CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cybersecurity Organisation: REPUBLIC OF KOREA

Sungbaek Cho
NATO CCDCOE Strategy Researcher

National Cybersecurity Governance Series

Tallinn 2022

About this study

This publication is part of a series of country reports offering a comprehensive overview of national cybersecurity governance by nation. The aim is to improve awareness of cybersecurity management in the various national settings, support nations enhancing their cybersecurity governance, encourage the spread of best practice and contribute to the development of interagency and international cooperation.

Primarily focusing on NATO Nations that are Sponsoring Nations of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), each country report outlines the division of cybersecurity roles and responsibilities between agencies and describes their mandate, tasks and competencies and the coordination between them. In particular, it covers the mandates of political and strategic management, operational cybersecurity capabilities and cyber incident management, military cyber defence and cyber aspects of crisis prevention and management. It offers an introduction to the broader digital ecosystem of the country and outlines National Cybersecurity Strategy objectives to clarify the context for the organisational approach in a particular nation.

CCDCOE

The NATO CCDCOE is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from military, government, academia, and industry, currently representing 38 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational, and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations, and law.

The CCDCOE produces the Tallinn Manual, the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cybersecurity experts the opportunity to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies, and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring. The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

harm arising from the use of the information contained in this publication and is not responsible for the content of external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and personal or educational use when for non-profit and non-commercial purposes, provided that copies bear a full citation.

Reports in this serie

National Cyber Security Organisation in Czechia

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in Luxembourg

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Poland

National Cyber Security Organisation in the Republic of Korea

National Cyber Security Organisation in Romania

National Cyber Security Organisation in Spain

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in Turkey

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the United States

China and Cyber: Attitudes, Strategies, Organisation

National Cyber Security Organisation in Israel

Series editor: Berend Valk (CCDCOE)

Information in this document has been checked for accuracy as of June 2022.

Table of Contents

1. Digital society and cybersecurity assessment

Country indicators

Population: 51.6 million[1]

Internet users: 46.8 million[2] (91.9% of the total population)

Area (km^2): 100,412[3] km^2

GDP per capita (USD): 34,984 USD[4]

International rankings*

ICT Development Index (ITU 2017): 2

E-Government Development Index (UN 2020): 2

International Digital Economy and Society Index (EU 2020): 14

Global Cybersecurity Index (ITU 2020): 4

National Cybersecurity Index (eGA 2021): 31

1.1 Digital infrastructure availability and take-up

Fixed-line broadband communication is universally available in virtually all regions across the Republic of Korea (ROK) as 83.6% of all households are connected to the fixed-line broadband network.[5] This amounts to 99.7% of all households if wireless internet is also counted.[6]

ROK's ultra-high-speed internet infrastructure boasts download and upload speeds of 500Mbps or 1Gbps and reached 99.1% coverage in 2018.[7] From October 2018, Korean telecommunications service providers began offering internet services with a maximum speed of 10Gbps in 85 major cities, to achieve more than 50% coverage by 2022.[8] The average download speed on basic broadband networks is 94Mbps[9] and that number rises to 470Mbps and 963Mbps on ultra-high-speed networks depending on service plans (500Mbps or 1Gbps plans).[10]

[1] https://jumin.mois.go.kr/statMonth.do (as of Dec.2020).

[2] 2020 한국인터넷 백서 (2020 Korea Internet White Paper; Written in Korean), Ministry of Science and ICT, 13.04.2021, p.18, https://www.nia.or.kr/common/board/Download.do?bcIdx=23250&cbIdx=99871&fileNo=2.

[3] https://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=2728 (as of Dec.2021).

[4] https://kosis.kr/statHtml/statHtml.do?orgId=101&tblId=DT_2KAA904_OECD (as of Dec.2021).

[5] 2020 Korea Internet White Paper, p.226.

[6] Ibid, p.16.

[7] 2020 국가정보화 백서 (2020 National Informatisation White Paper; Written in Korean), National Information Society Agency, 22.01.2021, p.299, https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=44086&bcIdx=22930&parentSeq=22930.

[8] Ibid, p.301-302.

[9] 2021 년 통신서비스 커버리지 점검 및 품질평가 결과 (2021 Wireless Communications Service Coverage and Quality Assessment Result; Written in Korean), Ministry of Science and ICT, 31.12.2021, p.55, https://www.korea.kr/news/pressReleaseView.do?newsId=156489512.

[10] Ibid, p.67.

In mobile phone networks (4G and 5G), the entire country is within coverage and the number of subscribers is 72.1 million, or 140% of the population.[11] The 4G network's nationwide average download speed stands at 153Mbps, with the number ranging from 147Mbp to 241Mbps in large cities.[12] The 5G network, which was launched in April 2019 as the world's first commercial 5G network, is still in its infancy and as of December 2021, covered only 19%[13] of the country, mostly metropolitan areas, with its average download speed remaining at 801Mbps.[14] The ROK government and telecommunications service providers are planning to build a nationwide 5G network by 2022 to promote the use of 5G[15] and to double the allocation of spectrum for 5G by 2026 as an alternative to the 2.68GHz currently in use.[16]

1.2 Digital public services

In 2001, to lay the foundation for e-government the ROK government enacted the Electronic Government Act[17] which stipulates the principles of electronic government, duties of government and public organisations, electronic processing of civil petitions, electronic administrative management and shared use of administrative information. In November 2002, the 'Government for Citizens' (G4C) website, an electronic civil petition portal site, was opened enabling citizens to apply for, view and have issued civil petition documents online without having to visit administrative agencies. In 2010, the name of the portal was changed to a more friendly 'Minwon24' (it means civil petition in Korean), and again to 'Government24' (www.gov.kr) in 2017. As of 2021, over 2,500 types of documents in various categories including resident registration, real estate, pension, tax, motor vehicle, immigration, medical care and education can be applied for, viewed or issued through this portal.[18]

The ROK government also developed and introduced the 'e-Government Standard Framework'[19] that can be used by public institutions (including central ministries and all other types of government organisations, but excluding the armed forces) and when developing e-Government services to ensure better quality while avoiding vendor lock-in and enhancing software reusability. The framework provides a standardised set of basic functions necessary for developing and running a Java-based system, assisting developers in building a complete system. By December 2021, a total of 252 common components were provided by the framework and secure-coded under the 'Government & Public

[11] 2021 년 10 월말 기준 무선통신 가입자 통계 (Wireless Communication Service Statistics as of Oct. 2021; Written in Korean), Ministry of Science and ICT, 31.11.2021, p.1, https://www.msit.go.kr/bbs/view.do?bbsSeqNo=79&nttSeqNo=3173432.

[12] 2021 Wireless Communications Service Coverage and Quality Assessment Result, p.40.

[13] Ibid, p.5.

[14] Ibid, p.21.

[15] 보도자료: 최기영 장관, 통신 3 사 대표와 '데이터 고속도로' 구축 가속화 논의 (Media Report: The Minister of SIT discuss Data Highway with the CEOs of Three Major ISP Companies; Written in Korean), Ministry of Science and ICT, 15.07.2020, https://www.korea.kr/news/pressReleaseView.do?newsId=156401245.

[16] 5G+ 스펙트럼 플랜 (5G⁺ Spectrum Plan; Written in Korean), Ministry of Science and ICT, 05.12.2019, p.8, https://www.korea.kr/common/download.do?fileId=189089603&tblKey=GMN.

[17] 전자정부법 (Electronic Government Act; Written in Korean), Enacted on 28.03.2001, Last revised on 29.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EC%A0%95%EB%B6%80%EB%B2%95.

[18] 정부 24 서비스 (Government24 Service; Written in Korean), Statistics Korea, https://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1026 (as of Dec.2020).

[19] 표준프레임워크 포털(Standard Framework Portal; Written in Korean), National Information Society Agency, https://www.egovframe.go.kr/home/main.do [accessed 31.12.2021].

Organization Information System Establishment Management Guidelines'[20] established by the Ministry of the Interior and Safety (MOIS).

