

Publication Registration Number
12-1025000-000003-01



National Cybersecurity Strategy



National Security Office

Preface

The Republic of Korea leads the world in information and communications technology (ICT) and related infrastructure, and the development of a diverse and convenient cyberspace has allowed people to broaden their horizons. Additionally, cyberspace is now the foundation for providing the government's administrative services as well as operating the nation's critical facilities.

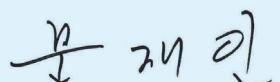
However, the recent rise in cybercrime and terrorism threatens the lives of ordinary people and business activities of companies. Systematic and sophisticated cyber attacks present a grave challenge to national security.

To address these growing threats, the Korean government has drawn up this National Cybersecurity Strategy. We will safeguard the people's safety, rights and interests against cybercrime. We will swiftly detect and block cyber threats to guarantee that key operations of the government continue. We will foster cybersecurity talent and continue to support the development of the cybersecurity industry.

At the heart of cybersecurity lies the people, and the government has devised three fundamental cybersecurity principles to protect the people. We will guarantee the public's basic rights and carry out security activities rooted in the rule of law. We will realize clear and transparent cybersecurity by ensuring citizen participation.

With the cooperation of the government, companies and citizens alike, we can secure our cyberspace. The government will spare no effort in creating an open and safe online environment. I call on my fellow Koreans to join in these endeavors to make Korea a leading cybersecurity nation.

President **Moon Jae-in**
Republic of Korea





CONTENTS

I BACKGROUND	5
1. Changing Environment and New Challenges	6
2. Review and Evaluation	8
3. A New Course of Action	10
II VISION AND GOALS	11
III STRATEGIC TASKS	13
1. Increase the Safety of National Core Infrastructure	14
① Strengthen security of national information and communications networks	14
② Improve cybersecurity environment for critical infrastructure	15
③ Develop next-generation cybersecurity infrastructure	15
2. Enhance Cyber Attack Response Capabilities	16
① Ensure cyber attack deterrence	16
② Strengthen readiness against massive cyber attacks	16
③ Devise comprehensive and active countermeasures for cyber attacks	17
④ Enhance cybercrime response capabilities	17
3. Establish Governance Based on Trust and Cooperation	18
① Facilitate the public-private-military cooperation system	18
② Build and facilitate a nation-wide information sharing system	19
③ Strengthen the legal basis for cybersecurity	19
4. Build Foundations for Cybersecurity Industry Growth	20
① Expand cybersecurity investment	20
② Strengthen the competitiveness of the cybersecurity workforce and technology	20
③ Foster a growth environment for cybersecurity companies	21
④ Establish a principle of fair competition in the cybersecurity market	21
5. Foster a Cybersecurity Culture	22
① Raise cybersecurity awareness and strengthen cybersecurity practice	22
② Balance fundamental rights with cybersecurity	22
6. Lead International Cooperation in Cybersecurity	23
① Enrich bilateral and multilateral cooperation systems	23
② Secure leadership in international cooperation	24
IV PLANS FOR IMPLEMENTATION	25

I

BACKGROUND

1. Changing Environment and New Challenges
2. Review and Evaluation
3. A New Course of Action

01

Changing Environment and New Challenges

❶ Increased vulnerability in cyberspace

The Republic of Korea has built one of the most convenient and prosperous cyberspace environments, drawing upon our world-class information and communications technology(ICT) and related infrastructure.

Today cyberspace is crucial to the daily lives of people, as well as to the economic activities of businesses and the operations of the government, including the provision of basic services.

However, interconnection across various information and communications devices is sharply increasing the complexity of cyberspace, making it harder to manage in a safe manner.

The borderless nature of cyberspace enables vulnerabilities of certain ICT devices to threaten cyberspace as a whole.

Furthermore, cyberspace threats are starting to affect our physical environment with the increasing use of convergent technologies, enabled by the Internet of Things (IoT) for home appliances, medical devices, smart factories and critical infrastructure.

❷ The severity of cyber threats

In the past, malicious cyber activities were carried out mainly by individuals or hacker groups. With the growing involvement of criminal and terrorist groups, supported by state actors, cyber attacks are becoming more organized and executed on a larger scale.

The methods of cyber attacks are diversifying as well, from theft of confidential information and money, to causing social unrest for political purposes, and even cyber terrorism to disrupt or destroy infrastructure.

