

National Cybersecurity Strategy



OFFICE OF THE PRESIDENT
REPUBLIC OF KOREA

OFFICE OF
NATIONAL SECURITY

National Cybersecurity Strategy

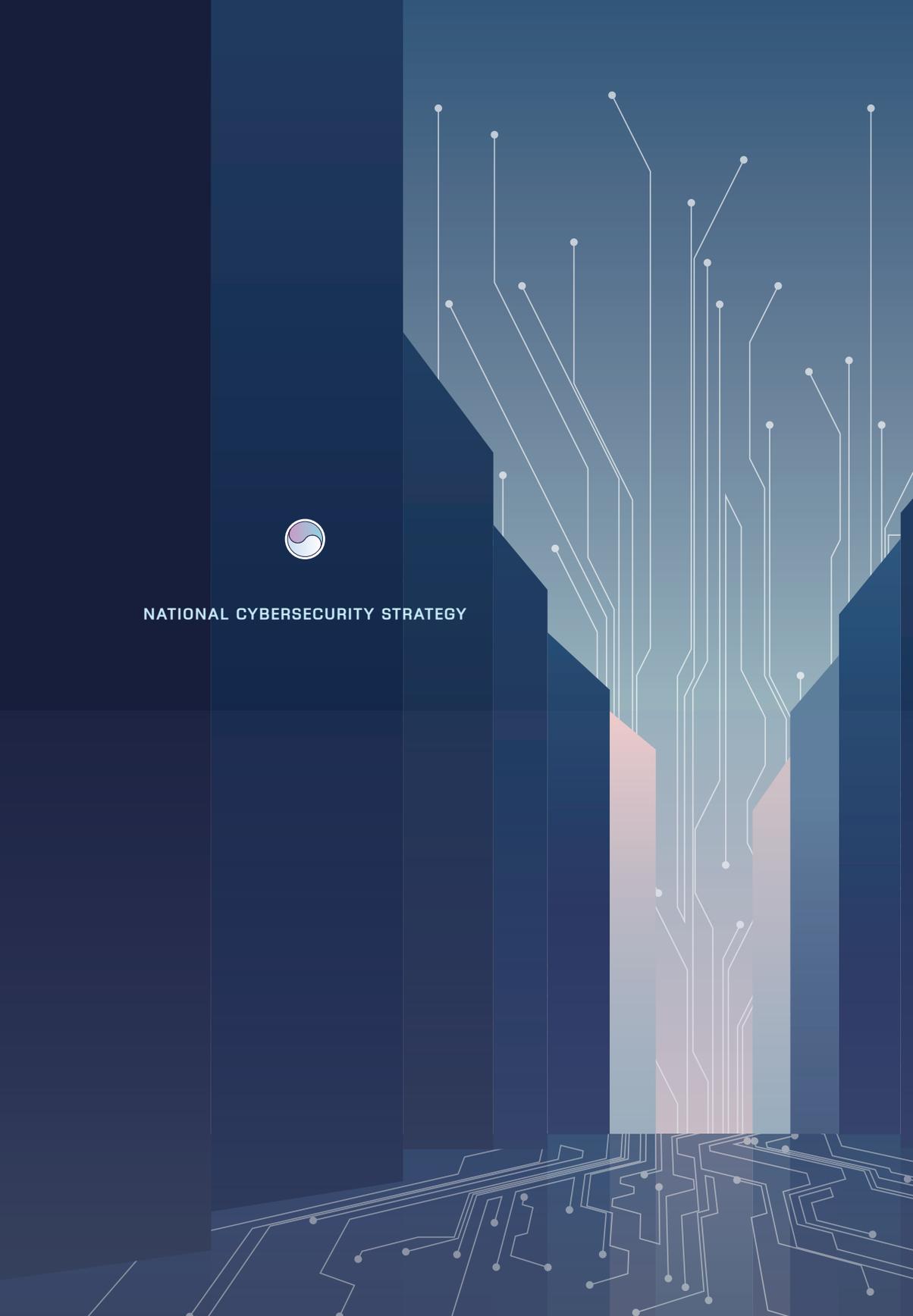


OFFICE OF THE PRESIDENT
REPUBLIC OF KOREA

OFFICE OF
NATIONAL SECURITY



NATIONAL CYBERSECURITY STRATEGY



A Global Pivotal State

upholding the values of freedom, human rights,
and the rule of law in cyberspace,
fulfilling its roles and responsibilities in the international community

