



UNIDIR

RESEARCH PAPER SERIES – PAPER 6

International Cyber Operations: Doctrines and Capabilities of the Republic of Korea

SO JEONG KIM



Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study was produced by an external consultant, contracted to produce studies for the Security and Technology Programme's Cyber Stability workstream, which is funded by the Governments of Australia, Canada, Czechia, France, Germany, the Netherlands, Norway, Singapore, Switzerland, the United Kingdom and the United States of America, and by Microsoft.

Gratitude is extended to Kuyoun Chung (Kangwon National University), Sunha Bae (National Security Research Institute, Republic of Korea), Giacomo Persi Paoli (UNIDIR) and an anonymous representative of the Government of the Republic of Korea for providing their thoughts on this paper.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the Government of the Republic of Korea, United Nations, UNIDIR, its staff members or sponsors.

Author

So Jeong KIM is the Director of Emerging Security Studies and a Senior Research Fellow at the Institute for National Security Strategy (INSS), Republic of Korea. She is also an Adjunct Fellow (Non-resident) of the Center for Strategic and International Studies (CSIS), United States. The report reflects the state of affairs as of July 2025.

Contents

Acknowledgements	2
1. INTRODUCTION AND SCOPE	5
<hr/>	
2. DOCTRINE: STRATEGIES, POLICY DOCUMENTS AND REGULATION	6
<hr/>	
2.1 Strategies and policies	6
2.1.1 The 2024 National Cybersecurity Strategy	6
2.1.2 Top 120 National Tasks of the Yoon Administration	7
2.1.3 The 2019 National Cybersecurity Strategy	8
2.1.4 Comparing Cybersecurity Strategies across Administrations	8
2.2 Laws and regulations	9
2.3 The 2023 Defense White Paper and efforts on the military	11
2.4 National Position of the Republic of Korea on the Application of International Law in Cyberspace	12
3. CAPABILITIES AND ORGANIZATIONAL FRAMEWORK	13
<hr/>	
3.1 Cyber Operations Command	13
3.2 Human capacity	15
4. CONCLUSION	16
<hr/>	
5. REFERENCES	18
<hr/>	



Credit: © DC Studio/Shutterstock.com

On the Research Paper Series

The number of States possessing the capability to conduct international cyber operations against or through foreign information and communications technology (ICT) infrastructure is on the rise. These cyber operations can signal a mounting large-scale threat to the security of a State, could be understood as a violation of sovereignty and may lead to an escalation.

To facilitate transparency, advance trust among States and thus promote stability in international cyberspace, the UNIDIR Security and Technology Programme commissioned a series of research papers outlining national capabilities to conduct international cyber operations and the relevant national doctrines regulating the conduct of such operations. In the resulting papers, nine scholars and practitioners provide an overview of the capabilities and doctrines of 15 States across different regions: Australia, Brazil, Canada, China, France, Germany, India, the Islamic Republic of Iran, Israel, Japan, the Republic of Korea, the Russian Federation, Saudi Arabia, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

To read more about the research paper series, please refer to the “International Cyber Operations: National Doctrines and Capabilities” paper, available at www.unidir.org/cyberdoctrines.

Andraz Kastelic

Lead Cyber Stability Researcher

Security and Technology Programme, UNIDIR

1. Introduction and scope

Cybersecurity capabilities encompass a spectrum of defensive and offensive measures. Various assessments, such as the Global Cybersecurity Index of the International Telecommunication Union (ITU), recognize that the Republic of Korea has a robust defensive posture, which is reflected in strong legal frameworks and international cooperation. In contrast, it is significantly harder to accurately evaluate its capabilities to conduct international cyber operations or its offensive cyber capabilities.¹ The inherent secrecy surrounding offensive cyber operations, coupled with the lack of publicly attributed operations, shrouds these capabilities in ambiguity.

This inherent opacity is further compounded by the diverse perspectives and priorities of different evaluating bodies. While some organizations (e.g. the Australian Security Policy Institute) assess cyber maturity holistically, focusing on such factors as policy development and societal readiness, these evaluations often prioritize defensive capabilities and cyberresilience. This emphasis on defensive aspects can inadvertently overshadow the development and deployment of offensive cyber capabilities, which are crucial for national security in an increasingly contested cyberspace.

The 2019 National Cybersecurity Strategy of the Republic of Korea acknowledged the escalating nature of cyberthreats, emphasizing the need to fortify defences and enhance resilience.² However, the more recent 2024 strategy underscored the criticality of offensive cyber power, suggesting a shift in emphasis. This transition towards a more offensive posture, while necessary in the face of evolving threats, raises crucial questions regarding the nature and scope of the Republic of Korea's offensive cyber capabilities and the doctrines guiding their use.