There is also an increasing likelihood of a cyber war, where cyber attacks may incur damage equal to that caused by traditional armed attacks.

❶ Intensified cybersecurity competition among states

Political, economic, and military disputes among states are escalating to conflicts in cyberspace. In some cases, cyber attacks are conducted prior to or after physical attacks.

Recognizing cyber capabilities as asymmetric powers with potential to significantly impact national security, states have long fostered cybersecurity experts and expanded cybersecurity organizations.

In addition, governments have invested substantial budget in developing state-of-the-art cyber technologies based on artificial intelligence (AI) and big data analytics, as well as strengthening capabilities to collect cyber intelligence, disturb Internet networks, and disrupt major facilities.

❷ Increased harm to the public due to cybercrime

Cybercrime damage to businesses and people continues to grow with the increasing use of advanced technology and sophistication of cyber attacks, such as stealing and encrypting personal information.

The involvement of state actors and terrorist groups is also creating greater and more serious cybercrime damage, increasing the number of incidents that threaten national security.

02

Review and Evaluation

The Republic of Korea has achieved remarkable success in becoming an IT powerhouse, but the nation's cyberspace has been vulnerable to a range of threats.

The government has continuously enhanced the national cybersecurity system by establishing and implementing comprehensive measures in concert with relevant ministries and agencies whenever a massive incident occurred.

Despite these efforts, the rapid development of cyberspace and increased threats to cybersecurity demand more proactive attention and action.

Response Capabilities

The government has continued to bolster its cyber defense capabilities by building a system to detect and respond to cyber attacks in real time, as well as separating internal government networks from the public Internet.

However, it is time to further enhance the resilience of national core services and implement active response measures to evolving cyber attacks.

Human resources and budget

The Korean government has continuously increased the cybersecurity budget and invested in fostering more cybersecurity personnel, while companies have also expanded resources dedicated to cybersecurity.

Yet, the ratio of the government's cybersecurity budget in proportion to the national budget still falls short that of developed countries, and there remains a shortage of talented cybersecurity experts, while there is the increasing demand for security skills and experience.

Industry and technology

The government has enacted relevant laws and regulations to enhance the competitiveness of the security industry and create more jobs, and has created and implemented R&D plans for related technologies.

However, there is still a perception of security as cost, and the lack of sufficient investment and research in basic and next-generation security technologies limits our ability to narrow the technological gap with other leading countries.

Security Awareness

The government's efforts to raise awareness, coupled with increased damage caused by malicious cyber attacks, has improved both individuals' and companies' awareness of the importance of cybersecurity.

Still, many people do not practice basic security rules, while many companies do not take the action needed to protect information and security, creating a gap between awareness and practice.

International cooperation

In order to respond to transnational cyber threats, the government is striving to build a cooperative mechanism with allies and international organizations, such as the UN and ITU.

At the same time, we need to pursue systematic and practical international cooperative activities, such as joining international conventions, sharing information and technology, and drawing up international rules on cybersecurity.

03

A new course of action

Changes and challenges in cyberspace, combined with the realities facing our nation, demand a more strategic and systematic approach towards national cybersecurity.

In order to respond to threats and achieve national prosperity, we must strengthen cyber capabilities and promote cooperation across sectors under a consistent strategy.

Recognizing the cyber threat to national security, the government has devised the nation's first *National Cybersecurity Strategy* in line with the *National Security Strategy* to integrate all capabilities against cyber threats.

The achievements, response systems, institutions, and capabilities of previous policies were extensively evaluated in the process of establishing this Strategy.

This *National Cybersecurity Strategy* sets out the future cybersecurity vision and goals of the Republic of Korea and outlines strategic tasks for individuals, companies, and the government.

The Strategy further elaborates on the roles and responsibilities of all members of society to create a national culture of security practice, ultimately enhancing the nation's cyber defense capacities.

Furthermore, the Strategy aims to protect our cyberspace from threats to allow all people to safely enjoy cyberspace.