Strategic Tasks

1	2	3	4	5
Strengthening Offensive Cyber Defense Activities	Establishing a Global Cyber Cooperation Framework	Enhancing Cyber Resilience of Critical Infrastructure	Securing a Competitive Edge in Critical and Emerging Technologies	Strengthening the Operational Foundation
				





“

President Biden and I have also agreed to get the ball rolling on discussions about expanding our alliance into the cyber and space realms by applying **the Mutual Defense Treaty** in cyberspace and space as well. We have also agreed that **‘the Strategic Cybersecurity Cooperation Framework’** adopted this time around will serve as the foundation on which we address cyber threats together and boost cooperation in information sharing, collection and analysis.

”

Remarks by President Yoon Suk Yeol
at the ROK-US Joint Press Conference on April 27, 2023

Preface

Cyberspace continues to evolve and expand, driven by the boundless potential of digital technology. While we enjoy the various benefits that cyberspace provides, we are also exposed to numerous threats originating from digital means. It is imperative to establish universal and valid principles and norms that can enhance the benefits of cyberspace while preventing instability and confusion.

In particular, North Korea continues its illicit cyber activities, including crypto assets theft, to fund its nuclear weapons and missile development programs. Hacking groups around the world are using sophisticated cyber threat methods to steal state secrets and advanced technologies. The indiscriminate production and dissemination of fake news and misinformation in cyberspace are undermining the order of liberal democracy and threatening national security.

The publication of the “National Cybersecurity Strategy” encapsulates our government’s fundamental strategy to counter these increasing cyber threats. Building on the foundation

of the “National Security Strategy” published 2023 June, this document details our government’s approach to cybersecurity.

With this strategy, our government will proactively address cybersecurity threats and enhance our cyber capabilities and resilience to safeguard the Republic of Korea. Furthermore, we will strengthen cybersecurity cooperation with our allies and partners who share the values of freedom, human rights, and the rule of law, contributing to peace and prosperity in the international community.

The Republic of Korea government prioritizes the protection of the fundamental rights of the people, such as freedom and human rights, and will diligently implement the “National Cybersecurity Strategy” in partnership with our citizens.

February 2024

President of the Republic of Korea

Yoon Suk Yeol

윤석열

TABLE OF CONTENTS



BACKGROUND 10

01 Digital Transformation and Challenges 14

02 Assessment and Necessities 15

VISION AND OBJECTIVES 18

01 Vision 18

02 Objectives 19

03 Principles 22

III

STRATEGIC TASKS

24

- 01 Strengthening Offensive Cyber Defense Activities 24
- 02 Establishing a Global Cyber Cooperation Framework 28
- 03 Enhancing Cyber Resilience of Critical Infrastructure 32
- 04 Securing a Competitive Edge in Critical and Emerging Technologies 35
- 05 Strengthening the Operational Foundation 37

IV

IMPLEMENTATION

42

I BACKGROUND

Cyberspace is a dynamic domain where various state and non-state actors are interconnected and continuously exert influence. In the Republic of Korea, cyberspace is the foundation of liberal democracy, supporting diverse political, economic, social, and cultural activities. It is also a central security domain where critical infrastructure and government systems, closely linked to citizens' lives, are operated and managed.



Recent years have seen a surge in malicious cyber activities by threat actors, including international and state-sponsored hacking groups, posing a grave national security threat. These activities include the theft of advanced technologies, crypto assets heists, the dissemination of fake news to manipulate public opinion, and the incapacitation of critical infrastructure. Additionally, ransomware attacks have been paralyzing government agencies and essential national facilities worldwide, with incidents targeting healthcare institutions directly threatening citizens' lives.

Notably, North Korea has been enhancing its cyber attack capabilities, which can have destructive impacts across various global sectors, including military, financial, and telecommunication systems. Via illicit cyber activities, North Korea evades international sanctions and secures funds necessary for its nuclear weapons and missile development programs.

Cybersecurity involves identifying, countering, and preventing cyber activities that threaten national security and interests, particularly those perpetrated by threat actors like North Korea. It also entails implementing necessary countermeasures to safeguard the nation and its citizens.

Given the growing importance of cybersecurity, countries around the world are developing national strategies to enhance their cybersecurity levels and are striving to improve relevant laws and institutions for more effective implementation. In line with these global trends, the Republic of Korea announced its National Cybersecurity Strategy in 2019.

