russia, China, and Iran, it is imperative to evaluate and develop tailored response strategies based on the distinct characteristics of each country. Additionally, a comprehensive and objective assessment of the effects resulting from the implementation of the 2024 National Cybersecurity Strategy is necessary, along with considerations for avenues of improvement to be incorporated in the third version five years later.

Second, clear communication of South Korea's stance on global issues and greater policy transparency are crucial for shaping international norms and alliances. The government must also share and coordinate information on the global projects distributed across ministries while analyzing the strengths and weaknesses of global discussion bodies. South Korea's national capabilities and international influence differ significantly from the past. For the 2024–2025 term, South Korea will serve as a non-permanent member of the United Nations Security Council, with a mandate to focus on cybersecurity issues. Such activities should align with its National Cybersecurity Strategy to derive optimum results while considering changes in the geopolitical environment and threat landscape. With an integrated incident response system, South Korea will be able to deter North Korea's malicious use of cyber activities as a global pivotal state.

Third, South Korea needs to formulate strategies based on objective assessments of the cybersecurity status, merits and

demerits, and demands of cooperating countries when engaging with allied and like-minded states. Such preparations will help streamline the coordination and implementation of policies, rules of engagement, and compliance guidelines that enable substantial cooperation. Additionally, the ROK must ensure that its policies, rules of engagement, decision-making criteria, and systems are based on its national security strategy and national cybersecurity strategy to avoid the unilateral adoption of foreign policies and standards.

Fourth, while opting for an offensive strategy may be justified in certain situational contexts, logical and theoretical discussions and justifications are essential to avoid misconceptions about aggression in cyberspace. It is crucial to internally and externally clarify that the ROK's focus on strengthening preemptive and offensive capabilities is to proactively respond to and deter possible threats. Given that the U.S., as an allied nation, explicitly outlines the continuation of persistent engagement and defend forward strategies in its 2023 National Cybersecurity Strategy and Department of Defense Cyber Strategy, it is essential to articulate the direction of South Korea's proposed offensive strategy and provide clear reasoning for its approach.

The views and opinions expressed in this report are those of the author(s) and do not necessarily reflect the official position of INSS.