For the public to use e-government services, an accredited certificate issued by an accredited certification agency designated by the government is needed. The ROK government introduced an accredited certification procedure in 1999 under the Digital Signature Act[21]and has since designated accredited certificate authorities with the Korea Internet & Security Agency (KISA)[22] the highest certificate authority. Since November 1968, the ROK government has issued 13-digit Resident Registration Numbers to all residents of the country and these numbers are used for personal identification when issuing accredited certificates. To have an accredited certificate issued, citizens must visit a bank or a securities company as these organisations act as registration authorities. Certificates for e-government and general banking services are issued free of charge, but a small fee must be paid annually to add securities trading functions. In 2018, the 'Digital One-pass', a simplified login service, was introduced to minimise the inconvenience of using accredited certificates for public services. This smartphone-based authentication system enables users to access public services using fingerprints, face recognition, patterns, PIN and SMS besides accredited certificates. An amendment to the Digital Signature Act in June 2020 also abolished the mandatory application of accredited certificates, allowing the use of digital signatures generated on mobile devices.

The ROK also operates the Special Committee for Electronic Government to establish, implement and review the strategies and base plans for efficient e-government headed by the MOIS and participated in by the presidents of the National Information Society Agency, Korea Local Information Research & Development Institute, KISA and experts from various fields. The committee establishes and announces basic e-government plans every five years, with the latest 'e-Government Base Plan 2021-2025'[23] announced in 2021 laying the foundation for the execution of e-government advancement projects from 2021 to 2025.

In addition to the base plan, MOIS announced the 'Intelligent Government Base Plan'[24] in March 2017, which defines strategies and plans to build an intelligent government based on which the Ministry is currently carrying out projects to provide intelligent and customised services such as a virtual personal assistant, improved administrative processes backed by artificial intelligence and big data, and a blockchain-based administrative platform.

[20] 행정기관 및 공공기관 정보시스템 구축 운영 지침, (Government & Public Organization Information System Establishment Management Guidelines; Written in Korean), Ministry of the Interior and Safety, Enacted on 25.08.2009, Last revised on 19.01.2021, https://www.law.go.kr/LSW/admRulInfoP.do?admRulSeq=2100000197311&chrClsCd=010201.

[21] 전자서명법 (Digital Signature Act; Written in Korean), Enacted on 05.02.1999, Last revised on 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EC%84%9C%EB%AA%85%EB%B2%95.

[22] The KISA is a special corporation of the Ministry of Science and ICT.

[23] 전자정부 기본계획 2021-2025 (e-Government Base Plan 2021-2025; Written in Korean), Ministry of the Interior and Safety, 06.2021, https://www.mois.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_00103925EweePjH&fileSn=0.

[24] 지능형 정부 기본계획 (Intelligent Government Base Plan; Written in Korean), Ministry of the Interior and Safety, 03.2017, https://www.mois.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_00079136Xc5akfj&fileSn=0.

1.3 Digitalisation in business

According to the statistics on e-commerce transactions in the ROK released by the ROK government, online shopping transactions accounted for 33.5% or ₩159.4 trillion[25] (approximately €118.1 billion) of the country's total retail sales in 2020 of ₩475.2 trillion[26] (approximately €351.9 billion). When broken down by category, 32.1% and 67.9% of online shopping transactions took place on the internet and through mobile devices, respectively.[27] As of late 2020, 69.9% of the population shopped online five times a month, spending ₩167,000 (about €124) a month on average.[28]

The ROK government regularly conducts a sample survey of 3,000 domestic companies of different sizes in various industries on their use of IT products and services. According to the latest 2018 survey,[29] a majority of companies are actively using information systems with 93.5% using enterprise resource planning; 61.7%, groupware; 49.5%, customer relationship management; and 45.9%, supply chain management. In terms of new IT technologies, 51% of those surveyed responded that they have introduced a mobile system; 41%, cloud computing; 40.6%, big data; and 30.2%, AI.[30]

The manufacturing sector is also using the latest IT technologies to improve manufacturing processes and increase efficiency. In December 2018, the ROK government unveiled the 'Smart Manufacturing Innovation Strategy for Small and Mid-size Businesses'[31] including a plan to increase the number of small- and mid-size manufacturers which use smart technology to 30,000 and nurture 100,000 highly skilled workers in the smart factory industry by 2022.

1.4 Cyber threat landscape and cybersecurity assessment

The ROK government issues the 'National Information Security White Paper' every year in collaboration with six government organisations: the National Intelligence Service (NIS), in charge of national cybersecurity intelligence and security of the public sector; the Ministry of Science and ICT (MSIT), in charge of informatisation and information security in the private sector; MOIS, in charge of e-Government and security of public services; the Personal Information Protection Commission (PIPC), in charge of the governance of personal data protection and privacy; the Financial Services Commission (FSC), in charge of security of electronic finance; and the Ministry of Foreign Affairs (MOFA), in charge of international cooperation. The paper encompasses a wide range of issues including major information security issues; laws and institutions of information security; cybersecurity compromises; national cybersecurity activities; and the state of industry and manpower related to cybersecurity.

---

[25] 소매업태별 판매액 (Sales volume by retails; Written in Korean), Statistics Korea, https://kosis.kr/statHtml/statHtml.do?orgId=101&tblId=DT_1K31003.

[26] 온라인쇼핑몰 판매매체별/상품군별거래액 (Online Shopping Turnover by Sales Media/Product Family; Written in Korean), Statistics Korea, https://kosis.kr/statHtml/statHtml.do?orgId=101&tblId=DT_1KE10071.

[27] Ibid.

[28] 2020 년 인터넷이용실태조사 - 주요지표 인포그래픽 및 심층분석 보고서 (Internet Usage Survey of Korea 2020 - Key Indicators Infographic and In-depth Analysis Report; Written in Korean), Ministry of Science and ICT, 04.03.2021, p.4, https://www.korea.kr/common/download.do?fileId=194033804&tblKey=GMN.

[29] 2018 년 국내 기업 IT·SW 활용 조사 보고서 (Survey Report on Use of IT and S/W by Korean Companies in 2018; Written in Korean), National IT Industry Promotion Agency, 10.01.2019, p.27, https://www.nipa.kr/main/downloadBbsFile.do?key=112&bbsNo=8&bbsTy=bbs&atchmnflNo=8513.

[30] Ibid, p.264.

[31] 중소기업 스마트 제조 혁신 전략 (Smart Manufacturing Innovation Strategy for Small and Mid-size Businesses; Written in Korean), Authored by relevant Ministries of Korean Government, 13.12.2018, p.8, https://www.mss.go.kr/common/board/Download.do?bcIdx=1009781&cbIdx=256&streFileNm=495f543c-b12b-469d-bfd9-2526be0050d5.hwp.

The latest edition, which was released in May 2021, selected the following new threats to watch: (1) increased cyber campaigns, including state-sponsored hacking, which should not be dealt with as a mere cyber incident but as a national security threat; (2) the growing need for security assurance of cloud platforms along with the rise of work-from-home activities; (3) the increased risk of the dark web; (4) concerns over security and privacy issues of video teleconferencing solutions; (5) continued ransomware attacks; and (6) increased supply chain attacks, which threaten national security.[32] According to its statistics on cybersecurity compromises in the public and private sectors in 2020, 5.5% of public institutions suffered cyber attacks once or twice a year while 0.8% experienced three or more.[33] In the private sector, 2.0% of those surveyed responded that they had suffered from cyber attacks. When broken down by category (with multiple answers being allowed), ransomware was the most common kind of attack (59.8%), followed by malware infection (42.7%), unauthorised access from outsiders (6.6%), DDoS attacks (4.1%), Adware infection (4.0%) and leakage of important materials by insiders (1.6%).[34]

The '2021 Annual Report' by the National Cyber Security Centre (NCSC)[35] of the NIS stated that as of the end of 2020, key types of cyber threats against the government and public agencies included unauthorised email access (77%); spear-phishing email (13%); installation of command and control servers (7%); and malware infection (2%).[36] The report also reported that major cyber threats in 2021 were: (1) information theft targeting diplomatic and military sectors and supply chain attacks committed by state-sponsored actors; and (2) cryptocurrency theft and ransomware attacks by criminal groups for financial gain.[37] It predicted the following as major potential threats in 2022: (1) information theft related to the ROK presidential election by state-sponsored actors; (2) advanced persistent ransomware attacks against critical infrastructure and core IT services; (3) increased attacks on private and public cloud services; and (4) various industrial espionage activities against high-tech companies and research institutes.[38]

[32] 2021 국가정보보호백서 (2021 National Information Security White Paper; Written in Korean), Authored by relevant Ministries of Korean Government, 10.05.2021, p.4-8, https://www.ncsc.go.kr:4018/cmm/fms/FileDown.do?atchFileId=FILE_000000000001506&fileSn=0.
[33] Ibid, p.234.
[34] Ibid, p.251.
[35] The NCSC is the cybersecurity arm of the NIS.
[36] National Cyber Security Centre 2021 ANNUAL REPORT, National Cyber Security Centre, 31.12.2021, p.26, https://www.ncsc.go.kr:4018/cmm/fms/FileDown.do?atchFileId=FILE_000000000002233&fileSn=0.
[37] Ibid, p.16.
[38] Ibid, p.17.