This paper addresses this gap in understanding by analysing available public information to deduce the offensive cyber capabilities of the Republic of Korea. By examining official documents such as the National Cybersecurity Strategy, analysing relevant laws and regulations, and investigating the structure and functions of relevant government agencies, this research sheds light on the potential scope of the capabilities of the Republic of Korea to conduct international cyber operations and the principles that are likely to govern their deployment.

1 RaonSecure, "South Korea Ranks 4th in the ITU's Global Cybersecurity Index", 6 July 2021, <https://medium.com/raonsecure/south-korea-ranks-4th-in-the-itus-global-cybersecurity-index-9f7850514c45>.

2 Republic of Korea, Office of the President, National Security Office, "National Cybersecurity Strategy", 2019, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf, p. 7.



Credit: © 3Dsss/Shutterstock.com

2. Doctrine: strategies, policy documents and regulation

2.1 Strategies and policies

2.1.1 The 2024 National Cybersecurity Strategy

The revised National Cybersecurity Strategy of 2024 recognized the need for a novel approach that is rooted in a comprehensive understanding of the inherent characteristics of the cyber domain. The document explicitly emphasizes the need to assess threat actors in cyberspace and to secure active capabilities to respond to malicious cyber activities, including hybrid threats – that is, the combination of cyber and non-cyber instruments, along with hostile cyber-enabled actions that fall below the threshold of warfare.³ It also highlights as key missions the seamless provision of essential national information and communications technology (ICT) functions and the enhancement of resilience. Furthermore, the Republic of Korea committed to fulfil its responsibilities and contribute to the international community as a central global actor, declaring strengthened responsibility and cooperation as a responsible cyberspace actor. It also declared its intent to identify and counteract malicious actors through joint responses.

3 Republic of Korea, Office of the President, “National Cyber Security Strategy in 2024”, March 2024, <https://www.ncsc.go.kr/cmm/fms/PdfFileView.do?uuid=8c65a387-32be-4969-8531-b4a04f754d70&fileSn=0>, p. 7.

The 2024 National Cybersecurity Strategy placed significant emphasis on augmenting proactive cyberdefence measures. It endeavoured to formulate and execute proactive measures against cyber-threats that impinge upon national security in cyberspace. This encompasses the active identification and analysis of the sources of foreign cyber operations, pre-emptive countering of threats through the identification, neutralization and blocking of signals that indicate an impending malicious cyber operation, and the proactive initiation of responses in a pre-emptive manner.

The executive summary of the National Cybersecurity Basic Plan mandated the Government of the Republic of Korea to develop detailed plans for implementing five strategic tasks, one of them being the “Strengthening Offensive Cyber Defense Activities”. In pursuing this strategic task, the Basic Plan aims to “Secure deterrence by conducting preemptive and proactive cyber defense activities against cyber attacks and threat actors that undermine national security and interests, and establish a foundation for responding to ‘disinformation’ that divides public opinion and causes social unrest in cyberspace”.⁴ The detailed measures for the first strategic task also aim to “establish a foundation for countering disinformation that disrupts public opinion and fosters social unrest in cyberspace”. Shin Won-sik, the Republic of Korea’s National Security Adviser, argued in late 2024 that “We’re shifting from a predominantly defensive stance to a more proactive approach (in cybersecurity) [...] The key concept is to actively detect, identify and preemptively respond to threats”.⁵

2.1.2 Top 120 National Tasks of the Yoon Administration

The Top 120 National Tasks announced by President Yoon Suk-yeol in July 2022 serves as a valuable resource for gauging the policy direction pursued by Yoon while he was in office. This document contains information that had been made public since his election as president and includes explicit emphasis on enhancing the country’s cybersecurity capabilities.

The administration articulated the reinforcement of proactive capabilities against cyberthreats and underscored the establishment of a “cyber reserve” to ensure the availability of skilled personnel for cyberwarfare. Additionally, it highlighted the creation of a strategic command centre aimed at integrating and coordinating missile capabilities, cyber and electronic warfare, and space operations. The overarching goal of this integration was to amplify strategic deterrence and response capabilities.⁶

4 Republic of Korea, Office of the President, “National Cybersecurity Basic Plan Executive Summary”, 1 September 2024, <https://web.archive.org/web/20241207235150/https://eng.president.go.kr/briefing/TE0xsLB6>.

