UK Defence &
Security Exports

Homeland Security

Market Intelligence Report 2021

Part of

Department for International Trade

Report prepared by

Intralink

Registered in England. 2438141
www.intralinkgroup.com

Table of Contents

Table of Tables

Table of Figures

1. Introduction

South Korea (Korea) faces a unique set of security challenges due to its natural and geopolitical environments as well as its highly connected and digitised society. The country has made significant investments over the past decade in areas such as disaster response, cybersecurity, critical infrastructure, aviation and maritime security. This spending is set to continue over the coming years, creating opportunities for UK-developed solutions with strong value propositions.

The size of Korea's homeland security market, including both public and private expenditure, is estimated to reach KRW 5.41tn (GBP 3.84bn) in 2021, an increase of 2.3% from 2020. In the coming years, President Moon Jae-in's Korean New Deal will see KRW 44.8tn (GBP 28.5bn) invested in furthering the digitisation of government, society and the economy. An increasingly connected country will need to secure its digital infrastructure through best-in-class cybersecurity technologies. However, Korea still has a comparatively weak digital infrastructure that has often left it vulnerable to attack by both state and non-state actors.

Recent administrations have prioritised investments in public safety in response to incidents such as the 2014 Sewol ferry disaster, ongoing cyberattacks against banks and nuclear power plants, as well as new threats such as drones and spycams. The country has developed an integrated, data-driven disaster response system which, among other things, proved decisive in its much-lauded handling of the COVID-19 pandemic. As a result of that success, the Korean economy is expected to emerge from the pandemic having recorded a contraction of just 1.1% in 2020 and is projected to grow more than 3% in 2021.

Specific areas of opportunities for UK firms include cybersecurity products and services that can detect and respond to threats, as well as solutions to secure an increasingly cloud-based, data-driven infrastructure. AI and data processing capabilities, including images and videos, will find interest for aviation security, disaster response and post-pandemic public safety protocols. Leading Korean automotive OEMs and defence contractors are working on autonomous mobility solutions for land, air and sea, meaning companies that can deliver or secure these technologies will also find opportunities. The aviation sector is expected to present continued demand for aircraft components, maintenance, avionics and sensors, as well as new business areas such as anti-drone solutions capable of detecting or mitigating intrusions in a range of settings.

The Korean market is not without its challenges, particularly for companies seeking to do business in the public security sector. UK companies may find the public sector procurement process difficult to navigate without an in-country partner, while regulatory differences may impede the adoption of new technologies. We recommend that UK companies seeking to take advantage of opportunities in the Korean market work with a local channel partner – a systems integrator (SI) or value-added reseller (VAR), for example that can combine their technology into a solution for delivery to government end-users. A well-positioned local partner can identify lucrative projects in the public sector while taking on the responsibility for navigating the procurement and regulatory processes.

2. Public Security

Korea faces a diverse array of homeland security challenges aside from the geopolitical tension with neighbouring countries and the persistent nuclear threat from North Korea. These challenges include natural disasters, drones, maritime territorial disputes, chemical and biological weapons, as well as threats to its critical infrastructure. Korea relies on a network of government agencies, the national police agency and its armed forces to meet the challenge of these threats.

The estimated size of Korea's homeland security market, including both public and private expenditure, in 2021 is KRW 5.41tn (GBP 3.84bn) an increase of 2.3% from 2020.[1] Approximately two-thirds of the market focuses on physical assets, while the remaining one-third represents Korea's rapidly growing cybersecurity market. Korean public sector customers have made major improvements in their capabilities in recent years, particularly in areas such as cybersecurity and anti-drone detection but will need to make continued investments in new technology to counter emerging threats.

2.1. Public safety

Korean National Police Agency (KNPA) statistics show 3,108 reported crimes per 10,000 people, about half that of the UK.[2] Similarly, the national homicide rate is approximately 1.0 per 100,000, several times lower than the OECD average of 3.7.[3] However, the proportion of Koreans who feel safe walking alone at night (67%) is actually lower than the OECD average of 68%.[4] Major public safety issues in Korea include violence against women, illicit filming and the high rate of traffic fatalities.