2. National cybersecurity strategy and legal framework

2.1 National cybersecurity foundation

SQL Slammer,[39] which nearly shut down nationwide internet access in the ROK in January 2003, served as an opportunity to highlight the importance of cybersecurity. In the wake of the incident, the NCSC was established in February 2004 on the President's instructions to the NIS, which is under the direct jurisdiction of the President. The NIS used to oversee all cybersecurity issues from high-level policymaking to working-level issues until the establishment in 2015 of the post of Secretary to the President for Cybersecurity within the President's National Security Office (NSO). Since then, the NSO has been the highest national authority in planning and coordinating cybersecurity issues at a whole-government level. The ROK government published the 'National Cybersecurity Strategy'[40] under the coordination of the NSO in April 2019 to lay out a future vision and a mid- to long-term policy direction for national cybersecurity, and to establish strategic assignments for individuals, enterprises and the government. It was prepared by nine government organisations including the NIS, MSIT and the Ministry of National Defence (MND) and signed by the President.

2.2 National cybersecurity strategy

The ROK's National Cybersecurity Strategy has three objectives: seamless operation of the country's major functions; a firm response to malicious cyber campaigns; and establishment of a solid foundation for cybersecurity assurance. It has six key strategic assignments and 18 major sub-assignments. The sub-assignments have been reflected in the 'National Cybersecurity Base Plan'[41] and are being carried out as 100 individual tasks.

The six key strategic assignments and 18 major sub-assignments detailed in the National Cyber Security Strategy are:

(1) **Improving the security of national key infrastructure**. Its goal is to continuously provide services that serve as the foundation of the ROK citizens' lives by strengthening the survivability and resilience of national key infrastructure to cyber attacks. The key sub-assignments include reinforcing national information network security, improving key infrastructure facilities security and developing next-generation security infrastructure.

(2) **Advancement of the capability to respond to cyber attacks**. Its goal is to secure pre-emptive and comprehensive capability to deter cyber attacks efficiently in advance and promptly respond to accidents. The key sub-assignments include acquiring cyber attack deterrence, strengthening large-scale attack readiness posture, devising comprehensive and active measures and enhancing the capability to respond to cybercrimes.

(3) **Establishment of governance based on trust and cooperation**. Based on mutual trust and cooperation among individuals, enterprises and the government, its goal is to establish a futuristic

[39] https://en.wikipedia.org/wiki/SQL_Slammer.
[40] National Cyber Security Strategy, National Security Office, 03.04.2019, https://www.msit.go.kr/bbs/view.do?sCode=user&bbsSeqNo=68&nttSeqNo=1735913.
[41] 국가사이버안보기본계획 (National Cybersecurity Base Plan; Written in Korean), Authored by relevant Ministries of Korean Government, 03.09.2019, https://www.korea.kr/common/download.do?fileId=190113953&tblKey=GMN.

cybersecurity performance system that covers the private, public and military sectors. The key sub-assignments include invigorating the private-public-military cooperative system, building and invigorating a transnational information-sharing system and strengthening the legal basis for cybersecurity.

(4) **Construction of the basis for the growth of the cybersecurity industry**. This promotes the creation of an ecosystem for security industry innovation through reforming systems and expanding support to secure a competitive edge in technology, human resources and industry, which serves as the basic capability for national cybersecurity. Key sub-assignments include expanding cybersecurity investment, strengthening security human resources and technology competitiveness, creating a growth environment for security enterprises and establishing the principle of fair competition.

(5) **Achievement of a cybersecurity culture**. This aims to have the citizens recognise the importance of cybersecurity and practice it while the government respects basic rights while executing policies, all the while promoting citizen participation. The key sub-assignments include raising cybersecurity awareness and strengthening its execution and maintaining a balance between basic rights and cybersecurity.

(6) **Leading international cooperation in the field of cybersecurity**. This aims to defend national security and interests through securing leadership as a guiding nation in the cybersecurity field by reinforcing global partnerships and pioneering the formation of international norms. Its sub-assignments include developing bilateral and multilateral cooperative systems and securing international cooperation leadership.

2.3 Cybersecurity legislation

The ROK does not have a single cybersecurity law that covers all sectors of the nation, but rather defines cybersecurity-related matters based on individual laws of each sector.

Public Institutions

In regards to the cybersecurity of public institutions including all government organisations, the National Intelligence Service Act, [42] Cyber Security Operational Rule [43] (Presidential Decree), Security Operational Rule [44] (Presidential Decree), National Cyber Security Management Regulation [45] (Presidential Directive), Electronic Government Act and the Enforcement Decree of the Public Records

[42] 국가정보원법 (National Intelligence Service Act; Written in Korean), Enacted on 10.06.1961, Last revised on 19.10.2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EA%B0%80%EC%A0%95%EB%B3%B4%EC%9B%90%EB%B2%95.

[43] 사이버안보 업무규정(Cyber Security Operational Rule; Written in Korean), Enacted on 31.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EB%B3%B4%EC%97%85%EB%AC%B4%EA%B7%9C%EC%A0%95.

[44] 보안업무규정 (Security Operational Rule; Written in Korean), Enacted on 10.03.1964, Last revised on 31.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EB%B3%B4%EC%95%88%EC%97%85%EB%AC%B4%EA%B7%9C%EC%A0%95.

[45] 국가사이버안전관리규정 (National Cyber Security Management Regulation; Written in Korean), Enacted on 31.01. 2005, Last revised on 02.09.2013, https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2000000100482.

Management Act[46] are applied. Under these regulations, public institutions are required to comply with the security guidelines set by and implement security mechanisms confirmed by the NIS. To this end, the NIS issues the 'National Information Security Base Guideline'[47] which contains a minimum set of security principles and detailed rules for public institutions and it may check the compliance of public institutions. Central ministries and local governments are responsible for ensuring that institutions and organisations under their auspices comply with these security principles and rules. For e-government services, the MOIS is tasked with implementing security measures through consultation with the NIS. When a cyber incident occurs in a public institution, it must report it to the NIS immediately under the National Cyber Security Management Regulation, and the NIS may request the institution take measures to reduce the impact of the incident and prevent its recurrence.

Telecommunications

Under the Act on Promotion of Information and Communications Network Utilisation and Information Protection,[48] information service providers (including network operators, portals and internet shopping malls) and clustered ICT facility operators such as internet data centres are required to implement security measures to protect their networks in line with standards set by the MSIT. They are also required to report cyber incidents immediately to the MSIT. In case of significant incidents, the MSIT may form a public-private joint investigation committee to identify root causes. Large companies (those with a larger number of customers or volume of sales than pre-defined thresholds set by the MSIT) are required to obtain ISMS (Information Security Management System) certification from the MSIT. The Act also empowers the MSIT to operate a voluntary security certification scheme for telecommunication devices, including Internet of Things (IoT) devices. Regarding IT and security products, there are two other voluntary schemes operated by the MSIT: the IT security certification scheme based on the Common Criteria under the Framework Act on Intelligent Informatisation;[49] and the performance evaluation scheme that tests processing capacity (bandwidth, response time, connections per second) of security products under the Act on the Promotion of Information Security Industry.[50] All these MSIT tasks are supported by the KISA.

---

[46] 공공기록물 관리에 관한 법률 시행령 (Enforcement Decree of the Public Records Management Act; Written in Korean), Enacted on 07.12.1999, Last revised on 16.12.2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B3%B5%EA%B3%B5%EA%B8%B0%EB%A1%9D%EB%AC%BC%EA%B4%80%EB%A6%AC%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0%EC%8B%9C%ED%96%89%EB%A0%B9.