5 Ji Da-gyum, “S. Korea Announces ‘Offensive Cyber Defense’ Strategy”, *The Korea Herald*, 1 September 2024, <https://www.koreaherald.com/article/3465045>.

6 Yoon Seok-yeol Administration’s Top 120 National Tasks—104. Enhancing Capabilities to Counter North Korea’s Nuclear and Missile Threats”, 22 July 2022, <https://www.korea.kr/archive/expDocView.do?docId=40075> (in Korean).

2.1.3 The 2019 National Cybersecurity Strategy

In response to cyberthreats in the region,⁷ the administration of President Moon Jae-in released a National Cybersecurity Strategy in 2019. This revealed the commitment of the Republic of Korea to prioritizing robust and resilient national cybersecurity, which encompassed addressing the threats to national security.

This endeavour also encompassed substantial investments in cybertechnologies incorporating artificial intelligence (AI) and big data analytics. In response to the evolving nature of cyber threats, the government has undertaken proactive measures to reinforce national cyber intelligence collection capabilities, safeguard Internet networks from disruption, and enhance the protection and resilience of critical information infrastructure. The strategy also highlights the need to further bolster the resilience of essential national services.⁸

The 2019 National Cybersecurity Strategy had three objectives:

- Seamless operation of the country's major functions
- A firm response to malicious cyber campaigns
- The establishment of a solid foundation for cybersecurity assurance

While the strategy did not explicitly mention the acquisition of direct cyber offensive capabilities, it underscored the importance of enhancing cyberattack deterrent capabilities by fostering responsive cyberattack capabilities. It specifically outlined actions such as aligning response strategies with norms of responsible State behaviour in cyberspace during significant cybersecurity threats; devising tailored countermeasures; reinforcing military capabilities; and acquiring pivotal technologies to safeguard national security and national interests in the cyber domain. The strategy also underscored the importance of training cyberwarfare specialists and nurturing responsive organizations to efficiently carry out cybersecurity initiatives.⁹

2.1.4 Comparing Cybersecurity Strategies across Administrations

The cybersecurity strategies of the Republic of Korea demonstrate both continuity in objectives and evolution in approaches.

The 2019 strategy prioritized resilience and defence, focusing on protecting critical infrastructure, investing in technologies such as AI and big data, and aligning responses with international norms. Offensive capabilities were not explicitly emphasized, with a greater focus on strengthening deterrence through defensive measures.

7 See, e.g., United Nations, Security Council, "Letter dated 3 March 2023 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council", UN Doc. S/2023/171, 7 March 2023, <https://docs.un.org/S/2023/171>.