II

Vision and Goals



Vision

Create a free and safe cyberspace to support national security,
promote economic prosperity,
and contribute to international peace

Goals

- ① **Ensure stable operations of the state:** Strengthen the security and resilience of the nation's core infrastructure to enable continuous operation despite any cyber threats
- ② **Respond to cyber attacks:** Strengthen security capabilities to deter cyber threats, detect and block them quickly, and respond to any incident promptly
- ③ **Build a strong cybersecurity foundation:** Nurture a fair and autonomous ecosystem where cybersecurity technology, human resources, and industries are competitive

Basic Principles

- ① **Balance individual rights with cybersecurity:** Strike a balance between protecting cyberspace and safeguarding the fundamental rights of the people, e.g. privacy.
- ② **Conduct security activities based on the rule of law:** Carry out the government's cybersecurity policies and activities in a transparent manner and in compliance with the domestic and international laws
- ③ **Build an system of participation and cooperation:** Encourage individuals, businesses, and the government to participate in cybersecurity activities, and pursue close cooperation with the international community



STRATEGIC TASKS

1. Increase the Safety of the National Core Infrastructure
2. Enhance Cyber Attack Response Capabilities
3. Establish Governance Based on Trust and Cooperation
4. Build Foundations for Cybersecurity Industry Growth
5. Foster a Cybersecurity Culture
6. Lead International Cooperation in Cybersecurity



01

Increase the Safety of the National Core Infrastructure

Strengthen security and resilience of the national core infrastructure against cyber attacks to ensure continuous provision of critical services

1 Strengthen security of national information and communications networks

- 1) Implement phased security measures to ensure national information and communications networks are secure against cyber threats throughout their establishment, operation, and disposal.
- 2) Develop the means for year-round inspections and improvements to detect and prevent any threats from security vulnerabilities in national information and communications networks and related equipment.
- 3) Take measures to strengthen the resilience of national information and communications network services, including system performance advancements and expanding back-up facilities, to guarantee provision of services in the face of diverse cyber attacks.
- 4) Develop and apply security technologies and systems in a timely manner to protect the ICT environment, including mobile and cloud facilities.
- 5) Advance both cryptographic and confidential information security systems so the government's confidential information is protected against data leaks or damage.
- 6) Strengthen compliance with both domestic and international technical standards in building national information and communications networks to facilitate prompt response in the event of security incidents.

2 Improve cybersecurity environment for critical infrastructure

- 1) Improve schemes to enable the government to designate and swiftly protect critical infrastructure facilities whose disruption in the case of an attack would significantly unsettle people's daily lives.
- 2) Support institutions operating critical infrastructure to create departments dedicated to cybersecurity and allocate sufficient budget for cybersecurity
- 3) Issue guidelines for institutions to factor in security at the initial phase of establishing critical infrastructure and create relevant inspection schemes.
- 4) Foster an environment that allows voluntary security assessments of network/information equipment acquired by infrastructure operators in the private sector.
- 5) Compose evaluation standards for sector-specific security vulnerabilities and implement measures to ensure services continue in the event of a security incident.

3 Develop next-generation cybersecurity infrastructure

- 1) Prepare technical and institutional plans to respond to emerging security threats triggered by technological convergence and the advent of new technologies.
- 2) Implement “security by design” in ICT products and services that directly impact peoples’ lives to ensure their safety.
- 3) Develop and distribute high-assurance networks which are fundamentally protected against cyber threats.
- 4) Establish next-generation security authentication infrastructure to enable the public to conveniently and safely use online services in a hyper-connected and AI-driven environment.

02

Enhance Cyber Attack Response Capabilities

Expand capacity to efficiently deter cyber attacks in advance and respond to security incidents promptly

① Ensure cyber attack deterrence

- 1) Actively respond to all cyber attacks that infringe upon national security and national interests by concentrating national capabilities.
- 2) Strengthen preventive capacity by building a system that efficiently collects, manages, and eliminates vulnerabilities in cyberspace.
- 3) Acquire practical capabilities to analyze causes of cyber attacks and identify the culprits.

② Strengthen readiness against massive cyber attacks

- 1) Evaluate and enhance the system of information sharing, investigation and response by the relevant agencies regarding a cyber attack or crisis.
- 2) Expand the scope of detecting cyber attacks to enable real-time detection and blocking, and develop AI-based response technologies.
- 3) Enhance response capabilities against cyber crisis nation-wide through public-private-military joint drills, including national crisis management drills such as the Eulji Exercise.
- 4) Facilitate the mission and functions of public-private-military cooperation, including the duties of issuing cyber crisis warnings, sharing threat information, and conducting joint examinations and investigations.