[47] 국가정보보안기본지침 (National Information Security Base Guideline; Written in Korean), National Intelligence Service, Enacted in 01.2000, Last revised in 11.2021, https://www.ncsc.go.kr:4018/template/resources/file/nis_guide_lines_2021_11_1.hwp.

[48] 정보통신망 이용촉진 및 정보보호 등에 관한 법률(Act on Promotion of Information and Communications Network Utilisation and Information Protection; Written in Korean), Enacted on 01.07.2001, Last revised on 08.06.2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0.

[49] 지능정보화기본법 (Framework Act on Intelligent Informatization; Written in Korean), Enacted on 01.01.1996, Last revised on 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A7%80%EB%8A%A5%EC%A0%95%EB%B3%B4%ED%99%94%EA%B8%B0%EB%B3%B8%EB%B2%95.

[50] 정보보호 산업의 진흥에 관한 법률 (Act on the Promotion of Information Security Industry; Written in Korean), Enacted on 22.06. 2015, Last revised on 08.06.2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EC%82%B0%EC%97%85%EC%9D%98%20%EC%A7%84%ED%9D%A5%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%95%EB%A5%A0.

Critical Infrastructure

The Act on the Protection of Information and Communications Infrastructure [51] defines Critical Information Infrastructure (CII) as industrial control systems or information systems related to national security, administration, defence, public safety, finance, communications, transport, energy and so on, and stipulates special protective procedures for key CII that has been designated as such after considering their national and social importance. It requires the operators of key CII to perform an annual vulnerability assessment, fix identified problems and report results to the government. The Office for Government Policy Coordination under the Prime Minister operates the Critical Information Infrastructure Protection (CIIP) Committee consisting of deputy ministers of 19 ministries to designate key CII and deliberate on national CIIP policy. As of December 2020, 274 systems in the public sector and 148 in the private sector, a total of 422, had been designated as key CII.[52] At the working level, responsibility for developing and disseminating annual protection plans that are commensurate with up-to-date threats and checking whether corresponding measures have been adequately implemented within CII are divided between two organisations: the NIS for the public sector and the MSIT for the private sector. Regarding the compulsory annual vulnerability assessment, the MSIT in consultation with the NIS sets out the standards procedures and assessment criteria.[53]

Financial Sector

In the financial sector, under the Electronic Financial Transactions Act and the Regulation on Supervision of Electronic Financial Transactions (FSC Directive),[54] financial companies and e-finance business operators must implement security measures for financial transactions, assess vulnerabilities in transaction platforms and report their findings to the Financial Services Commission (FSC).[55] They are also required to report any cyber incidents to the FSC immediately. The Financial Supervisory Service (FSS) and the Financial Security Institute (FSEC), special corporations administered by the FSC, undertake tasks at the working level to implement preventive measures and respond to cyber campaigns in the financial sector.

Military Sector

Under the Act on Establishment of Infrastructure for Informatisation of National Defence and

---

[51] 정보통신기반 보호법 (Act on the Protection of Information and Communications Infrastructure; Written in Korean), Enacted on 26.01.2001, Last revised on 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EA%B8%B0%EB%B0%98%20%EB%B3%B4%ED%98%B8%EB%B2%95.

[52] 2021 National Information Security White Paper, p.93.

[53] 주요정보통신기반시설 취약점 분석・평가 기준 (Vulnerabilities Analysis and Assessment Criteria for Key Critical Information Infrastructure; Written in Korean), The Ministry of Science and ICT, Enacted on 28.05.2011, Last revised on 29.03.2021, https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A3%BC%EC%9A%94%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EA%B8%B0%EB%B0%98%EC%8B%9C%EC%84%A4%EC%B7%A8%EC%95%BD%EC%A0%90%EB%B6%84%EC%84%9D%C2%B7%ED%8F%89%EA%B0%80%EA%B8%B0%EC%A4%80.

[54] 전자금융거래법 (Electronic Financial Transactions Act; Written in Korean), Enacted on 28.04.2006, Last revised on 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B1%B0%EB%9E%98%EB%B2%95.

[55] 전자금융감독규정 (Regulation on Supervision of Electronic Financial Transactions; Written in Korean), Financial Services Commission, Enacted on 29.12.2000, Last revised on 21.12.2018, https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B0%90%EB%8F%85%EA%B7%9C%EC%A0%95.

Management of Informational Resources for National Defence,[56] the MND protects military information to enhance the armed forces' operational capability, including prevention, detection, tracing and blocking of cyber intrusion into military networks. The Act requires the MND to establish military information security response frameworks to respond to and recover from infringements in peacetime and emergency. To enhance military information security, the MND is also required to: investigate and analyse trends in cyber incidents and technical aspects of threat information; establish a monitoring system to identify the infringement of military information; develop cyber response technologies such as traceback of breaches and threats; and develop policies, procedures and technologies to enable rapid recovery of compromised systems.

High-tech and Defence Industry

Pursuant to the Act on Prevention and Protection of Industrial Technology Leakage[57] and the Defence Technology Security Act,[58] the Ministry of Trade, Industry and Energy (MOTIE) and the Defence Acquisition Programme Administration (DAPA) of the MND are tasked with protecting national core technologies and defence industry technologies. The NIS is also tasked with this role as a national counterintelligence agency. Institutions and businesses that possess national core technologies and defence industry technologies must implement the security measures stipulated by these Acts. If a cyber campaign targeting these technologies has taken place or if there are concerns of a potential incident, this information must be reported to the MOTIE, DAPA or other intelligence and investigative agencies such as the NIS, the Defence Security Support Command (DSSC), the Prosecution Service and the National Police Agency.

Health Sector

Under the Medical Service Act,[59] the Ministry of Health and Welfare (MOHW): collects and disseminates threat information in the health sector; issues security warnings; examines vulnerabilities; takes emergency measures; and detects and analyses security breaches. To streamline these tasks, it operates the Social Security Information Service (SSIS), a special corporation of the MOHW specialised in the informatisation of social welfare systems and the protection of medical information.

Small and Medium-sized Enterprises (SMEs)

The Ministry of SMEs and Start-ups (MSS) provides a security monitoring service for small and medium-sized enterprises to prevent security breaches of SME technologies under the Act on Support for

---

[56] 국방정보화 기반조성 및 국방정보자원관리에 관한 법률 (Act on Establishment of Infrastructure for Informatization of National Defence and Management of Informational Resources for National Defence; Written in Korean), Enacted on 04.02.2010, Last revised on 03.02.2022, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EB%B0%A9%EC%A0%95%EB%B3%B4%ED%99%94%EA%B8%B0%EB%B0%98%EC%A1%B0%EC%84%B1%EB%B0%8F%EA%B5%AD%EB%B0%A9%EC%A0%95%EB%B3%B4%EC%9E%90%EC%9B%90%EA%B4%80%EB%A6%AC%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0/(18800,20220203).

[57] 산업기술의 유출방지 및 보호에 관한 법률 (Act on the Prevention and Protection of Industrial Technology Leakage; Written in Korean), Enacted on 27.04.2007, Last revised on 31.03.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%B0%EC%97%85%EA%B8%B0%EC%88%A0%EC%9D%98%EC%9C%A0%EC%B6%9C%EB%B0%A9%EC%A7%80%EB%B0%8F%EB%B3%B4%ED%98%B8%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0%EC%8B%9C%ED%96%89%EA%B7%9C%EC%B9%99.

[58] 방위산업기술 보호법 (Defence Technology Security Act; Written in Korean), Enacted on 29.12.2015, Last revised on 22.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EB%B0%A9%EC%9C%84%EC%82%B0%EC%97%85%EA%B8%B0%EC%88%A0%EB%B3%B4%ED%98%B8%EB%B2%95.

[59] 의료법 (Medical Service Act; Written in Korean), Enacted on 25.09.1951, Last revised on 29.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%9D%98%EB%A3%8C%EB%B2%95.

Protection of Technologies of Small and Medium Enterprises.[60] The MSS also helps SMEs design and establish an appropriate security system by the same Act.