8 Republic of Korea, "National Cybersecurity Strategy", 2019, p. 7.

9 Republic of Korea, "National Cybersecurity Strategy", 2019, pp. 8–17.

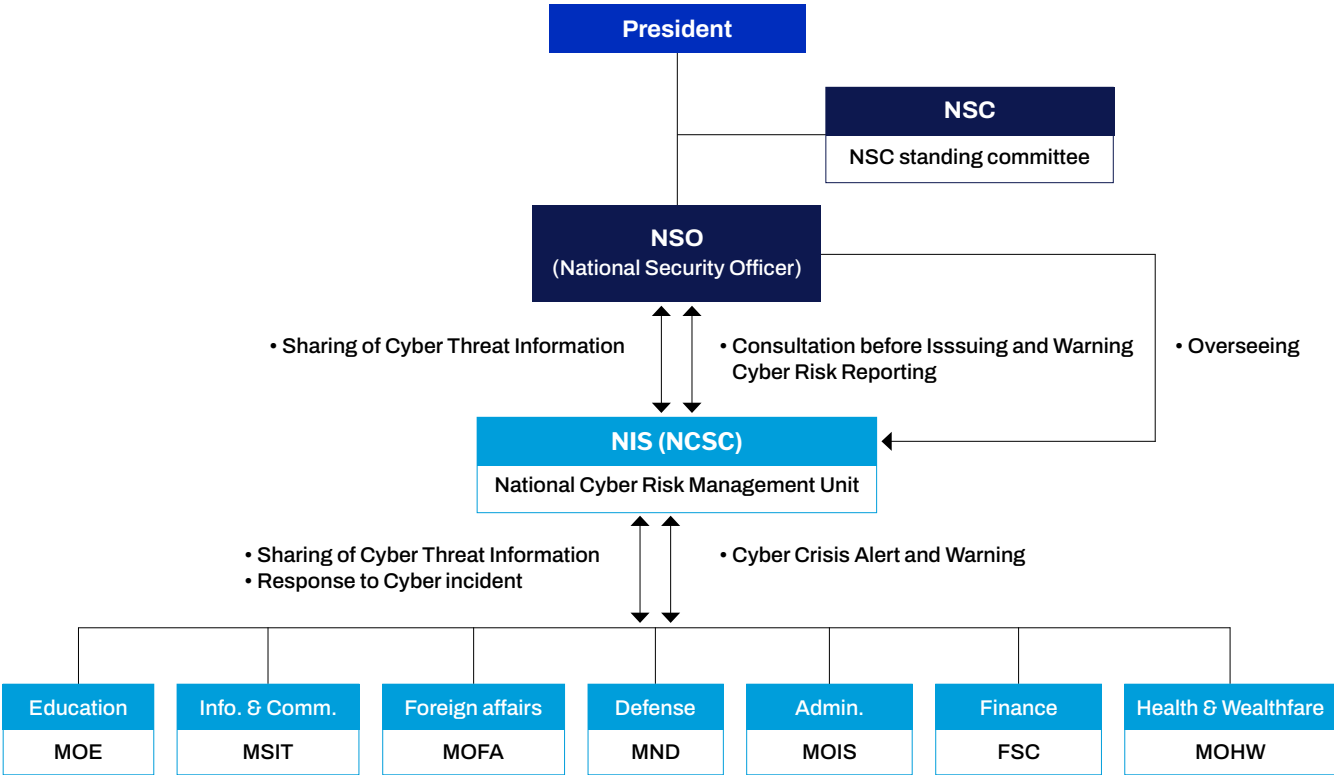
In contrast, the 2024 strategy marked a shift toward a proactive and offensive approach, emphasizing the need for pre-emptive actions to neutralize threats at their source. This includes securing offensive cyber capabilities and actively countering hybrid threats. A key difference between the two strategies is the explicit identification of the Democratic People’s Republic of Korea as a major threat in the 2024 strategy. The 2024 strategy emphasized a clear commitment to counter malicious cyber operations, further strengthening the focus on offensive cyber capabilities.

Yoon’s 2022 national tasks reinforced this shift by proposing a “cyber reserve” and integrating cyber, missile and space operations to enhance strategic deterrence. The explicit designation of a primary threat, combined with a focus on offensive capabilities, underscored the progression from a defence-centric framework to one that actively incorporates offensive cyber capabilities to address the growing complexity of cyberthreats.

2.2 Laws and regulations

The National Cybersecurity Framework of the Republic of Korea has been formulated and is operated by the National Security Office (NSO) in the Office of the President. The NSO coordinates overall cybersecurity tasks at the national level and devises and reviews medium- to long-term policy directions. A simplified overview of the country’s cybersecurity governance is illustrated in Figure 1.

FIGURE 1: CYBERSECURITY GOVERNANCE STRUCTURE OF THE REPUBLIC OF KOREA¹⁰



10 Diagram provided to the author by the Government of the Republic of Korea.

While cybersecurity governance of the Republic of Korea reflects broad coordination, individual ministries maintain distinct perspectives and priorities based on their respective roles. The Ministry of Foreign Affairs (MOFA) is committed to advancing international norms, fostering global cooperation, and promoting trust and responsible state behaviour in cyberspace. The Ministry of National Defense (MND) prioritizes bolstering offensive cyber response to malicious cyberthreats to national security. Meanwhile the National Intelligence Service (NIS), as the primary agency responsible for cybersecurity, protects the safety of citizens by collecting, preparing and distributing cybersecurity information related to international and national hacking organizations. The NIS also identifies, monitors and prevents activities committed by foreign States that infringe on national security, pursuant to the National Intelligence Service Korea Act.

The core concept of cybersecurity is to protect national security, the security of citizens and the national interest by identifying, monitoring and preventing any threat actors from undertaking activities that harm national security and the national interest while devising and implementing countermeasures. With this in mind, the government designated the NIS as the lead agency that responds to cyberthreats, as the NIS can provide cybersecurity information and can protect against cyber activities to preserve the safety of people in all parts of the country. It also established the National Cyber Risk Management Unit, a joint public-private integrated-response organization under the management and supervision of the National Security Office of the Office of the President, to provide unified efforts to protect cyber security at the national level. From a national and governmental perspective, a three-tiered cyber-defence structure has been established. At the apex, the NSO functions as the central control tower, overseeing and coordinating national cybersecurity policy and response. Beneath it, designated lead agencies within each central administrative ministry assume sector-specific responsibility, while at the operational level, frontline cybersecurity authorities manage and implement security measures within their respective domains.