However, since the announcement of the National Cybersecurity Strategy, the cyber environment has rapidly changed due to factors such as the global pandemic caused by COVID-19 and the competition for technological leadership among major powers. Cybersecurity threats from threat actors have been continually increasing. Disruptions to IT services used by citizens daily have caused inconvenience and socio-economic unrest. Given these backgrounds, the Republic of Korea must redefine its national cybersecurity policy direction to effectively address these challenges.

The Republic of Korea government recognizes the need to expand its strategic scope based on an understanding of the inherent characteristics of cyberspace. This includes enhancing offensive cyber defense capabilities, deepening cooperation with other nations, and developing new strategies to ensure the stable operation of critical state functions and the protection of individual citizens.

Significantly, during the Republic of Korea-United States Summit in April 2023, the “ROK-US Strategic Cybersecurity Cooperation Framework” was established, which includes discussions on applying the ROK-US Mutual Defense Treaty to cyberspace. This represents a significant turning point in the Republic of Korea’s international cybersecurity cooperation, highlighting the need to enhance security capabilities through increased cooperation with the United States and to present a vision for joint responses in the international community.

Furthermore, at the ROK-US-Japan Trilateral Summit in August 2023, the three nations' leaders agreed to strengthen cyber cooperation against North Korea and announced the establishment of a working group for this purpose. In November 2023, commemorating the 140th anniversary of diplomatic relations with the United Kingdom, a "Strategic Cyber Partnership" was signed to elevate bilateral cooperation in information sharing, joint training, and civil exchange to a higher level.

Unlike the previous strategy, which focused on enhancing domestic information security capabilities and protecting critical infrastructure, the new strategy emphasizes close cooperation with relevant countries to secure offensive cyber defense capabilities and global leadership in cybersecurity. Additionally, it includes a strategic concept of mobilizing national capabilities to enhance cyber resilience and respond to malicious cyber activities, thereby protecting critical state functions and the digital lives of our citizens.



1. Digital Transformation and Challenges

The rapid transition to a hyperconnected society and a virtual digital environment has transformed our daily lives into an inseparable relationship with ICT and exposed us to new security risks.

Critical infrastructure and government systems now face various cyber threats as they become more closely linked to cyberspace, following the advancement and sophistication of ICT.

While crypto assets utilizing blockchain technology is gaining recognition as a secure asset, it can also be exploited for illegal money laundering. North Korea, in particular, continues to steal significant amounts of crypto assets to fund its nuclear weapons and missile programs, posing a major threat not only to the Republic of Korea but also to the international community.

Emerging security threats, such as misinformation and manipulation of public opinion, challenge the foundations of liberal democracy. Additionally, ransomware attacks by criminals demanding ransom for encrypted data are on the rise as well.

As information technology becomes more ubiquitous and ICT products manufactured through processes involving multiple countries and vendors are used more widely throughout the nation, security threats that can embed

vulnerabilities in parts and components at all stages of the supply chain from development to deployment, maintenance, and management are also expected to increase.

2. Assessment and Necessities

In 2019, the Republic of Korea established and announced its first National Cybersecurity Strategy, presenting six strategic tasks. In September of the same year, the government introduced the National Cybersecurity Basic Plan to support these strategic tasks, outlining 18 key initiatives and 100 detailed tasks for phased implementation.

The existing strategy served as a milestone, marking the government's first comprehensive document aimed at enhancing the stability of critical infrastructure, improving cyber attack response capabilities, and establishing cybersecurity governance.

A cybersecurity strategy must reflect the national security perspectives and core values outlined in the broader National Security Strategy.

However, the 2019 Strategy has been partially insufficient particularly in addressing North Korea's cyber threats, which pose the most significant real threat to the Republic of Korea. The strategy also fell short in adopting

a security-centric policy direction, such as offensive cyber defense, and in demonstrating global leadership in response to the evolving cybersecurity landscape, including the rise of ransomware and hybrid threats.

Additionally, the existing strategy has been assessed at times to have not surpassed the information protection levels of the previous informatization era. The detailed tasks in the basic and action plans were often extensions of ongoing duties of the relevant ministries or related to specific agencies' information security missions.

As evidenced by the evolving cybersecurity landscape, it is imperative to develop a new strategy from a comprehensive 'cybersecurity' perspective that addresses the full spectrum of national security issues arising in cyberspace, moving beyond the traditional, technology-centric viewpoint of information protection. Moreover, it is essential to stipulate and formalize the role of the Office of National Security (NSO), which oversees and coordinates national security comprehensively, and to designate the lead agency for crisis management, thereby establishing a national cybersecurity framework that clearly defines the roles and responsibilities among various operational systems.