Other Sectors

Although not clearly stipulated in the law, other central ministries and local governments may also perform cybersecurity activities for the sectors under their purview in the course of their duties under the Government Organisation Act[61] and other laws and directives. For example, the Ministry of Education, with its comprehensive authority to supervise private schools as stipulated in the Private School Act,[62] operates the Education Cybersecurity Centre to protect private school networks. The Ministry of Land, Infrastructure and Transport (MOLIT), under the 'MOLIT Cybersecurity Centre Operational Guidelines'[63] (MOLIT Directive), operates the MOLIT Cybersecurity Centre for agencies and organisations under its jurisdiction. The Ministry of Food and Drug Safety (MFDS) operates the 'MFDS Cybersecurity Centre' by the 'MFDS Cybersecurity Centre Operational Guidelines'[64] (MFDS Directive) that authorises the MFDS to supervise relevant agencies and organisations, including in the private sector. Likewise, the Ministry of Employment and Labour; Ministry of Economy and Finance; Ministry of Culture, Sports and Tourism; Ministry of Trade, Industry and Energy; Ministry of Unification; Ministry of Fisheries; Cultural Heritage Administration; Military Manpower Administration; and National Fire Agency also operate their own cybersecurity centres based on their respective directives and conduct protective activities in their sectors.

[60] 중소기업기술 보호 지원에 관한 법률 (Act on Support for Protection of Technologies of Small and Medium Enterprises; Written in Korean), Enacted on 28.05.2014, Last revised on 20.10.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A4%91%EC%86%8C%EA%B8%B0%EC%97%85%EA%B8%B0%EC%88%A0%EB%B3%B4%ED%98%B8%EC%A7%80%EC%9B%90%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0.

[61] 정부조직법 (Government Organisation Act; Written in Korean), Enacted on 17.07.1948, Last revised on 31.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B6%80%EC%A1%B0%EC%A7%81%EB%B2%95.

[62] 사립학교법(Private School Act; Written in Korean), Enacted on 26.06.1963, Last revised on 10.08.2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%AC%EB%A6%BD%ED%95%99%EA%B5%90%EB%B2%95.

[63] 국토교통 사이버안전센터 운영규칙 (Land, Infrastructure and Transport Cybersecurity Centre Operational Guidelines; Written in Korean), Enacted on 20.05.2009, Last revised on 15.02.2016, https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000040140.

[64] 식품의약품안전처 사이버안전센터 운영규정(Food and Drug Safety Cybersecurity Centre Operation Guidelines; Written in Korean), Enacted on 27.03.2018, Last revised on 18.06.2019, https://mfds.go.kr/brd/m_212/down.do?brd_id=data0006&seq=14276&data_tp=A&file_seq=1.

3. National cybersecurity governance

3.1 Strategic leadership and policy coordination

The supreme decision-making authority on all matters of national security in the ROK, including cybersecurity, lies with the President and the NSO assists the President in their national security duties. In 2015, the NSO created the post of Secretary to the President for Cybersecurity. Should national security issues, including cybersecurity matters, arise, the Director of the NSO can convene a National Security Council (NSC) Standing Committee meeting consisting of ministers related to national security, the director of the NIS and two deputy directors of the NSO under the National Security Council Act[65] or call a National Cybersecurity Policy Coordination Meeting consisting of deputy ministers of ministries related to the issues in question under the 'National Crisis Management Base Guideline' (undisclosed Presidential Directive) to deliberate on and coordinate cybersecurity matters.

The actual administrative responsibility for cybersecurity lies with the organisations that have been established under the Government Organisation Act. While the NIS oversees the collection, analysis, and compilation of national cybersecurity information as well as safeguarding the government and public sector, central ministries have responsibility for security and protective activities for their own sectors in close cooperation with other ministries and agencies. Figure 1 is a simplified diagram of the ROK's cybersecurity governance structure. The diagram is for explanatory purposes and does not list all of the relevant ministries or organisations.

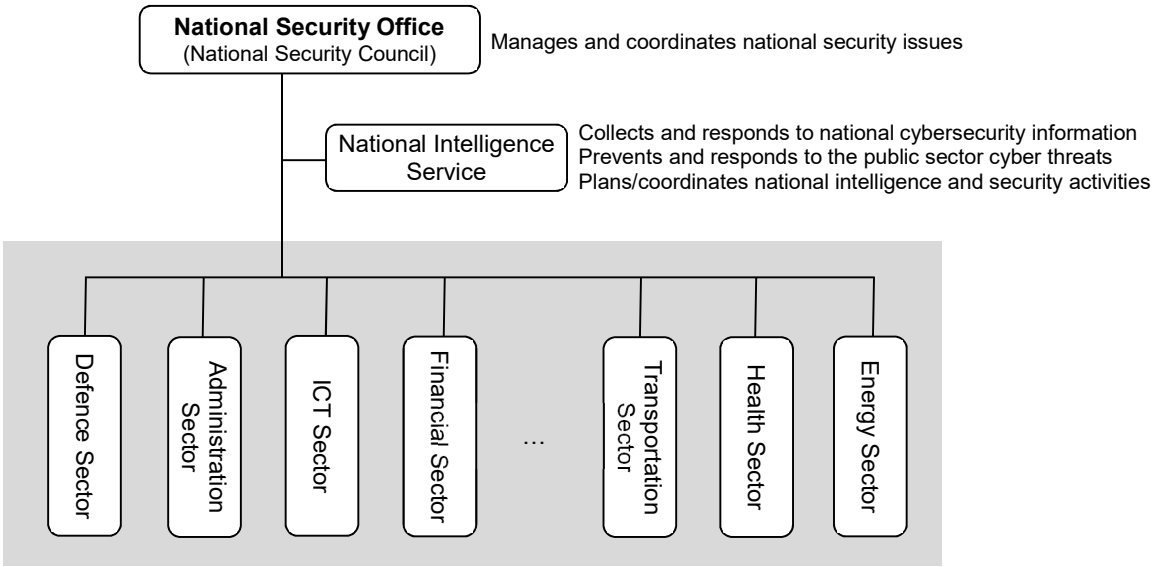

Figure 1. Simplified cybersecurity governance structure.

3.2 Cybersecurity authority and cyber incident response

The following is a list of the key organisations that play an integral role in the ROK's cybersecurity, along with a description of those roles.

[65] 국가안전보장회의법 (National Security Council Act; Written in Korean), Enacted on 14.12.1963, Last revised on 10.01. 2014, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EA%B0%80%EC%95%88%EC%A0%84%EB%B3%B4%EC%9E%A5%ED%9A%8C%EC%9D%98%EB%B2%95.

National Intelligence Service

The NIS serves as both a national intelligence agency and national security agency and was established under the Office of the President in 1961 to carry out intelligence and security activities with the primary objective of ensuring national security. As a national intelligence agency, the NIS collects, analyses and disseminates cybersecurity information related to international and state-sponsored hacking groups and takes measures to respond to them. When deemed necessary for national security, the NIS may carry out investigations and request documents and testimony from anyone under the National Intelligence Service Act, request information on user identities from information service providers under the Telecommunications Business Act,[66] and employ stronger legal measures such as requests for detailed communication history and electronic surveillance with court authorisation or the President's approval under the Protection of Communications Secrets Act.[67] To share cybersecurity information with domestic organisations, the NIS has been operating 'National Cyber Threat Intelligence' (NCTI), an information-sharing system, since 2016, and 302 public institutions were using the system as of July 2021.[68] For information sharing with the private sector, it also operates another information-sharing system called 'Korea Cyber Threat Intelligence' (KCTI) with private companies that could directly affect national interest and security such as defence industries and high-tech companies.[69]

As a national security agency, the NIS is responsible for preventing and responding to cyber attacks against public institutions. Its tasks include the conduct of basic cybersecurity measures for public institutions; security accreditation of information systems and networks to be used by public institutions; security validation of security solutions and network equipment to be used by public institutions; provision of security consulting services (including penetration testing); education, training and exercises; official assessment of security posture of public institutions; the operation of governmental security monitoring systems; issuing cybersecurity alerts for the public sector; the investigation and attribution of cyber attacks; and the development and distribution of technology and equipment to protect classified information. Under the Act on the Protection of Information and Communications Infrastructure, when a significant threat to key CII that could affect national security is imminent, the NIS may provide support not only to the public sector but also to the private sector, even if the CII operator has not requested such support.