Each government ministry carries out cybersecurity or information-protection activities within its respective field in accordance with the National Intelligence Service Korea Act, the Electronic Financial Transactions Act, and the Information and Communications Network Act, among others. The Republic of Korea defines cybersecurity and its implementation based on individual laws of each sector (e.g., public institutions, telecommunications, critical infrastructure, financial, military, high-tech and defence industry, healthcare, small and medium-sized enterprise, etc.).¹¹ With regard to the cybersecurity of the public sector, the relevant legal framework is provided by the National Intelligence Service Act (NISA), the Cyber Security Operational Rule (Presidential Decree), the Security Operational Rule (Presidential Decree), the National Cyber Security Management Regulation (Presidential Directive), the Electronic Government Act and the Enforcement Decree of the Public Records Management Act. In addition, the National Information Security Base Guideline, issued by the NIS, contains a minimum set of security principles and detailed rules for public institutions; the NIS may monitor the compliance of public institutions.¹²

11 Republic of Korea, "National Cybersecurity Strategy", 2019, pp. 11–16.

Despite efforts spanning from 2006 to establish a foundational, cross-sectoral cybersecurity law, its implementation has been hindered. Public distrust of the NIS, historically rooted in its controversial role during previous administrations and stemming from concerns over potential domestic surveillance, has fuelled resistance to NIS-led legislative initiatives.¹³ This has left cybersecurity governance fragmented, with the public, private and military sectors managing cybersecurity independently through separate laws and regulations.

Pursuant to the 2019 strategy and its 2024 revision, it was articulated that the NSO would assume a central coordinating role, clearly delineate inter-agency responsibilities, and advance the enactment of a Basic Cybersecurity Law.¹⁴

The enactment of such legislation would contribute to the establishment of a comprehensive cybersecurity governance framework and the institutionalization of inter-agency coordination, thereby enhancing the coherence and effectiveness of cybersecurity policy implementation and strategic execution. It would also facilitate the systematic allocation of critical resources (e.g., personnel, budget, and technological capabilities) necessary for proactive cyber operations, while providing a foundational legal and institutional basis to support offensive cyber capabilities in accordance with international norms.

2.3 The 2022 Defense White Paper and efforts of the military

According to the 2022 Defense White Paper, in 2019 the Ministry of National Defense (MND) published a National Defense Cybersecurity Policy to set the cybersecurity vision and goals, and to propose medium- to long-term goals and plans. The policy contains plans for developing a system for execution of the defence cybersecurity mission; professionalizing and nurturing professional cybersecurity personnel; improving the capability to respond to various cyberthreats; and strengthening international cooperation in defence cybersecurity.¹⁵

Details of how the Republic of Korea regulates cybersecurity from a military perspective remain undisclosed. Occasional insights into military cybersecurity policy intentions can be gleaned from media reports. For instance, during a parliamentary hearing in 2014, a senior military official articulated the intention of the military to develop offensive cyber capabilities as a proactive measure for deterring

12 Republic of Korea, “National Cybersecurity Strategy”, 2019, p. 13.

13 Republic of Korea, “National Cybersecurity Strategy”, 2019, p. 9.

14 Kang Jin-gyu, “Will the National Cyber Security Act reflect offensive content?”, *Digital Today*, 19 July 2023, <http://www.digitaltoday.co.kr/news/articleView.html?idxno=482190> (in Korean).

15 Republic of Korea, Ministry of National Defense, “2022 Defense White Paper”, 2022, p. 63.

cyberthreats.¹⁶ A visit by President Yoon to the MND's Cyber Operations Command in 2023 emphasized the imperative of transitioning from a reactive response-oriented approach to a proactive and active strategy, and argued for the urgent need to bolster the ranks of cyber specialists.¹⁷ Later that year, the Defense Minister, Shin Won-sik, also mentioned that the MND "will draw up a proactive and offensive cybersecurity strategy to counter sophisticated threats in cyberspace".¹⁸

2.4 National Position of the Republic of Korea on the Application of International Law in Cyberspace

In 2025, the Republic of Korea published the National Position on the Application of International Law in Cyberspace, which elaborated on limits imposed by the existing international law on State use of ICT.¹⁹ A number of legal principles and rules of international law outlined in the document are relevant for the context of this paper since they provide for limitations on international behaviour of States in cyberspace, including the Republic of Korea.