A hand from the right side of the frame points towards a vertical, glowing digital network structure. The structure is composed of numerous interconnected nodes and lines, resembling a complex web or data flow. The nodes are bright yellow and white, and the lines are thin and light blue. The background is a dark, gradient blue, transitioning from black at the top to a lighter blue at the bottom. The overall aesthetic is futuristic and technological.

Offensive cyber
defense and
response

II

VISION AND OBJECTIVES

1. Vision

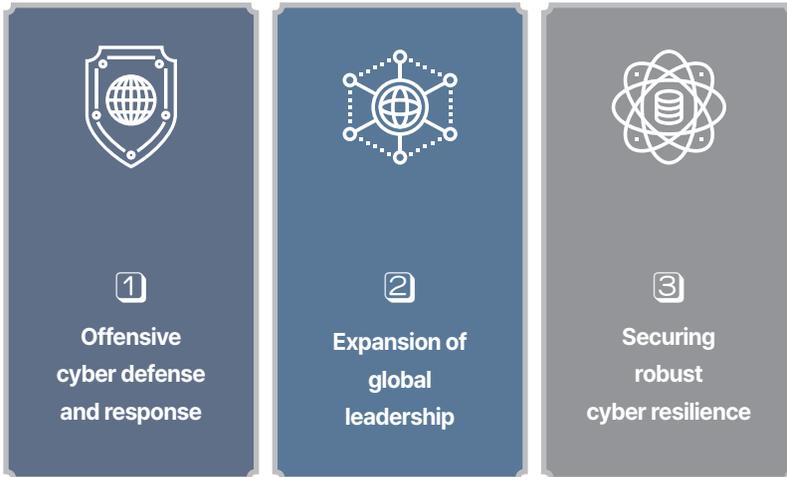


A Global Pivotal State

upholding the values of freedom, human rights, and the rule of law in cyberspace,
fulfilling its roles and responsibilities in the international community

- Cyberspace is the cornerstone of liberal democracy, enabling the free conduct of political, economic, social, and cultural activities.
- The Republic of Korea upholds liberal democracy as a core value of the nation, protecting national interests and the values of freedom and democracy in cyberspace, thereby safeguarding the fundamental rights of the citizens.
- The Republic of Korea actively engages in international efforts to develop cybersecurity policies, systems, and technological advancements, leading responsible state actions to build a safe and reliable cyberspace.
- This strategic vision will be realized through the achievement of three key objectives : ① Offensive cyber defense and response, ② Expansion of global leadership, ③ Securing robust cyber resilience.

2. Objectives



① Offensive cyber defense and response

- Reinforcing defensive capabilities alone is insufficient to effectively counter malicious cyber activities, such as the theft of confidential information, the dissemination of fake news and misinformation, and crypto assets heists, particularly by threat actors like North Korea.
- As the actors and methods of cyber threats have become increasingly diverse, complex, and sophisticated, comprehensive prevention and response at a technical level remain limited.

→ Therefore, the Republic of Korea must shift the paradigm to offensive responses to threats, including those from North Korea, to elevate the nation's cybersecurity to a higher level.

② Expansion of global leadership

- Establishing robust cybersecurity partnerships with allies and partners is essential for upholding the values of freedom, human rights, and the rule of law in cyberspace, as well as for effectively preventing and responding to cyber threats.
- Through tailored cooperation that aligns with each nation's capabilities and objectives, the Republic of Korea aims to enhance deterrence against cyber threats and elevate the level of international cooperation and solidarity, including the development of norms for responsible state behavior in cyberspace.

Expansion of global leadership

③ Securing robust cyber resilience

- The increasingly sophisticated nature of cyber attacks is expected to target not only critical infrastructure with high impact potential, such as energy, transportation, and communications, but also essential services integral to the citizens' daily lives.
- Cyber threats, including external hacking and breaches, as well as critical network disruptions caused by poor management or technical errors, pose significant security risks that can lead to state function paralysis and societal chaos.

→ **The Republic of Korea will mobilize national capabilities to establish a constant state of preparedness, ensuring the protection of both critical infrastructure and the digital lives of the citizens.**



3. Principles

- The Republic of Korea must adhere to the following principles in achieving the aforementioned three objectives :

First, prioritize balancing the importance of national core values with the economic interests of the citizens in conducting cybersecurity activities.