Ministry of Science and ICT

The MSIT is tasked with controlling and managing policies and systems for information security in the private sector and the protection of the information and communications sector. The MIST has entrusted a large part of its working-level tasks to the KISA and therefore the KISA operates the Korean Computer Emergency Response Team (KrCERT) to assist cyber incident response activity in the private sector. KrCERT provides consultation about and receives reports on vulnerabilities and incidents;[70] issues up-

[66] 전기통신사업법 (Telecommunications Business Act; Written in Korean), Enacted on 12.30.1983, Last revised 19.10.2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EA%B8%B0%ED%86%B5%EC%8B%A0%EC%82%AC%EC%97%85%EB%B2%95.

[67] 통신비밀보호법 (Protection of Communications Secrets Act; Written in Korean), Enacted on 27.12.1993, Last revised on 16.03. 2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%86%B5%EC%8B%A0%EB%B9%84%EB%B0%80%EB%B3%B4%ED%98%B8%EB%B2%95.

[68] National Cyber Security Centre 2021 Annual Report, p.22.

[69] Ibid.

[70] Under the Promotion of Information and Communications Network Utilisation and Information Protection, the KISA shall analyse the cause of an incident and advise on necessary measures. However, to pursue legal action such as the arrest of the perpetrator, a separate report is required to investigative agencies including the

to-date security recommendations on vulnerabilities to the private sector; offers support for security checks on personal computers and IoT devices; provides consultations to small and medium-sized businesses; gives support to enhance website security; conducts cyber exercises in the private sector;[71] shares cyber threat information targeting private corporations and academic circles; and monitors malware infection of 4 million Korean websites.[72] The KISA started to use an automated threat information-sharing system called the 'Cyber Threats Analysis System' (C-TAS)[73] in 2014 to share threat information with private companies and academia. KISA also provides technical assistance to the MOIS for securing public e-services[74] and the PIPC for personal information protection activities stipulated in the Personal Information Protection Act.[75] KISA operates several security-related certification and evaluation schemes on behalf of the MSIT including the ISMS certification scheme for private companies, the Cloud Security certification scheme for cloud service providers, and the IT Security Product Performance Evaluation scheme for security product vendors and developers. The KISA also provides security competence designation and qualification for companies and individuals such as the 'Service Company Specialised in Information Security' designation;[76] the 'Security Monitoring Specialised Company' designation;[77] and the 'Specialist for Information Security' and ISMS Auditor qualifications for individuals.

Financial Services Commission

The FSC is tasked with protecting electronic financial transaction users and establishing security policies for electronic financial transactions. The FSS and the FSEC, both under the FSC, undertake various tasks at the working level. In line with its mandate as an inspection and supervisory body, the FSS is responsible for e-finance security measures and all related tasks. It establishes and implements detailed security standards for financial institutions, conducts a security validation when financial institutions begin new e-finance businesses and analyses and confirms evaluation results of the vulnerabilities of e-finance infrastructure. The FSEC is specialised in cybersecurity for the financial sector. It operates a special information-sharing system; issues forecasts and warnings about cyber intrusions; operates an integrated security monitoring centre; investigates and analyses incidents;[78] operates a DDoS attack emergency response centre; carries out cyber exercises against incidents; and provides security technology.

---

prosecution and police. Reporting is voluntary for general citizens and private companies, but information service providers and data centres are required to report incidents.

[71] The private sector exercise is voluntary, but the public sector cyber exercise is mandated to be conducted regularly by the National Cyber Security Management Regulation.

[72] The 2021 National Cybersecurity White Paper, p.79: Automated dynamic inspection solution continuously monitors for malicious link insertion against Korean web sites. Upon detection of malicious activities, the KISA contacts the operator of the web site for removal.

[73] According to the 'National Information Security White Paper 2020' (p.106), a total of 260 organisations, including companies and portal companies, being participated as of the end of 2019.

[74] Pursuant to the Electronic Government Act, the MOIS should consult the NIS before implementation of security measures even if technical support has been received from the KISA.

[75] 개인정보 보호법 (Personal Information Protection Act; Written in Korean), Enacted on 29.02.2011, Last revised on 04.02.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95.

[76] For private security consulting companies to offer security advisory service to CII operators, they must be designated as a 'Service Company Specialising in Information Security' in accordance with the Act on the Promotion of Information Security Industry.

[77] The National Cyber Security Management Regulation allows public institutions to use personnel from private companies to carry out network security monitoring tasks. Instead, the Regulation requires the MSIT to conduct a screening process for private companies that offer security monitoring services in consultation with the NIS for quality outsourcing.

[78] Under the Regulation on Supervision of Electronic Financial Transactions, the FSC may organise an incident investigation team including the FSEC to analyse the causes of incidents and take emergency measures.

Ministry of the Interior and Safety

MOIS provides e-government services. It operates an IT architecture for e-government (the e-Government Standard Framework); issues and amends secure coding standards; provides IT audit standards including security provisions that are to be applied when public institutions establish information systems and networks; and operates an IT audit scheme. The National Information Resources Service (NIRS) is a centre under MOIS that provides information and communications network and cloud platform services used by central ministries. Its portfolio also includes security management and security monitoring activities for those services. It provides services and support to local governments through the Korea Local Information Research and Development Institute (KLID), a special corporation tasked with security monitoring and technical assistance for the 226 local governments and the 17 metropolitan cities and provinces.[79]

Ministry of National Defence

The MND is in charge of preventing and responding to security incidents targeting military networks. The ROK established the Cyber Operations Command (since renamed from the ROK Cyber Command) in 2010 to carry out operations in cyberspace. Under the Cyber Operations Command Decree,[80] the Command plans and conducts cyber operations; carries out cybersecurity activities related to the operations; develops and implements required systems; educates and trains its workforce; shares information with relevant institutions; and collects and analyses threat information. The DSSC, established under the DSSC Decree,[81] carries out military security and counterintelligence operations and provides support for defence activities related to each level of Cyberspace Protection Conditions (CPCON),[82] information warfare and cybersecurity of the defence industry.

National Security Research Institute

The National Security Research Institute (NSR) is a government-funded research institute[83] that carries out research and development in support of activities related to national cybersecurity, such as national cryptographic research and incident detection technology. The NSR operates the Cyber Security Training & Exercise Centre (CSTEC) to offer training courses to employees of public institutions to improve the response capability of the public sector to cyber crises.[84] The Common Criteria (CC) certification in the ROK, which was conducted by the NIS in the past, was transferred to the NSR in 2012 and therefore the NSR carries out tasks related to the Common Criteria Recognition Arrangement (CCRA) as the certification body of the ROK.

---

[79] Seventeen metropolitan cities and provinces also conduct their own network security monitoring for their local governments and affiliated organisations.

[80] 사이버작전사령부령 (The Cyber Operations Command Decree; Written in Korean), Enacted in 26.02.2019, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%AC%EC%9D%B4%EB%B2%84%EC%9E%91%EC%A0%84%EC%82%AC%EB%A0%B9%EB%B6%80%EB%A0%B9.

[81] 군사안보지원사령부령 (The Defence Security Support Command Decree; Written in Korean), Enacted 21.08.2018, Last revised on 04.02.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%B0%EC%82%AC%EC%95%88%EB%B3%B4%EC%A7%80%EC%9B%90%EC%82%AC%EB%A0%B9%EB%B6%80%EB%A0%B9.

[82] CPCON is a warning system in the military sector ranging from Level 1 to Level 5 to effectively respond to anticipated or actual cyber attacks on military systems and networks.

[83] The MSIT is in charge of the overall administration of all government-funded science and technology research institutes.

[84] According to 'National Cyber Security Centre 2021 Annual Report', the NIS provided 26 courses, including malicious code analysis, through the Cybersecurity Training and Exercise Centre to train 1,112 officials from government and public organisations on a total of 49 occasions, in 2020.