In 2016, a high-profile murder of a woman in a public toilet near Seoul's Gangnam station highlighted weaknesses in public safety, particularly women's safety, as the perpetrator specifically targeted the victim as a woman.[5] The use of spycams and illicit filming is also a major issue, with the number of reported cases almost doubling in the last five years.[6] The illicit installation of spycams has been reported in many public places, including schools, hospitals, workplaces and public bathrooms.

Korea also has a high rate of traffic fatalities at 8.1 deaths per 100,000 people, approximately 60% higher than the OECD average of 5.2. The rate of pedestrian fatalities is 3.3 per 100,000, almost triple the OECD average of 1.0.[7]

The Korean National Police Agency is Korea's national police force and deals with street crimes, emergencies, and public threats. Major cities such as Seoul, Busan and Daegu have their own police agencies, as does each province. The KNPA's Special Weapons and Tactics (SWAT) unit is charged with counterterrorism operations and responsible for serving high-risk arrest warrants, and hostage rescues.

> Industry Insider's Thoughts
>
> Out of all public institutions, the KNPA leads in the adoption of CCTV. KNPA spends the most on R&D for security equipment and smart safety infrastructure.
>
> Dr Joo Lak Lee, Professor – Department of Industrial Security, Chung-Ang University

Local governments have responded to concerns about crime in part by introducing design features such as mirrors, emergency bells, LED signs, and CCTV cameras. The city of Seoul also launched the Get Home Safely Scout app, aimed at women walking at night, that allows users to a call for police assistance through the app.

2.2. CBRN

The largest risk for nuclear hazards and chemical accidents in South Korea is from North Korea, which possesses both nuclear and chemical weapons. Experts consider North Korea to have stockpiled its chemical weapons near the Demilitarized Zone (DMZ) which separates the two Koreas. South Korea regularly holds civil defence drills that account for the risk of a chemical weapon attack and mass transit stations in Seoul have gas masks ready for use in case of a chemical or biological attack.

South Korea also has 24 nuclear power plants which supply one-third of its electricity. In 2016, Korea experienced a potential nuclear plant disaster when two earthquakes each over 5.0 magnitude hit Gyeongju, the southern city near many of South Korea's nuclear reactors. Although none of the plants was directly affected, four were shut down as a precautionary measure.

Korea's Chemical, Biological, Radiological, and Nuclear (CBRN) Command is established under the Korean Armed Forces to set up safety and security training protocols in response to potential CBRN-related disasters. During the onset of the COVID-19 pandemic in the Daegu metropolitan area, the CBRN Command was deployed to support quarantine enforcement in universities and hospitals.

2.3. Disaster response

Korea is prone to typhoons, floods, and landslides. In August 2020, heavy rains in what was Korea's longest rainy season in years, caused flooding and landslides across the country, killing 30 and leaving 12 missing.[8] A total of four typhoons also struck the Korean peninsula in 2020, the most in a single season as Korea typically sees just one typhoon make landfall.[9] Landslides caused by heavy rain during the summer are also a perennial concern.

Government data indicate that the size of the overall disaster response market as of 2019 was KRW 12.6tn (GBP 8.0bn), largely fragmented across thousands of small companies.[10] The National

Disaster and Safety Status Control Center under the Ministry of the Interior and Safety (MOIS) manages nationwide response and operating procedure for all disasters. The Korea Meteorological Association (KMA) monitors for potential anomalies in weather and seismic activity. KMA recently instituted an Earthquake Early Warning (EEW) system to monitor for earthquakes. When signs of earthquakes are detected, the EEW system deploys immediate alerts to local government agencies.

Korea has been widely praised for the effective containment of the COVID-19 pandemic, with total infections limited to just over 90,000 as of March 2021. The country initially witnessed a quick spike of cases in February 2020, but quickly contained the spread of the disease by instituting contract tracing, setting up high-volume testing sites, and instituting a mandatory quarantine system in the early weeks of the pandemic. In the second year of the pandemic, the success of contact-tracing technology, mobile entry logs and health reporting has been crucial. Korea's response to the pandemic has been coordinated by the Korea Disease Control and Prevention Agency, the Ministry of Health and Welfare (MOHW), and the Ministry of Interior and Safety (MOIS).

2.4. Maritime security

The Korean peninsula is surrounded by water on three sides and South Korea has longstanding maritime territorial and boundary disputes with North Korea, Japan, and China. The disputes over Dokdo, an island controlled by South Korea but claimed by Japan, and demarcation of an exclusive economic zone (EEZ) in the surrounding seas contribute to strained relations between South Korea and Japan.