Second, ensure all stakeholders, including the government, industry, and academia, collaborate to recognize the importance of cybersecurity and jointly respond to threats.

Third, protect the fundamental rights of citizens from concerns such as privacy infringements resulting from cybersecurity activities by performing duties with legitimate purposes and lawful means, based on established norms.



National Cybersecurity Strategy

III STRATEGIC TASKS

1. Strengthening Offensive Cyber Defense Activities



Enhance deterrence against malicious cyber activities that threaten national security and interests, and bolster offensive defense capabilities against cyber attacks by threat actors.

A. Enhancing Offensive Responses to National Security Threats

- 1) Identify the perpetrators of cyber attacks that threaten national security and interests and consolidate legal and technical capabilities necessary for accountability to elevate national response levels.
- 2) Enhance response capabilities to sophisticated cyber threats, such as crypto assets hacking, ransomware, and supply chain attacks, by advancing systems for identifying attack origins and tracking the dark web and crypto assets transactions.

- 3) Develop deterrence strategies against national security threats in cyberspace and secure practical deterrence through establishing implementation guidelines, coordinated execution among participating agencies, and the joint issuance of security advisories with allies and partners.

- 4) Task intelligence agencies and the military with actively detecting and analyzing the sources of attacks to identify early indicators, rapidly sharing relevant information with related agencies, and preparing for anticipated attacks to preemptively and offensively respond to threats.

- 5) Identify the entities behind cyber attacks against the nation and impose corresponding accountability for malicious actions based on scientific evidence.

B. Strengthening the Foundation for Threat Information Collection and Analysis

- 1) Establish a domestic legal and institutional framework adhering to the principles of the rule of law, including judicial oversight, to enable intelligence and military agencies to collect and analyze digital information both domestically and internationally, containing the activities of hacking organizations.

- 2) Enhance surveillance and tracking capabilities of intelligence and military

agencies against threat actors by conducting intelligence gathering and reconnaissance activities before any breach to proactively prevent cyber attacks that threaten national security.

- 3) Exchange cyber threat information necessary to prevent and respond to cyber attacks through close cooperation with major national intelligence and security agencies, domestic and international cyber intelligence firms, and other relevant organizations.
- 4) Develop and operate a national-level cyber threat collection and analysis system utilizing new technologies, such as artificial intelligence, to identify and disseminate threat factors in advance, thereby preventing damage.
- 5) Formulate diverse strategies and tactics and advance core technologies and systems to protect national security and interests.

C. Countering Influence Operations in Cyberspace

- 1) Monitor influence operations and misinformation originating from North Korea and abroad that can cause national division and socio-economic disruption, and develop diplomatic and technological countermeasures.
- 2) Strengthen collaboration among relevant ministries, agencies, and businesses to establish policies to counter fake news and manipulation of public opinion and improve deficient laws and institutions.

- 3) Raise public awareness and vigilance about the dangers of malicious influence operations to protect liberal democracy and foster a healthy public opinion environment.

D. Enhancing Prevention and Response Capabilities for Cybercrime

- 1) Strengthen investigative expertise to enhance response capabilities against evolving cybercrimes, such as ransomware distribution and crypto assets heists.
- 2) Raise public awareness about the security of digital platforms exploited for cybercrime and develop rapid support systems for cybercrime victims.
- 3) Expedite the collection and analysis of digital evidence related to individual and corporate damages and support the accumulation of data to prevent further harm.

Strengthening Offensive
Cyber Defense Activities



2. Establishing a Global Cyber Cooperation Framework



Enhance the effectiveness of responses to cyber threats through proactive international cooperation and contribute to building a safe and peaceful cyberspace as a Global Pivotal State.

A. Strengthening Cybersecurity Cooperation with Various Nations, Including the United States

- 1) Enhance cybersecurity cooperation with the international community that shares the values of freedom, openness, safety, and peace in cyberspace.
- 2) Engage in joint responses with the international community to malicious cyber activities based on concrete, objective, and reliable evidence and information.
- 3) Deepen cyber cooperation with the United States to the level of alliance based on the "Strategic Cybersecurity Cooperation Framework between the Republic of Korea and the United States," advancing towards becoming a global cybersecurity leader.