- 5) Devise plans for quantitative classification of cyber crises to enable individuals, businesses, and government to respond to such crises in a swift manner.

3 Devise comprehensive and active countermeasures for cyber attacks

- 1) Review and align all means of response with international rules in the event of a major cybersecurity threat and plan specific measures.
- 2) Develop various strategies and tactics, reinforce military strength, and acquire core technologies to safeguard national security and interests in cyber warfare.
- 3) Train cyber warfare specialists and foster response organizations in order to efficiently conduct cybersecurity activities.

4 Enhance cybercrime response capabilities

- 1) Strengthen the management of facilities and services exploited for cybercrimes and establish a cyber safety network, engaging all relevant agencies, businesses, organizations, and individuals.
- 2) Enhance the government's capacity to identify, arrest, and prosecute perpetrators of cybercrime by expanding expertise to investigate such crimes and cooperation with relevant agencies at home and abroad.

03

Establish Governance Based on Trust and Cooperation

Execute a future-oriented cybersecurity framework based on mutual trust and cooperation among individuals, businesses, and the government, encompassing the public, private, and military sectors

1 Facilitate the public-private-military cooperation system

- 1) Build a governance system under which all entities, including the government, share roles and responsibilities to cooperate for cybersecurity.
- 2) Support individuals and businesses to share the national vision for cybersecurity and enhance their capabilities to fulfil their roles.
- 3) Build a cooperation network of experts at home and abroad to conduct in-depth research on cybersecurity strategies, policies, and other relevant issues.
- 4) Make efforts to reduce cybersecurity blind spots in the private sector by improving cyber attack response, strengthening cooperation between relevant agencies, and expanding resources for supporting institutions.
- 5) Expand dedicated organizations and experts and facilitate collaboration with the private sector in order to establish a self-management system of security in the public sector.
- 6) Improve national cybersecurity defense to actively respond to threats to information and communications networks in the defense sector.
- 7) The National Security Office shall oversee public-private-military cooperation, and develop and implement cybersecurity policies at the national level.

2 Build and facilitate a nation-wide information sharing system

- 1) Build a national information sharing system encompassing all public, private, and defense sectors to facilitate prompt sharing of cyber threat information.
- 2) Develop measures to share cyber threat information in the public-private-military sectors to the maximum extent and improve the operations of these systems
- 3) Devise legal measures to guarantee confidentiality and to prevent non-purpose use such as privacy infringement when information is shared.
- 4) Actively promote information sharing with specialized organizations overseas and share relevant information with domestic organizations to respond to transnational cyber threats.

3 Strengthen the legal basis for cybersecurity

- 1) Improve laws and institutions with the purpose of systematically responding to cybersecurity threats by maximizing cybersecurity capabilities in the public, private and military sectors, and concentrate national capabilities.
- 2) Devise legal measures to allow systematic sharing, analysis and utilization of cyber threat information among public, private and military sectors.
- 3) Strengthen the legal basis to respond to the changing cybersecurity environment, such as the emergence of new vulnerabilities due to AI technology utilization.

04

Build Foundations for Cybersecurity Industry Growth

Create an innovative ecosystem for the cybersecurity industry to secure the competitiveness of technology, human resources, and industries which are critical to national cybersecurity

1 Expand cybersecurity investment

- 1) Promote regulatory reform and support to allow the cybersecurity industry to play a key role in improving the nation's cybersecurity level.
- 2) Continuously expand the government's budget for information security and devise measures for financing to be used in emergencies, for example when responding to massive cyber attacks.
- 3) Promote the "Public Notification of Information Security" system to encourage investment in the private sector and extend tax support for investments in security systems and R&D.

2 Strengthen the competitiveness of the security workforce and technology

- 1) Equip cybersecurity personnel with world-class expertise and competitiveness to respond to sophisticated cybersecurity threats.
- 2) Strengthen customized personnel development programs to provide businesses, government, the military and society with a cyber workforce equipped with diverse capabilities.
- 3) Devise measures to improve cybersecurity expertise and recruit talented personnel.

- 4) Significantly increase the cybersecurity R&D budget to narrow our technological gaps with developed countries and acquire innovative core source technologies to lead the global market.