Relations between China and South Korea are made more difficult by unresolved EEZ boundaries and widespread illicit fishing by Chinese vessels in South Korean waters. The Northern Limit Line (NLL) serves as the maritime boundary between the two Koreas but this boundary is not recognized by North Korea, meaning that it continues to be a source of contention between the two nations.

Korea's maritime surveillance continues to develop by incorporating new technology such as communication devices, sensors and radars to counter illegal fishing activities and to improve search and rescue methods. The Korea Coast Guard, which is responsible for coastal security duties, was disbanded in 2014 after the Sewol ferry disaster and absorbed into the Ministry of Public Safety and Security, now known as the Ministry of the Interior and Safety (MOIS). In 2017, the Korea Coast Guard was re-established under the Ministry of Oceans and Fisheries.

Coastal authorities have been criticised for their loose surveillance as the frequency of undetected North Korean fishing vessels has increased in the recent years. In September 2019 Korea developed a new maritime surveillance radar, the Surveillance Radar-II at an estimated cost of USD 27m. The radar monitors vessels such as hovercraft and high-speed boats, as well as aircrafts flying at low altitudes. The radar transfers the data to the Korean Naval Tactical Data System.[11] Defence contractor LIG Nex1 also introduced a real-time remote management system for maritime vessels in 2020.[12]

The government also amended the Coast Guard Affairs Act in December 2020 to expand the focus of the Coast Guard to include new terror threats arising from 4IR technologies such as drones and autonomous surface ships. The Coast Guard also plans to revise its Maritime Counterterrorism Plan every five years.[13]

2.5. Aviation security

Incheon International Airport (IIA) is Korea's largest international air transport and cargo hub, operated by Incheon International Corporation (IIAC). Incheon Airport ranks as one of the busiest airports worldwide for passenger and cargo traffic, ranking 14th and 5th respectively. Korea Airports Corporation (KAC) is a public-private consortium that also operates 14 airports in Korea including Gimpo and Jeju Airports. Civil aviation security in Korea is directly handled by IIAC and KAC under the significant legislative and regulatory influence of MOLIT. Customs and immigration services at international airports are handled by the Korea Customs Service (KCS) and the Korea Immigration Service (KIS) respectively.

MOLIT statistics from 2019 indicate overall spending on aviation security equipment was KRW 95.3bn (GBP 61.2m).[14] Key issues in aviation security in Korea include international terrorism and smuggling as well as the increasing prevalence of drones. Incheon Airport has been breached by drones on multiple occasions, leading to flights being diverted and grounded.[15] Incheon Airport installed anti-drone radars in mid-2020 capable of detecting, identifying and neutralizing radars, but a breach in November 2020 raises questions about the efficacy of the solution.

Korea's aviation industry plans to institute touch-free technologies to simplify the passenger experience and reduce human interaction by relying on greater automation.[16] Incheon Airport is among the first airports worldwide to deploy autonomous vehicles capable of carrying passengers and cargo.[17] Incheon Airport has a long-term strategy to transform into a smart airport by 2025 through an integrated passenger and freight security management system using biometric information systems.

In February 2021, the Korean government approved construction of a new airport in Busan, Korea's second-largest city, that will significantly increase capacity over the existing Gimhae Airport. The new airport, named for its location on the island of Gadeok-do off Korea's southern coast, will connect Busan to more than 100 cities in 39 countries, including 18 cities in 14 European countries, and increase the number of international flights from 1,306 to 3,000. Several analyses have indicated that construction will likely exceed MOLIT's estimate of KRW 28.6tn (GBP 18.4bn).[18] Major issues to be addressed in the airport's construction and operation will be the suitability of the site, which will require significant engineering work, as well safety concerns related to air traffic congestion from Busan's current Gimhae International Airport, which is less than 20 km from Gadeok-do.[19]

2.6. Large events

Korea has significant experience in hosting major international events, including the 1988 Summer Olympics, the 2002 FIFA World Cup, the 2010 G20 Summit, the 2018 Winter Olympics and numerous high-level bilateral summits. According to the Ministry of Economics and Finance, of the KRW 130bn (GBP 83.4m) budget to host the G20 Summit, KRW 27bn (GBP 17.3m) was used for security and safety procedures. As for the 2018 Winter Olympics in Pyeongchang, the Presidential Protection Services reported that around KRW 1.9bn (GBP 1.2m) out of the event's total budget, KRW 2.4tn (GBP 1.6bn), was used for security, which primarily focused on protecting foreign heads of state or officials.