- 4) Strengthen trilateral cybersecurity cooperation among the Republic of Korea, the United States, and Japan, based on "The Spirit of Camp David," to prevent North Korea's illicit cyber activities, such as crypto assets heists and IT workforce exploitation, and to jointly respond to global cyber threats.

- 5) Expand and strengthen cyber cooperation with the United Kingdom through "The Strategic Cyber Partnership," jointly responding to cyber threats across all domains and establishing a mutual support system in advance.

- 6) Reinforce cyber policy coordination with major partner countries in the Indo-Pacific region, such as Australia, Canada, and India, as well as NATO member states, by expanding the sharing of cyber threat information and technology and by expanding the international cyber cooperation network.

- 7) Raise international awareness around North Korea's cyber threats, including the illicit funding of nuclear weapons and missile development programs, and lead international cooperation efforts to prevent and deter such activities.

- 8) Enhance the response to cybercrimes threatening national security by pursuing membership in multilateral cybercrime cooperation agreements and participating in international efforts.

B. Active Participation in International Cyber Norms Discussions and Confidence-Building Measures

- 1) Lead international discussions on the interpretation and application of international law in cyberspace at forums such as the UN and NATO, promoting the establishment of a norms-based cyberspace order.
- 2) Participate in global discussions on the implementation of existing international laws and norms and strengthen bilateral and multilateral cooperation to respond to transnational cyber threats effectively.
- 3) Reaffirm and build consensus on the position that a territorial state has international legal obligations for malicious cyber activities using its information and communication systems.
- 4) Enhance the transparency and credibility of cybersecurity policies by periodically disclosing our perception of national security threats from malicious cyber activities and policies and rationale underpinning our responses.
- 5) Expand existing intergovernmental cybersecurity policy consultations to a broader range of countries, commensurate with the nation's power and status, to foster mutual understanding and trust, thereby deterring global cybersecurity threats and preventing escalations.
- 6) Strengthen our influence within the international community to ensure that our national interests and security considerations are reflected in

various international standards, norms, and trade agreements related to cybersecurity, including emerging technologies and data transfers.

C. Expanding Cooperation with Private Sector and International Organizations and Global Capacity Building

- 1) Expand the exchange of cyber threat information, security technologies, and policies among the government, domestic and international firms, and international organizations, and encourage and support international cooperation among private entities.
- 2) Facilitate forums for domestic and international discussions between government and private sector experts, such as 1.5-track policy consultations, to develop cybersecurity policies that involve various stakeholders.
- 3) Promote capacity-building programs for developing countries to equip them with the capabilities to respond to cyber threats and participate in building a secure cyberspace.
- 4) Expand the scope of assistance from technical and material resources to include the capabilities for developing national strategies, legislation, and policies, thereby establishing sustainable cooperation relationships.
- 5) Coordinate capacity-building programs with international organizations and major donor countries to ensure adequate resource allocation for the substantial improvement of global cybersecurity capabilities.

3. Enhancing Cyber Resilience of Critical Infrastructure



Strengthen the cyber resilience of critical infrastructure and vital systems to ensure the safety and reliability of essential services for all businesses and citizens.

A. Strengthening Security of Critical Information Systems

- 1) Establish and enhance minimum security requirements covering the lifecycle of critical infrastructure operating systems and expand technical support to maintain a constant state of preparedness.
- 2) Develop a rapid response system by establishing a government-wide integrated monitoring and recovery framework and refining system operation and maintenance protocols to mitigate information system disruptions.
- 3) Expand threat detection systems for infrastructure control systems to defend against sophisticated cyber attacks that threaten national security.

- 4) Define clear criteria to classify the types and severity of cyber incidents and improve related systems to streamline responses based on the level of the incident.
- 5) Develop and implement security technologies suitable for infrastructure integrated with IT technologies, such as smart grids, to enhance the stability and efficiency of critical infrastructure operations.

B. Reestablishing Security Management Systems for Implementing the Digital Platform Government

- 1) Ensure the visibility of identities (IDs), systems, networks, and data to implement a 'Zero Trust' security strategy, and develop and execute a phased plan to apply this strategy.
- 2) Clearly define security management according to protection levels, such as classified, confidential, and public information, and provide all citizens with secure methods to utilize digital platforms.
- 3) Secure the safety of digital platforms for the adoption and expansion of technologies like the Internet of Things (IoT) and cloud computing and improve related security certification systems.