3.3 Cyber crisis management

In the ROK, the NSO is the highest-level body responsible for managing and responding to crises relating to national security, including cybersecurity. The level of national cyber crisis warning and its response principle use a system defined by the NIS under the 'Standard Manual for National Cyber Crisis Management' (non-public document). According to the NCSC's website,[85] the warning system has 4 stages: moderate, substantial, severe and critical:

> (1) **Moderate**. There is a need to monitor cyber threats as there is a growing possibility of worm, virus or hacking attacks; and rising cyber attacks in foreign countries may affect the ROK.
>
> (2) **Substantial**. Some of the country's network and information systems have failed, some institutions have been attacked or there is an increasing possibility that malicious attacks may spread to some other institutions, thus the country is required to improve the security of its entire IT system.
>
> (3) **Severe**. Many institutions are required to take joint countermeasures as several ISP or backbone networks have failed and a large number of institutions have been compromised or the possibility of large-scale damage is increasing.
>
> (4) **Critical**. A joint response at a national level is necessary as network and information systems have failed, cyber attacks have been made against the nation as a whole, or massive damage has occurred.

Under the National Cybersecurity Management Regulation, the NIS, MSIT and MND exchange information and issue an alert to their respective sectors. When a warning of moderate or higher is issued, every public institution in the ROK conducts prevention, response and recovery activities corresponding to each warning level. Under the National Cyber Security Management Regulation, the ROK government organised a Public and Private Joint Response Team in 2012 in the NCSC to generate synergy through mobilising response capability in the private, public and military sectors at times of major national crisis. The Regulation also authorises the NIS to activate the 'Pan-government Cyber Crisis Countermeasures Headquarters' to integrate national crisis response capability.

3.4 Military cyber defence

The 2020 Defence White Paper[86] stated that the ROK military has been making diverse efforts to strengthen capability and ensure cybersecurity. Centring around the Joint Chiefs of Staff (JCS), in 2019 the military built a system for cyber operations to enhance cyber operational readiness and respond to cyber threats more efficiently. The military also set up a cooperation mechanism among the JCS, Cyber Operations Command and military branches (Army, Air force, Navy and Marine Corps) to flexibly control cyber operations and report cases. The ROK Cyber Command was changed to Cyber Operations Command in 2019 and was designated as a joint unit to carry out the orders of the Chairman of the JCS. The headquarters of each military branch also has its own Cyber Operation Centre.

The personnel administration system, consisting of recruitment, training, assignment and promotion, continues to develop to further boost the cyber workforce's capability. A military occupational speciality for cybersecurity was introduced for commissioned and non-commissioned officers in 2019 and for military civilian employees in 2020 to secure cyber manpower and enable appropriate personnel

---

[85] 경보 단계(Warning Levels; Written in Korean), National Cyber Security Centre, https://www.ncsc.go.kr:4018/PageLink.do?link=forward:/cop/bbs/selectBoardList.do?bbsId=CyberCrisis_main&tempParam1=&menuNo=020000&subMenuNo=020100&thirdMenuNo=#cnt1 [accessed 28.02.2022].

[86] 2020 Defence White Paper, The Ministry of National Defence, December 2020, p.80~83, https://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_202106300300426680.pdf.

management. The training system for the new positions was also improved. A cyber operation system was launched to collect and visualise information to further advance fighting power and response capability. It allows commanders to make decisions and exercise command and control. Efforts have been made to respond to atypical cyber attacks by using cutting-edge technologies including artificial intelligence. Cyber exercises assuming various cyber crises are also conducted regularly.

The MND is also key in international cooperation on national cybersecurity. It has been operating the ROK-US Cyber Policy Working-level Committee with the US Department of Defence since 2014 and participates in multilateral conferences such as the ASEAN Defence Ministers' Meeting-Plus (ADMM-Plus) and the Seoul Defence Dialogue (SDD), which is a vice-ministerial level multilateral security consultative body led by the MMD. Having chaired a cyber working group of the SDD since 2014, the MND shares cyber threat information and information on cybersecurity policy and systems with 20 to 30 countries every year. The ROK has become a co-chair country of the ADMM-Plus working group meeting with Malaysia from 2021 to 2023, facilitating information sharing and discussion among member countries. The MND established 'National Defence Cybersecurity Guidelines' in October 2019 and 'Cyber Operations Instructions' in December 2019 under the National Cybersecurity Strategy published in April 2019. However, these documents have not yet been released to the public.

3.5 Engagement with the private sector

According to the 2020 Survey for Information Security Industry in Korea,[87] a total of 1,283 information security-related entities – 531 cybersecurity companies and 752 physical security companies – operate in the ROK. With this strong industrial infrastructure, the ROK government has promoted a public-private-academic partnership to strengthen national cybersecurity competitiveness. The MSIT, with support from the KISA, has initiated several projects with academia and industry. Announcing the Comprehensive Plan for Information Security in the Private Sector 2019,[88] the MSIT aimed to allocate ₩850 billion (approximately €6.3 billion) and nurture professionals with expertise in security services including AI security and security convergence until 2022, with the three strategies of the expansion of cyber safety, support to innovative growth in the security industry and promotion of information security foundation. The NIS cooperates with the NSR and the MND with the Agency for Defence Development (ADD), a government-funded military technology research institute, to promote partnerships with industries and academia to proceed with several research projects.

On top of the R&D efforts, the ROK government has increased cooperation with the private sector to develop security measures on various technical issues and share cyber threat information. A case in point is the 'Council for Security Monitoring Technology Exchanges'[89] organised by the NIS in 2006 to share cyber threat information among the public, private and military sectors. The council consists of 5 government organisations including the NCSC, KISA and Cyber Operations Command along with 19 domestic security companies specialised in security monitoring, and it holds both regular and special

[87] 2020 국내 정보보호산업 실태조사 보고서 (2020 Survey for Information Security Industry in Korea; Written in Korean), Korea Information Security Industry Association, 30.06.2021 https://www.kisia.or.kr/bucket/uploads/2021/06/30/%E2%98%852020%20%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EC%82%B0%EC%97%85%20%EC%8B%A4%ED%83%9C%EC%A1%B0%EC%82%AC_%EC%9B%B9_%EC%95%95%EC%B6%95.pdf.

[88] 민간부문 정보보호 종합계획 2019 (Comprehensive Plan for Information Protection in the Private Sector in 2019; Written in Korean), the Ministry of Science and ICT, 15.01.2019, https://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=4&dno=2333&fseq=2.

[89] National Cyber Security Centre 2020 ANNUAL REPORT, National Cyber Security Centre, 14.05.2020, p.31, https://www.ncsc.go.kr:4018/cmm/fms/FileDown.do?atchFileId=FILE_000000000001472&fileSn=0.

meetings when necessary to exchange detection techniques and discuss new types of cyber campaigns. The NIS, MSIT, MND and FSC also operate various advisory committees to get advice from academia and industry when making important policy decisions. One example is the Korea Cryptography Forum,[90] to receive policy and technical advice concerning national cryptography. In addition, the ROK government makes great efforts to prevent advanced technology leakage from the private sector. The NIS established the National Industrial Security Centre in 2013 to provide focal services such as preventing the leakage of advanced technologies abroad, providing industry security training, consulting and operating an industrial espionage reporting office.[91] In the military sector, the DSSC conducts security assessments and provides consulting services for defence contractors to prevent the leakage of confidential information in pursuance of the Defence Security Support Command Decree.

[90] The Korea Cryptographic Forum was launched in June 2011 by the NIS and has carried out various activities such as advice on national cryptographic policies and education/training for industries.
[91] The 'Act on the Prevention and Protection of Industrial Technology Leakage' stipulates that the Korean government shall implement comprehensive activities of preventing industrial technology leakage. Against this backdrop, the National Industrial Security Centre was established within the NIS.

References

Policy

National Cyber Security Strategy, National Security Office, 03.04.2019, https://www.msit.go.kr/bbs/view.do?sCode=user&bbsSeqNo=68&nttSeqNo=1735913.

국가 사이버안보 기본계획 (National Cyber Security Base Plan; Written in Korean), Authored by relevant Ministries of Korean Government, 03.09.2019, https://www.korea.kr/common/download.do?tblKey=GMN&fileId=187917483

Law

국가정보원법 (National Intelligence Service Act; Written in Korean), 15.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EA%B0%80%EC%A0%95%EB%B3%B4%EC%9B%90%EB%B2%95.

사이버안보 업무규정 (Cyber Security Operational Rule; Written in Korean), Presidential Decree No. 31356, 31.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EB%B3%B4%EC%97%85%EB%AC%B4%EA%B7%9C%EC%A0%95.