Korea also regularly sees large public gatherings, including political rallies, with participants numbering in the tens of thousands or even higher. Since the outbreak of COVID-19, many such large-scale events have been canceled or postponed.

The Korean National Policy Agency (KNPA) is responsible for public safety, riot control and dignitary protection. The KNPA is able to deploy large numbers of auxiliary police officers for large events as necessary, but the auxiliary police are scheduled to be abolished in 2023.[20] For potential counter-terrorism activities and in security planning for major events, the National Intelligence Service (NIS) houses an enforcement function under its Threat Information Integration Center.

2.7. Critical infrastructure

The Korean government designates various types of infrastructure, including power plants, transportation hubs, bridges, tunnels, ports and telecommunications networks, as vital to national security under the United Defense Act. The designation is made by the Ministry of Defense (MND) in consultation with other government agencies, including the National Intelligence Service (NIS).

Korea has more than 100 power plants, most notably 60 coal plants and 24 nuclear power plants. The Nuclear Safety and Security Commission (NSSC), established in 2011, is the primary organisation responsible for standards and regulations related to nuclear power plant security. The Ministry of Science and ICT (MSIT) and the Ministry of Trade, Industry and Energy (MOTIE) also play a role in the security of power plants, as do plant operators such as the state-owned Korea Hydro & Nuclear Power (KHNP). A 2014 cyberattack against KHNP, eventually attributed to North Korea, led to data such as blueprints being compromised.[21]

A key issue for power plants has been reports of drone sightings and the failure to prevent or identify the source of these breaches, highlighting the need for better solutions. Korea first established security guidelines against drones in 2015, establishing a manual for immediate response measures such as circulation of information and cooperation with local authorities to track the source.[22] From 2015 to late 2019, the MSIT reported 13 sightings and the drone operator could not be identified in seven of the cases.[23] Recent reports suggest more frequent sightings over some facilities with

Busan Police reporting a total of 14 cases from August 2019 to June 2020. While some culprits were fined, in other cases the drone operators could not be identified.[24]

In November 2018, a large portion of Seoul suffered internet and phone disruptions caused by a fire at a KT facility in western Seoul. The fire burned a 150-metre-long tunnel through which underground network cables passed and was extinguished after 10 hours. The incident highlighted the vulnerability of cable network infrastructures and KT in response implemented a new detection system that uses artificial intelligence and cloud computing to detect temperature changes and immediately extinguish the fire.

The fire at the KT facility became a major catalyst for change and the Ministry of Science and the ICT (MSIT) established its Telecommunications Disaster Management Committee in January 2019. The Committee classifies telecommunication facilities by their size and level of impact and implements measures to prevent and respond to disasters. Greater security measures are required for facilities classified higher in the grading system.[25]

Security for Korea's land transport network, including railways and bridges, is handled by the Ministry of Land, Infrastructure and Transport (MOLIT) in coordination with the Korea Railroad Corporation (Korail), local governments and police agencies. Securities to ports is handled by individual port operators as well as the Ministry of Oceans and Fisheries. In 2016, threats from North Korea aimed at the Han River Rail Bridge in central Seoul, as well as the broader rail network, prompted the installation of a thermal imaging camera on the bridge. Korail also installed unmanned security systems and infrared detectors at its train depots.

3. Cybersecurity

3.1. Background

Korea is a highly digitised and connected country with the world's fastest internet speed, the highest rate of broadband penetration and the highest rate of smartphone ownership. However, the advancement of Korea's digital infrastructure has outpaced the development of its cybersecurity infrastructure, which has suffered attacks from both domestic and overseas actors.