More specifically, the Republic of Korea commits to the principle of sovereignty and maintains that "a State exercises authority over cyber infrastructure located within its territory, over individuals engaging in cyber activities from within its borders, and over the cyber activities themselves".²⁰ Accordingly, States are prohibited from using cyber operations to intervene in the domestic affairs of other States;²¹ the prohibition applies to both cyber operations that amount to the use of force as well as those failing to reach that threshold due to their limited scope or effects.²² According to the Republic of Korea's interpretation of the existing international law in cyberspace, States have the right to respond to unlawful cyber operations with countermeasures and/or measures of self-defence, within the limitations of the law of State responsibility and the law of self-defence, respectively.

16 Zachary Keck, "South Korea Seeks Offensive Cyber Capabilities", *The Diplomat*, 11 October 2014, <https://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites>.

17 Han-kyung Kim, "Former Army Cyber Commander Jae-Seon Byun: 'We Need a Research Group That Will Appoint Experts as Cyber Operations Commanders and Develop Cyberwarfare Concepts and Strategies through Long-Term Research'", *news2day*, 27 June 2023, <https://www.news2day.co.kr/article/20230627500126> (in Korean).

18 Joe Saballa, "S. Korea to Create Offensive Cyber Strategy to Counter Threats", *The Defense Post*, 17 November 2023, <https://thedefensepost.com/2023/11/17/south-korea-cyber-strategy>.

19 Republic of Korea, "National Position of the Republic of Korea on the Application of International Law in Cyberspace", 2025, [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/National_Position_of_the_Republic_of_Korea_on_the_Application_of_Internation.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/National_Position_of_the_Republic_of_Korea_on_the_Application_of_Internation.pdf) (the "National Position").

20 Republic of Korea, "National Position", p. 2.

21 Republic of Korea, "National Position", p. 2.

22 Republic of Korea, "National Position", p. 3.



Credit: © Summit Art Creations/Shutterstock.com

3. Capabilities and Organizational Framework

3.1 Cyber Operations Command

The Ministry of National Defense is in charge of preventing and responding to security incidents that target military networks. The Republic of Korea first established the Cyber Operations Command to carry out operations in cyberspace in 2010. Under the Cyber Operations Command Decree, the Command plans and conducts cyber operations; carries out cybersecurity activities related to those operations; develops and implements required systems; educates and trains its cyber operators; shares information with relevant institutions; and collects and analyses threat information.²³

When it was established in January 2010, the Cyber Command (as Cyber Operations Command was called at the time) was under the jurisdiction of the MND Intelligence Headquarters. Its establishment was closely linked to President Roh Moo-hyun's Defense Reform 2020 initiative, which sought to develop specialized strategies to combat hacking, protect sensitive information from breaches and address Distributed Denial of Service (DDoS) attacks. The burgeoning significance and responsibilities

23 Sungbaek Cho, "National Cybersecurity Organization: Republic of Korea", NATO CCDCOE National Cybersecurity Governance Series, p. 20.

of the Cyber Command necessitated its transition from being under the aegis of the MND Intelligence Headquarters to become an autonomous military unit directly overseen by the MND. This transition was formalized through Presidential Decree no. 23,006 in July 2011.²⁴

In 2019, the Cyber Command was reorganized into the Cyber Operations Command and designated as a joint force to strengthen cyber operations. In addition, the Cyber Protection Center of each military branch was reorganized into a unified Cyber Operation Center and reinforced with capacity suitable for executing cyber operations.

In 2021, the Cyber Operations Command was once more reorganized to play a leading role in planning and conducting cyber operations, research and development, and education and training.²⁵ Details regarding the internal structure or current personnel of the Cyber Operations Command have not been disclosed.

As outlined in Presidential Decree no. 29,561, the Cyber Operations Command functions under the aegis of the MND, bearing responsibility for conducting cyber operations and rendering support within the cyber domain. The mission portfolio of the Cyber Operations Command encompasses the following key objectives:

- Planning and execution of cyber operations
- Cybersecurity activities in conjunction with cyber operations
- Development and implementation of critical systems for cyber operations
- Education and training of cyber operations specialists
- Information sharing and collaboration with related entities
- Collection, analysis and utilization of threat intelligence for cyber operations, etc.

Significantly, practical measures have accompanied these strategic developments. To prepare for future challenges, cyber operation information systems have been formally incorporated into weaponry systems. The MND amended the Defense Strategy Development Operation Regulations to include cyber operation information systems and cyber training information systems within the detailed classification of weaponry systems. This revision aims to enhance the efficient implementation of weaponry systems and power supply systems that support information.

24 [National Intelligence Agencies Leading Cyberwarfare: South Korea (2)], *IPNews*, 31 March 2020, <https://www.boannews.com/media/view.asp?idx=87297> (in Korean).