3] Foster a growth environment for cybersecurity companies

- 1) Foster an environment for entrepreneurship based on cooperation among industry, academia, and research institutions. Build an information security cluster to enable innovative technologies and ideas to be commercialized.
- 2) Strengthen governmental support for and continuously improve schemes to nurture cybersecurity start-ups and SMEs to grow into competitive companies.
- 3) Strengthen the global competitiveness of the domestic security industry by encouraging strategic partnerships with global companies and expanding overseas bases to provide support to their entry into the global market.

4] Establish a principle of fair competition in the cybersecurity market

- 1) Improve the technological competitiveness of the market by transforming the procurement system for cybersecurity products and services from “price-centric” to “performance-centric.”
- 2) Devise ways to guarantee proper pricing for cybersecurity services and thoroughly investigate and correct illegal practices of sub-contracting.

05

Foster a Cybersecurity Culture

The people should recognize the importance of cybersecurity and strive to practice basic security rules, and the government should respect citizens' fundamental rights when implementing policies and facilitate citizen participation

1 Raise cybersecurity awareness and strengthen cybersecurity practice

- 1) Develop and distribute basic rules of cybersecurity so people can realize the importance of cybersecurity and easily put such rules into practice in their daily lives.
- 2) Develop and employ education programs for cyber ethics and security customized to specific sectors of society, such as students, government officials, military personnel, and company employees.
- 3) Strengthen corporate social responsibility of businesses to protect cyberspace and maintain an appropriate level of security in their products and services.

2 Balance fundamental rights with cybersecurity

- 1) Respect citizen's fundamental rights in a free and open cyberspace and ensure the government does not infringe upon these rights or interfere illegally.
- 2) Develop multiple means to collect public opinion to promote public participation and confidence in the national cybersecurity policymaking process.
- 3) Actively and transparently disclose information about cybersecurity to the public to the extent that is not detrimental to national interest.

06

Lead International Cooperation in Cybersecurity

Become a leading country in cybersecurity by strengthening international partnerships and guiding the formation of international rules

[1] Enrich bilateral and multilateral cooperation systems

- 1) Explore means for practical cooperation, both bilateral and multilateral, and establish mutual assistance systems by holding consultations on cyber policies, strengthening partnership with international organizations, and acceding to international agreement.
- 2) Promote cooperation in sectors such as national defense, intelligence, and law enforcement, as well as exchange with the private sector to respond to cybersecurity threats, including acts of war, terrorism, and crime.
- 3) Provide mechanisms to allow relevant agencies to propose policy directions for the government and share collected information throughout the process of international cooperation.

2 Secure leadership in international cooperation

- 1) Increase participation in the process of establishing universally accepted international rules on cybersecurity and take the lead in disseminating international rules and best practices.
- 2) Actively engage in discussions regarding trust building to prevent escalation between states due to any misunderstandings in cyberspace.
- 3) Expand foreign assistance projects for cybersecurity capacity building to developing countries in a reciprocal manner and share cybersecurity technologies and systems.

IV

Plans for Implementation



The government will fulfil its responsibilities and exercise leadership to achieve the vision and goals of the *National Cybersecurity Strategy* in cooperation with its citizens and businesses, as well as the international community.

We will establish and carry out the *National Cybersecurity Basic Plan* and the *National Cybersecurity Implementation Plan* to give shape to and implement this Strategy.

Each Ministry and agency must pursue the goals set out in this Strategy, comply with the basic principles, and carry out the strategic tasks in promoting the laws, institutions, and policies related to cybersecurity.

The National Security Office will regularly monitor the implementation of this Strategy and improvement in cybersecurity for individuals, businesses and governmental entities.

In addition, the Office will review the appropriateness of the cybersecurity framework necessary to implement the Strategy, including the budget, personnel and organizations, and strive to make improvements where necessary.

It will further review the efficiency of cybersecurity execution and implementation strategies in light of the changing security environment, remedy any deficiencies, and reflect those in the Strategy as needed.

Cybersecurity requires participation of not only the government but also individuals and businesses, and the government will strengthen cooperation and open doors to that end, and enhance policy transparency with the ultimate goal of continuously implementing cybersecurity policies based on the public trust.



National Cybersecurity Strategy

Published date April 2019

Publisher National Security Office

Question 02-770-7393
jykim0110@president.go.kr

Publication Registration Number 12-1025000-000003-01