Major cyberattacks in South Korea attributed to North Korea date back to at least 2011, when a DDoS attack on the South Korean bank Nonghyup paralysed its servers and left customers unable to access their accounts for three days. Subsequent attacks by North Korean actors have managed to shut down TV networks and banks, and breach the defence of a nuclear reactors. A Korean web-hosting company paid USD 1m (GBP 780,000) after the Erebus ransomware attack in 2017 denied access to servers hosting the websites of more than 3,000 companies. In recent years, 91% of the country's cyberattack cases resulting in leaks of technology information have occurred to SMEs, highlighting their vulnerability. As a consequence of these attacks, the Ministry of National Defence's white papers have designated North Korea's cyberattacks as a main security threat.

The cybersecurity market has grown with a rapid increase in the number of domestic firms entering the space, rising more than 50% from 311 to 473 between 2016 and 2019. However, relatively low levels of spending on cybersecurity in both the public and private sectors, as well as a similarly low public awareness of the importance of information security contributes to a continued weakness in Korea's digital infrastructure. The Korean government's cybersecurity spending, based on the 2021 MSIT budget of KRW 240 bn (GBP 151 m), is far below that of other nations such as Japan (JPY 88.1bn or GBP 581m) or the United States (USD 17.4bn or GBP 12.6bn).

According to MSIT statistics, Korea's cybersecurity market was estimated to be worth KRW 1.98tn (GBP 1.26bn) in 2020, largely controlled by Korean firms such as SK Infosys and global players such as Microsoft, Symantec and Cisco. A significant amount of work is also done by systems integrators, typically the IT arms of major conglomerates such as Samsung SDS, LG CNS or SK C&C, who provide cybersecurity solutions as part of broader platforms. Spending on tools and products accounts for 75% of the market (KRW 1.49tn or GBP 941m), while the remaining quarter is for services (KRW 487 bn or GBP 307m). In terms of end users, government customers (35%) and financial institutions at 18% represent more than half of all purchasing, with other private companies accounting for the rest.

The MSIT categorizes products into network security tools, the largest single category at KRW 468bn (GBP 300m), followed by information leakage prevention (KRW 311bn or GBP 198m) and system-level security (KRW 216.9bn or GBP 138m). Services are driven chiefly by design and

installation projects, worth KRW 204bn (GBP 130m) in 2020, followed by consulting and maintenance services, worth KRW 115bn (GBP 73m) and KRW 112bn (GBP 71m) respectively.

Table 1: Cybersecurity Market Size by Total Sales 2020-2022

Market	Types	2020	2021	2022
Products	Network security	300m	313m	325m
	System security	138m	140m	147m
	Contents/information leakage prevention	198m	202m	209m
	Password/authentication	57m	62m	72m
	Encryption	101m	103m	110m
	Other	155m	156m	162m
	Total	949m	976m	1.02bn
Services	Consulting	73m	75m	77m
	Maintenance	77m	74m	80m
	Projects	129m	133m	139m
	Training/education	955,000	1m	2m
	Authentication services	34.8m	37m	44m
	Total	314m	320m	342m

Source: Korea Information Security Industry Association & MSIT

3.2. Key players

Over half of the Korean cybersecurity market is controlled by domestic firms selling largely to small and medium-sized companies, as well as public sector customers. However, approximately 40% of the market consists of imported solutions, mostly from American companies such as Microsoft, Symantec and Cisco. Industry experts generally regard the most sophisticated solutions to come from overseas, recognising Korea's comparative weakness in both in terms of technology and human resources in this field. A significant proportion of the domestic companies are SMEs with no very large, specialised players. Growing demand for higher security standards from the government, however, has led local firms to offer increasingly specialised products that keep pace with global best practices.

The largest domestic player is SK Infosec (annual revenue of KRW 270bn or GBP 172m) which specialises in consulting, monitoring and systems integration. SK Infosec is followed by Ahnlab, best known for its online and network security solutions, with annual revenue of KRW 178.2bn (GBP 113m), anti-DDOS and IDS specialists SECUI (KRW) and Wins (KRW) as well as Igloo Security (KRW), which offers integrated enterprise solutions. In late 2020, SK Infosec merged with a fellow

subsidiary of the largest mobile telecommunications service provider SK Telecom, ADT Caps, which focuses on physical security, to create one of Korea's largest security companies. The new company, with combined revenues in excess of KRW 1tn (GBP 640m), will offer integrated security solutions as a competitor of Samsung's S1, which has revenues of KRW 2.2tn (GBP 1.39bn), largely from its physical security business. S1's cybersecurity offerings include antivirus programs, VPNs and intrusion detection systems.