3.2 Human capacity

When the Cyber Operations Command commenced its operations in 2010, its initial workforce consisted of approximately 400–500 personnel. Subsequently, as a result of organizational growth and development, this contingent expanded to roughly 600 individuals by 2016. The MND planned in 2012 to expand the Command’s personnel to approximately 1,000 and to elevate the rank of its commander from brigadier general to major general.²⁶ By 2021, there had been an observable escalation in staffing, with its estimated personnel strength reaching beyond 1,000 members.²⁷

Additionally, the Top 120 National Tasks of the Yoon Administration included a pledge to reinforce proactive capabilities against cyberthreats and underscored the establishment of a “cyber reserve” to ensure the availability of skilled personnel for cyberwarfare.²⁸

25 Republic of Korea, “2022 Defense White Paper”, p. 63.

26 Kim Hye-young, “Military ‘Cyber Command to be expanded... Commander Promoted to Major General’”, *Hankooki*, 10 June 2012, <https://web.archive.org/web/20130625104454/http://news.hankooki.com/lpage/society/201206/h2012061019165321950.htm> (in Korean).

27 Chung Min-uck, “Cyber Warfare Command’s Manpower to be Doubled”, 10 June 2012, *The Korea Times*, https://koreatimes.co.kr/www/nation/2023/07/113_112748.html.

28 “Yoon Seok-yeol Administration’s Top 120 National Tasks—101. Strengthening National Cybersecurity Response Capabilities”, 22 July 2022, <file:///C:/Users/sjkim/Downloads/202207%20%EC%9C%A4%EC%84%9D%EC%97%B4%EC%A0%95%EB%B6%80%20120%EB%8C%80%20EA%B5%AD%EC%A0%95%EA%B3%BC%EC%A0%9C.pdf> (in Korean), p. 170.



Credit: © vectorfusionart/Shutterstock.com

CAPABILITIES AND ORGANIZATIONAL FRAMEWORK 16

4. Conclusion

This paper analyses the offensive cyber capabilities of the Republic of Korea by examining relevant strategic and policy considerations, the implementation of strategies, and the organizational framework and resources. Although there is a lack of clarity regarding the Republic of Korea's ability to conduct international cyber operations, it is evident that the country is increasingly focused on taking a proactive stance in cyberspace.

First, the 2019 National Cybersecurity Strategy emphasized the importance of offensive cyber capabilities for the Republic of Korea, and the revised 2024 strategy further underscored the need to enhance these capacities. This emphasis was reinforced by President Yoon Seok-yeol's remarks during his visit to the Cyber Operations Command, where he stressed the importance of strengthening offensive capabilities. The Republic of Korea has demonstrated a firm stance against States exploiting the cyber domain, and it has intensified its collaboration with allies to support the tangible realization of proactive strategies. This commitment is evident in measures such as imposing sanctions, naming and shaming, and drafting joint guidelines. The shift towards a more proactive approach represents a significant strategic departure from the traditional focus on strengthening defensive capabilities. Nonetheless, the full implementation of offensive cyber capabilities remains incomplete due to the lack of public disclosure of the operational specifics (e.g., organizational structure, budget and personnel allocation) necessary for executing such operations.

Second, the 2022 Defense White Paper provides a detailed account of the Ministry of National Defense's initiatives to enhance its cyber capabilities. It highlights active participation in collaborative training and exercises with allied States, particularly in crisis-response scenarios. While official military documents remain confidential, the Cyber Operations Command's efforts in capacity-building, personnel expansion, and research and development suggest the establishment of the foundations needed to achieve a competitive edge in cyberspace and to proactively address emerging threats.

Third, there is a noticeable absence of a generally accessible operational framework, including rules of engagement, to guide the strategic direction for securing offensive cyber capabilities.²⁹ Future measures (e.g., criteria and procedures for proportionate responses to malicious cyber activities) are expected to be addressed during the implementation of the 2024 strategy.

Finally, the establishment of a foundational national cybersecurity law is a recognized institutional priority, with a clear commitment outlined in the 2023 National Security Strategy. This legislative development is expected to foster enhanced cross-sector collaboration and coordination, contributing to greater legality and transparency in mission execution. Concurrently, efforts to acquire additional personnel and resources demonstrate a robust commitment to addressing cyberthreats.

The Republic of Korea's transition from a traditionally defensive posture to a proactive response mechanism, supported by dedicated resources and capabilities, is evident. The country's growing engagement in international training and exercises further underscores its intent to expand its participation in global cybersecurity initiatives.