C. Establishing a Comprehensive National ICT Supply Chain Security Policy and Response System

- 1) Revise existing security-related regulations and guidelines to ensure the security of the procurement process for government ICT products and components and develop measures to designate and manage reliable suppliers.
- 2) Standardize configuration information and establish a management system for software to minimize security vulnerabilities during software development.
- 3) Build the capacity and environment for education, training, continuous management, and technical support to ensure ICT supply chain security.



Securing a Competitive Edge
in Critical and Emerging
Technologies

4. Securing a Competitive Edge in Critical and Emerging Technologies



Actively cultivate and securely protect critical technologies that form the foundation of national cybersecurity capabilities to ensure international competitiveness and technological leadership.

A. Strategic Industrialization of Core Technologies

- 1) Collaborate with industry, academia, and research institutions to identify critical technologies underpinning cybersecurity and continuously review and improve detailed policies for their strategic industrialization.



- 2) Expand research and development funding for foundational technologies to address new security threats posed by critical and emerging technologies such as AI and quantum technology, and establish and operate specialized organizations for cybersecurity-related technology and policy research and development.

- 3) Promote innovation in information security companies and secure international competitiveness by improving regulations on information security products incorporating new technologies, conducting international promotions, and investments.

B. Establishing a Cyber Risk Management System for Critical and Emerging Technologies

- 1) Develop a security management framework that can promptly respond to cybersecurity issues accompanying the emergence of new technologies and consistently formulate related security measures.

- 2) Expand the exchange, sharing, and transfer of new cybersecurity technologies developed by private companies and public research institutions and enhance support for security consulting to these organizations.

- 3) Implement quantum-resistant encryption systems to protect state secrets from potential data breaches utilizing quantum computers and actively participate in the development of international encryption standards to promote the adoption of encryption solutions.

5. Strengthening the Operational Foundation



Establish a comprehensive national response system that organically connects and harmonizes the roles and responsibilities of individuals, businesses, and the government.

A. Establishing a National Cyber Threat Response System

- 1) Recognize that cybersecurity is directly linked to national security by enacting the “Cybersecurity Act” to establish a national response system and provide an institutional foundation for substantive and concrete cybersecurity activities.
- 2) Establish the ‘National Cybersecurity Committee’ under the Office of National Security to coordinate matters related to nationwide cybersecurity policies and create conditions that allow the government’s overall cybersecurity capabilities and functions to be effectively utilized.
- 3) Enhance national joint response capabilities by creating an integrated response organization to quickly mobilize the core competencies of the government and businesses in the event of a cyber attack.

- 4) Designate the National Intelligence Service as the lead agency for cyber crisis management, overseeing the sharing of threat information, issuing alerts, and coordinating incident responses across all levels of government.

- 5) Build a national-level cybersecurity cooperation platform and hub to strengthen collaboration among relevant ministries, agencies, and businesses.

B. Establishing Roles and Responsibilities

- 1) Improve the institutional framework to ensure that cybersecurity tasks in various sectors are correctly carried out based on the scope of duties defined by individual laws and regulations.

- 2) Develop and revise guidelines and manuals related to cybersecurity crises, including the "National Crisis Management Basic Guidelines," to clearly outline procedures and action plans for relevant ministries and agencies.

- 3) Implement an evaluation system for the cybersecurity activities conducted by each agency in their respective sectors and establish a framework for subsequent improvement measures.

C. Expanding the Utilization of Private Sector Capabilities for National Cyber Crisis Response

- 1) Establish a collaborative platform to enhance cooperation among private stakeholders and promote voluntary and proactive participation from private entities.
- 2) Develop a structured information-sharing system between the government and businesses to enable the rapid exchange and response to cybersecurity-related information, such as vulnerability data and cyber threat indicators.
- 3) Actively utilize private sector experts from various fields to support domestic cybersecurity threat responses and international crisis management efforts in times of need.

D. Developing and Retaining Skilled Cybersecurity Personnel

- 1) Expand specialized cybersecurity education programs and establish an elite personnel development system, strengthening tailored training programs to ensure the supply of suitable cybersecurity professionals for both the public and private sectors.

- 2) Promote national-level joint training involving private and public sectors and organize international cyber defense exercises to establish a world-class, cutting-edge educational and training infrastructure.
- 3) Implement innovative systems and compensation frameworks to gradually integrate private-sector cybersecurity experts into national and public-sector cybersecurity operations and policy activities.
- 4) Continuously manage domestic cybersecurity talent by linking military service with post-service employment and entrepreneurship opportunities in related fields.
- 5) Train professionals and invest in education and research and developments to strengthen fundamental resilience against complex risk factors, such as supply chain security and hybrid threats.