A significant portion of the market is controlled by systems integrators (SIs) who are capable of delivering integrated systems with built-in security features for large customers with complex needs. Most major Korean conglomerates have an IT arm that counts among the leading SIs in Korea, with Samsung SDS, LG CNS and SK C&C being notable examples. Samsung SDS offers consulting, threat detection and response, AI-based cloud security and network security solutions such as firewall and authentication. Along with significant experience in smart factory platforms, LG CNS has developed a specialty in providing public sector digitisation services, a process that is expected to accelerate with the Digital New Deal. Key projects include an inter-agency criminal information database used by the KNPA, Supreme Prosecutor's Office and Ministry of Justice.[26] Major SIs can also acquire promising startups or major players, with Samsung SDS' majority stake in SECUI being one example.

Domestic firms are increasingly investing in a range of new cybersecurity technology such as AI, biometrics and big data develop total security solutions. AhnLabs recently acquired Jason, an AI-based data leakage prevention startup working with financial institutions and conglomerates, while S1 is investing in integrated solutions customised for aviation and healthcare, aiming to help lower the upfront cost of adopting a security solution. KISA is overseeing multiple projects to develop encryption technology, including one in cooperation with Korea's major telecommunications service providers and the MSIT against attacks on 5G technology. Another project involves the development of quantum cryptography in cooperation with a major defence contractor Hanwha, SK Telecom again and its Swiss subsidiary ID Quantique.

Table 2: List of key players in the information security industry

Company	2019 Sales	Employees	Key Products	Key Target Industries
SK Infosec	172m	1,065	Managing security services, consulting, SI	Public sector
Ahnlab	103m	1,211	Antivirus, online security, network security, firewalls, IPS and UTM	Public sector, financial institutions
SECUI	76m	399	Intrusion prevention systems, anti-DDoS security, vulnerability analysis, unified management systems	Financial institutions, gaming

Company	2019 Sales	Employees	Key Products	Key Target Industries
WINS	48m	408	Intrusion prevention, firewall, DDoS response, APT protection, integrated security monitoring, video privacy	Public sector, financial institutions
IGLOO SECURITY	48m	864	Managed security service and enterprise security management	Enterprise
KICA	27m	85	Licensed Korean certification authority; provides identity confirmation, secure transaction guarantees, compensation system	Public sector institution, financial institutions
SGA Solutions	25m	175	Antivirus, server security, firewalls, intrusion prevention and VPN	Public sector
Fasoo	17m	227	Secure printing solutions	Financial institutions, gaming
Penta Security Systems	17.5m	213	Firewalls, encryption and authentication	Public sector, financial institutions
NICSTECH	7m	119	Personal/enterprise network security, web/mobile service implementation	Enterprise
Genians	15.8m	140	Cloud-managed network access control, IT security services	Public sector, financial institutions
Hancom Secure	9.8m	127	Online integrated security solutions	Public sector
Raonsecure	18m	205	Security solutions development and consulting	Financial institutions, gaming
Inca, nProtect	6.4m	122	Antivirus software, online security	Public sector, financial institution

Source: Intralink research

3.3. Trends

Vulnerabilities in the national ICT infrastructure are a major concern to the Korean government and the Office of National Security, under the presidential Blue House, recommended a number of changes in its 2019 national cybersecurity strategy. [27] The strategy calls for developing preventative and response technologies that can detect and repel attacks in real time, as well as a regulatory framework to encourage greater spending on cybersecurity from companies and public institutions. The strategy identifies raising the competitiveness of local industry and increasing the number of cybersecurity personnel as a means of achieving these greater capabilities.

Other government initiatives also call for major investments in cybersecurity, including cloud and AI-based cyber solutions, with the goal of improving Korea's ranking in the International Telecommunications Union (ITU) global cyber security index from 15th to 5th over the next two years.[28] In January 2021, the Ministry of Science and ICT (MSIT) announced KRW 670bn (GBP 427m) in funding for domestic cybersecurity capabilities.[29] The plan, in keeping with the 2019 strategy, aims to improve response capability through real-time collection of threat information and to develop an infrastructure around securing government facilities, cloud service providers and data centres. The plan also expands threat intelligence to cover sectors such as healthcare and education.