29 So Jeong Kim, "ROK's New National Cybersecurity Strategy and Its Implications", *INSS Issue Brief*, 2024, vol. 106, no. 3, p. 6.

5. References

- Cho, Sungbaek. 2022. "National Cybersecurity Organization: Republic of Korea". NATO CCDCOE National Cybersecurity Governance Series. As of 16 March 2026: <https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf>
- Da-gyum, Ji. 2024. "S. Korea announces 'offensive cyber defense' strategy". *The Korea Herald*. 1 September. As of 16 March 2026: <https://www.koreaherald.com/article/3465045>
- Hye-young, Kim. 2012. "Military 'Cyber Command to be expanded... Commander Promoted to Major General'". *Hankooki*. 10 June. As of 16 March 2026: <https://web.archive.org/web/20130625104454/http://news.hankooki.com/lpage/society/201206/h2012061019165321950.htm> (in Korean)
- IP News. 2020. "National Intelligence Agencies Leading Cyberwarfare: South Korea (2)". *IP News*. 31 March. As of 16 March 2026: <https://www.boannews.com/media/view.asp?idx=87297> (in Korean)
- Jin-gyu, Kang. 2023. "Will the National Cyber Security Act reflect offensive content?". *Digital Today*. 19 July. As of 16 March 2026: <http://www.digitaltoday.co.kr/news/articleView.html?idxno=482190> (in Korean)
- Keck, Zachary. 2014. "South Korea Seeks Offensive Cyber Capabilities". *The Diplomat*. 11 October. As of 16 March 2026: <https://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites>
- Kim, Han-kyung. 2023. "Former Army Cyber Commander Jae-Seon Byun: 'We Need a Research Group That Will Appoint Experts as Cyber Operations Commanders and Develop Cyberwarfare Concepts and Strategies through Long-Term Research'". *news2day*. 27 June. As of 16 March 2026: <https://www.news2day.co.kr/article/20230627500126> (in Korean)
- Kim, So Jeong. 2024. "ROK's New National Cybersecurity Strategy and Its Implications". *INSS Issue Brief*. Vol. 106. No. 3
- Ministry of National Defense. 2022. *2022 Defense White Paper*.
- Min-uck, Chung. 2012. "Cyber warfare command's manpower to be doubled". *The Korea Times*. 10 June. As of 16 March 2026: https://koreatimes.co.kr/www/nation/2023/07/113_112748.html
- National Security Office. 2019. *National Cybersecurity Strategy*. As of 16 March 2026: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf
- Office of the President. 2022. "Yoon Seok-yeol Administration's Top 120 National Tasks—104. Enhancing Capabilities to Counter North Korea's Nuclear and Missile Threats". 22 July. As of 16 March 2026: <https://www.korea.kr/archive/exp-DocView.do?docId=40075> (in Korean)
- Office of the President. 2024. *National Cybersecurity Basic Plan Executive Summary*. 1 September. As of 16 March 2026: <https://web.archive.org/web/20241207235150/https://eng.president.go.kr/briefing/TE0xsLB6>
- Office of the President. 2024. *National Cybersecurity Strategy*. As of 16 March 2026: <https://ncsc.go.kr/cmm/fms/PdfFileView.do?uuid=cd0996ef-8729-4976-abee-83a1809a4aaf&fileSn=1>
- RaonSecure. 2021. "South Korea ranks 4th in the ITU's Global Cybersecurity Index". *Medium*. 6 July. As of 16 March 2026: <https://medium.com/raonsecure/south-korea-ranks-4th-in-the-itus-global-cybersecurity-index-9f7850514c45>
- Republic of Korea. 2025. *National Position of the Republic of Korea on the Application of International Law in Cyberspace*. As of 16 March 2026: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/National_Position_of_the_Republic_of_Korea_on_the_Application_of_Internation.pdf
- Saballa, Joe. 2023. "S. Korea to Create Offensive Cyber Strategy to Counter Threats". *The Defense Post*. 17 November. As of 16 March 2026: <https://thedefensepost.com/2023/11/17/south-korea-cyber-strategy>
- United Nations, Security Council. 2023. Letter dated 3 March 2023 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council. UN Doc. S/2023/171. 7 March. As of 16 March 2026: <https://docs.un.org/S/2023/171>



Credit: © MAXIMUM ART/Shutterstock.com

-  @unidir
-  /unidir
-  /un_disarmresearch
-  /unidirgeneva
-  /unidir



Palais de Nations
1211 Geneva, Switzerland

© UNIDIR, 2026

WWW.UNIDIR.ORG