E. Enhancing Public Awareness and Engagement

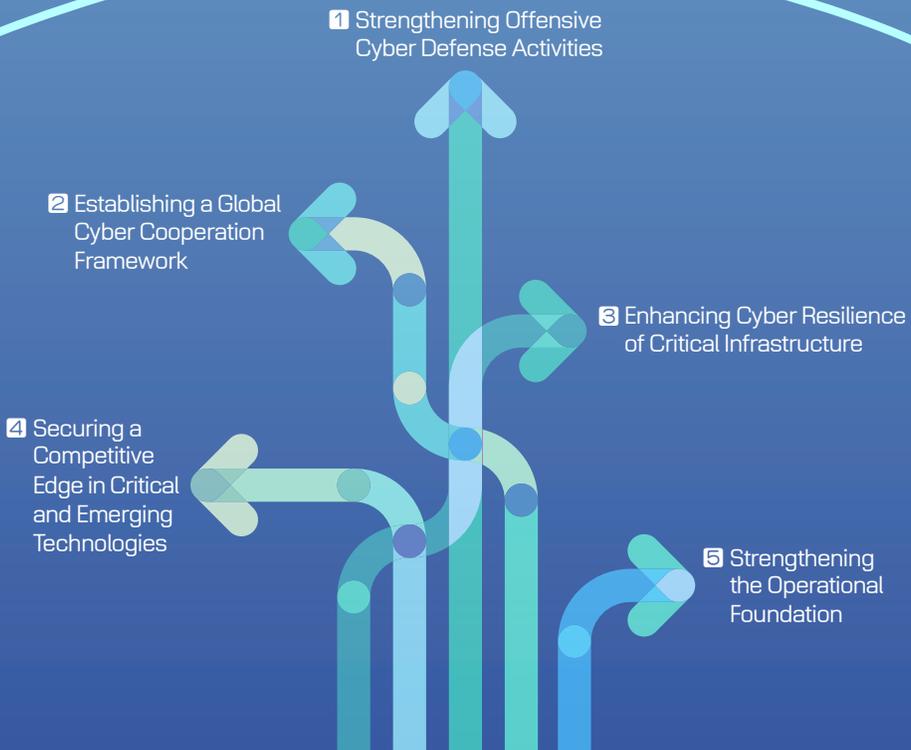
- 1) Activate public participation awareness campaigns using social media and mass media to help citizens understand the importance of cybersecurity and safety protocols.
- 2) Develop and provide tailored awareness programs and content to ensure that citizens recognize the importance of cybersecurity threats and avoid exposure to cyber risks in their daily lives.

The image depicts a complex digital environment. It features a dark background filled with a grid of glowing blue lines and numerous floating rectangular panels. Each panel displays various data visualizations, including line graphs, bar charts, and circular gauges. A prominent bright blue light source on the right side creates a lens flare effect, illuminating the scene. The overall aesthetic is high-tech and data-driven.

Strengthening
the Operational Foundation

IV IMPLEMENTATION

The National Cybersecurity Strategy will be revised every five years as a general principle. However, amendments may be made following the deliberation and resolution of the National Cybersecurity Committee should significant internal or external environmental changes necessitate an update to the strategy.



The Republic of Korea government is committed to collaborating with citizens, businesses, and the international community to achieve the vision and objectives of the National Cybersecurity Strategy. Additionally, the government will concretize and diligently implement the strategy by developing and advancing the National Cybersecurity Basic Plan and the National Cybersecurity Implementation Plan.

The government will review and improve the necessary budget, personnel, and organizational structures for strategy implementation and will pursue legislative measures. Efforts will be made to ensure these are actively reflected in each ministry's medium and long-term work plans.

Furthermore, all ministries must adhere to cybersecurity-related laws, regulations, and fundamental principles to achieve the strategic objectives. The Office of National Security will regularly inspect the implementation of strategic tasks and assess the improvement in cybersecurity levels resulting from these efforts.

National Cybersecurity Strategy

Published in February, 2024

Published by the Office of National Security in the Office of the President, Republic of Korea

Government Publications Registration Number 12-1025000-000013-13

G P R N

12-1025000-000013-13



OFFICE OF THE PRESIDENT
REPUBLIC OF KOREA

OFFICE OF
NATIONAL SECURITY