> Industry Insider's Thoughts
>
> "One strength of the Korean cybersecurity industry is that the private sector actively implements government policies and initiatives in this area."
>
> Team Leader of Communication Division of East Security

The MSIT allocated a total of KRW 240 bn (GBP 151 m) for information security in its 2021 budget, an increase of 29% compared to the 2020 budget.[30] Approximately one third of the spending (KRW 74.7bn or GBP 47.6m) is dedicated to information security R&D, while spending on incident response planning is doubled to KRW 53bn (GBP 33m) as the government seeks to build stronger digital security systems ahead of the increasing digitisation and connectivity of the economy. Other areas of spending include developing mobile-specific security and offering consulting services to SMEs lacking sophisticated security protocols.

3.4. Network security

Demand for network security solutions, defined by the MSIT as software and equipment capable of detecting and preventing attacks on networks, grew 10% in 2020 to reach KRW 825m (GBP 525m) as work-from-home became increasingly prevalent during the COVID-19 pandemic. The remote work environment especially created demand for a network security infrastructure across cloud technologies, interconnected devices, and virtual private networks (VPN) to secure private networks in public spaces. Broader government strategy, devised partly in response to high-profile

attacks, is also creating demand for Intrusion Prevention Systems (IPS) and DDoS prevention systems.

> Industry Insider's Thoughts
>
> For the Korean government, cybersecurity now applies to airports, subways systems, nuclear power plants, and industrial facilities. Security of network infrastructure in megacities is especially important as LAN wires and underground city networks of megacities are most vulnerable to network attacks.
>
> Kyu Duk Hong, Professor – Sookmyung Women's University, Korea Academic Association of Homeland Security (KAAHS)

The network security market in Korea is expected to grow approximately 10% between 2020 and 2022, with the public sector a particularly strong consumer of network security solutions.[31] Public sector customers are reported to have allocated at least KRW 52.3bn (GBP 33.3m) in 2021 budget specifically for the purchase of network security tools, with notable customers including the Ministry of National Defence, which plans to spend on KRW 20.9bn (GBP 13.3m) on encryption equipment, and KISA, which has allocated KRW 5bn (GBP 3.2m) on a malware detection system.

3.5. Threat intelligence and monitoring/ Incident response

Intelligence gathering and response capabilities are a strategic area of focus for the Korean government, which is seeking to improve the ability of public organizations and small firms to respond to threats. The ability to detect and respond to cyberattacks is a key part of the National Cybersecurity Strategy, as well as the 2021 MSIT R&D budget. Locally developed threat monitoring and response technologies are still in a development phase, but many local players have an offering, including both cybersecurity specialists and IT giants. A new development is the introduction of SOAR (Security Orchestration, Automation and Response) solutions.

More than 50 domestic companies are developing related products, including AhnLab and Igloo Security, while solutions from global players such as Palo Alto Networks and Fortinet are also available. However, some end users such as Nonghyup Bank are also investing in developing their own detect and response capabilities, perhaps pointing to the limitations of locally developed solutions in meeting industry demands.

> Industry Insider's Thoughts

> The Science and Technology Cyber Security Center at KISTI works closely with partners in industry and academia to detect malicious code and develop a coordinated threat response system such as the Asia Information System.
> Young Min Ko, Researcher – Science and Technology Cybersecurity Centre, KISTI

Korea's threat intelligence and monitoring solution providers have also integrated response functions within their products to allow for the identification of ransomware attacks and malicious code. Korea's Nuri Lab NAR (Nuri Anti-Ransom) provides a security solution which detects and blocks cryptographic behaviour and ransomware. WidgetNuri offers a whitelist-based software authentication blocking, as well as a cryptographic detection and blocking solution. Through an authentication system, the software analyses the action on the operating system to detect potential ransomware. The AhnLab Smart Defense solution has a built-in detect and block ransomware solution.

3.6. Endpoint security

The demand for endpoint detection and response (EDR) technologies has been growing rapidly globally in recent years and Korea has been no exception. Market leader AhnLab launched its first endpoint security solution in 2017 and has since diversified its offerings in this area to include AhnLab EDR, focusing on endpoint detection and response, along with AhnLab EPP, an endpoint protection platform.