보안업무규정 (Security Operational Rule; Written in Korean), Presidential Decree No. 31354, 31.12.2010, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EB%B3%B4%EC%95%88%EC%97%85%EB%AC%B4%EA%B7%9C%EC%A0%95.

국가사이버안전관리규정 (National Cyber Security Management Regulation; Written in Korean), Presidential Directive No. 316, 02.09.2013, https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2000000100482.

전자정부법 (Electronic Government Act; Written in Korean), 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EC%A0%95%EB%B6%80%EB%B2%95.

공공기록물 관리에 관한 법률 시행령 (Enforcement Decree of the Public Records Management Act; Written in Korean), 05.01.2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B3%B5%EA%B3%B5%EA%B8%B0%EB%A1%9D%EB%AC%BC%EA%B4%80%EB%A6%AC%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0%EC%8B%9C%ED%96%89%EB%A0%B9.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 (Act on Promotion of Information and Communications Network Utilisation and Information Protection; Written in Korean), 09.06. 2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0.

정보통신 기반보호법 (Act on the Protection of Information and Communications Infrastructure; Written in Korean), 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EA%B8%B0%EB%B0%98%20%EB%B3%B4%ED%98%B8%EB%B2%95.

주요정보통신기반시설 취약점 분석・평가 기준 (Vulnerabilities Analysis and Assessment Criteria for Key Critical Information Infrastructure; Written in Korean), The Ministry of Science and ICT Notice No. 2021-103, 29.03.2021, https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A3%BC%EC%9A%94%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EA%B8%B0%EB%B0%98%EC%8B%9C%EC%84%A4%EC%B7%A8%EC%95%BD%EC%A0%90%EB%B6%84%EC%84%9D%C2%B7%ED%8F%89%EA%B0%80%EA%B8%B0%EC%A4%80.

지능정보화 기본법 (Framework Act on Intelligent Informatisation; Written in Korean), 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A7%80%EB%8A%A5%EC%A0%95%EB%B3%B4%ED%99%94%EA%B8%B0%EB%B3%B8%EB%B2%95.

정보보호 산업의 진흥에 관한 법률 (Act on the Promotion of Information Security Industry; Written in Korean), 21.02. 2018, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EC%82%B0%EC%97%85%EC%9D%98%20%EC%A7%84%ED%9D%A5%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%95%EB%A5%A0.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 (Act on the Development of Cloud Computing and User Protection; Written in Korean), 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C%EC%BB%B4%ED%93%A8%ED%8C%85%20%EB%B0%9C%EC%A0%84%20%EB%B0%8F%20%EC%9D%B4%EC%9A%A9%EC%9E%90%20%EB%B3%B4%ED%98%B8%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%95%EB%A5%A0.

전자서명법 (Digital Signature Act; Written in Korean), 09.06.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EC%84%9C%EB%AA%85%EB%B2%95.

전자금융거래법 (Electronic Financial Transactions Act; Written in Korean), 19.05.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B1%B0%EB%9E%98%EB%B2%95.

전자금융감독규정 (Regulation on Supervision of Electronic Financial Transactions; Written in Korean), Financial Services Commission Notice No. 2018-36, 21.12.2018, https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B0%90%EB%8F%85%EA%B7%9C%EC%A0%95.

의료법 (Medical Service Act; Written in Korean), 29.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%9D%98%EB%A3%8C%EB%B2%95.

중소기업기술 보호 지원에 관한 법률 (Act on Support for Protection of Technologies of Small and Medium Enterprises; Written in Korean), 20.10.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A4%91%EC%86%8C%EA%B8%B0%EC%

97%85%EA%B8%B0%EC%88%A0%EB%B3%B4%ED%98%B8%EC%A7%80%EC%9B%90%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0.

국방정보화 기반조성 및 국방정보자원관리에 관한 법률 (Act on Establishment of Infrastructure for Informatization of National Defence and Management of Informational Resources for National Defence; Written in Korean), 06.09.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EB%B0%A9%EC%A0%95%EB%B3%B4%ED%99%94%20%EA%B8%B0%EB%B0%98%EC%A1%B0%EC%84%B1%20%EB%B0%8F%20%EA%B5%AD%EB%B0%A9%EC%A0%95%EB%B3%B4%EC%9E%90%EC%9B%90%EA%B4%80%EB%A6%AC%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%95%EB%A5%A0.

산업기술의 유출방지 및 보호에 관한 법률 (Act on the Prevention and Protection of Industrial Technology Leakage; Written in Korean), 31.03.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%B0%EC%97%85%EA%B8%B0%EC%88%A0%EC%9D%98%EC%9C%A0%EC%B6%9C%EB%B0%A9%EC%A7%80%EB%B0%8F%EB%B3%B4%ED%98%B8%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0.

방위산업기술 보호법 (Defence Technology Security Act; Written in Korean), 22.12.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EB%B0%A9%EC%9C%84%EC%82%B0%EC%97%85%EA%B8%B0%EC%88%A0%EB%B3%B4%ED%98%B8%EB%B2%95.

사이버작전사령부령 (The Cyber Operations Command Decree; Written in Korean), Presidential Decree No. 29561, 26.02.2019, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%AC%EC%9D%B4%EB%B2%84%EC%9E%91%EC%A0%84%EC%82%AC%EB%A0%B9%EB%B6%80%EB%A0%B9.

군사안보지원사령부령 (The Defence Security Support Command Decree; Written in Korean), Presidential Decree No. 29561, 04.02.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%B0%EC%82%AC%EC%95%88%EB%B3%B4%EC%A7%80%EC%9B%90%EC%82%AC%EB%A0%B9%EB%B6%80%EB%A0%B9.

전기통신사업법 (Telecommunications Business Act; Written in Korean), 19.10.2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EA%B8%B0%ED%86%B5%EC%8B%A0%EC%82%AC%EC%97%85%EB%B2%95.

통신비밀보호법 (Protection of Communications Secrets Act; Written in Korean), 16.03. 2021, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%86%B5%EC%8B%A0%EB%B9%84%EB%B0%80%EB%B3%B4%ED%98%B8%EB%B2%95.

개인정보 보호법 (Personal Information Protection Act; Written in Korean 04.02.2020, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95.

Other

2021 국가정보보호백서 (2021 National Information Security White Paper; Written in Korean), Authored by relevant Ministries of Korean Government, 10.05.2021, https://www.ncsc.go.kr:4018/cmm/fms/FileDown.do?atchFileId=FILE_000000000001506&fileSn=0.

National Cyber Security Centre 2020 ANNUAL REPORT, National Cyber Security Centre, 12.05.2020, https://www.ncsc.go.kr:4018/cmm/fms/FileDown.do?atchFileId=FILE_000000000001472&fileSn=0.

National Cyber Security Centre 2021 ANNUAL REPORT, National Cyber Security Centre, 31.12.2021, https://www.ncsc.go.kr:4018/cmm/fms/FileDown.do?atchFileId=FILE_000000000002233&fileSn=0.

2020 Defence White Paper, the Ministry of National Defence, December 2020, https://www.MND.go.kr/user/MND/upload/pblictn/PBLICTNEBOOK_20210630030042668O.pdf.

Acronyms

ADD	Agency for Defence Development
C-TAS	Cyber Threats Analysis System
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CSTEC	Cyber Security Training & Education Centre
DAPA	Defence Acquisition Program Administration
DSSC	Defence Security Support Command
FSC	Financial Services Commission
FSEC	Financial Security Institute
FSS	Financial Supervisory Service
KCTI	Korea Cyber Threat Intelligence
KISA	Korea Internet & Security Agency
KLID	Korea Local Information Research and Development Institute
MFDS	Ministry of Food and Drug Safety
MND	Ministry of National Defence
MOFA	Ministry of Foreign Affairs
MOHW	Ministry of Health and Welfare
MOIS	Ministry of the Interior and Safety
MOLIT	Ministry of Land, Infrastructure and Transport
MOTIE	Ministry of Trade, Industry and Energy
MSIT	Ministry of Science and ICT
MSS	Ministry of SMEs and Start-ups
NCSC	National Cyber Security Centre
NCTI	National Cyber Threat Intelligence
NIS	National Intelligence Service
NSC	National Security Council
NSO	National Security Office
NSR	National Security Research Institute
PIPC	Personal Information Protection Commission
ROK	Republic of Korea
SME	Small and Medium-sized Enterprises