> Industry Insider's Thoughts
> Endpoint threats have increased along with the prevalence of remote work, as employees used to working in an office environment often lack awareness of cyber vulnerabilities.
> General Manager – Information Protection Bureau, KISA

Another major player in Korea's cybersecurity market, INCA Internet launched its own endpoint solution product, called Tachyon, in 2018, which includes a mobile-specific version. INCA's nProtect is widely used in Korea to secure e-commerce, online gaming and financial transactions. Samsung SDS offers multiple endpoint solutions, including one through its partnership with SentinelOne, a US-based company offering an EDR platform that opened its Korean office in early 2021. Samsung SDS is also an investor in SentinelOne, which is valued at USD 3bn (GBP 2.16bn).

3.7. Encryption

Korea relies on the locally developed ARIA and SEED encryption technology standards as opposed to the internationally recognized AES encryption algorithm. In particular, ARIA and SEED technology are strongly favoured by the public sector and the NIS requires all network equipment procured by government entities to have encryption functionality based on the ARIA or SEED standards. This

even the case when dealing with facilities not generally considered to be sensitive such as educational institutions. The United States government has raised this issue in its National Trade Estimate report identifying trade barriers, including in its most recent 2020 update.[32]

Korea has increasingly strict data privacy laws that mandate the encryption of personal information. The Personal Information Privacy Act (PIPA) was amended in 2016 to require the encryption of sensitive data in various forms, such as text, image and video, that may contain national ID numbers. Further regulatory changes in 2020 created higher encryption standards for organizations storing large amounts of personal data while also expanding the type of information that must be encrypted. Many local firms have rolled out database encryption solutions to meet the increased demand. Hancom's SecureDB solution has major customers in the public and private sectors, including KISA, the National Tax Service, the Ministry of Justice and major financial institutions. Larger players such as SK C&C offer database encryption modules as security features within platform-level solutions.

3.8. Authentication

The Electronic Signatures Act was amended in December 2020 to authorise private companies' solutions for digital authentication, ending the cumbersome reliance on the public digital authentication system that required users to install Microsoft's ActiveX plugin. A number of major Korean tech firms including Naver, Kakao, Payco, BankSign and all three major mobile telecommunications service providers, are already active in the broader authentication market, estimated to be worth KRW 70bn (GBP 44.5m).[33] In December 2020, KB Financial Group's digital signature was selected by MOIS for use on government websites, beating out four other candidates.

> Industry Insider's Thoughts
>
> In Korea, when buying a house or taking out a bank loan, dozens of documents are required from various agencies but in the COVID-19 era, authentication systems should adapt to a contactless environment.
>
> Dr Ki Hyuk Lee, Professor – Department of Industrial Security, Chung-Ang University

Also in 2020, Korea's three major telecommunications service providers, SK Telecom, KT, and LG Uplus, jointly launched a blockchain-based digital identity app called Pass that can verify the user's ID and driver's licence.[34] The app, powered by the local fintech startup Aton, removes the complicated authentication procedures typically required by apps and websites for identity verification, allowing users to verify their identity via a six-digit number, fingerprint or iris recognition. Pass has close to 30 million users, well over half of Korea's total population.

3.9. IoT

Korea's IoT market, worth more than KRW 10tn (GBP 6.36bn), is among the five largest in the world. It is driven by a shift in focus from individual devices towards increasingly complex platforms and

services supported by 5G connectivity.[35] The market is projected to show strong growth in the coming years through investments in connected cars, factories, energy grids and public facilities. Smart factories, relying on technologies such as robotics, automation and sensors, have doubled between 2018 and 2020 to almost 20,000.[36]

The massive projected increase in connectivity for a breadth of applications ranging from manufacturing to mobility to governance and smart cities, as well as the speed of the networks utilized, will mean the nature of threats will diversify while the time to detect and respond will be reduced. All three major telecommunications service providers are making significant investments in securing the 5G networks expected to underpin this connectivity. The leading suppliers of smart factory platforms (Samsung SDS, LG CNS and SK C&C) all integrate security into their platforms, providing both consulting and solutions such as monitoring, access control and cloud control. SK C&C is partnering with Google Cloud Korea to supply cloud security for its smart factory platform.

> Industry Insider's Thoughts
>
> While cybersecurity challenges in today's hyperconnected society call for a control and monitoring system at bird's eye view, the government currently lacks capacity to act effectively as a central control tower.
>
> Kyu Duk Hong Professor – Sookmyung Women's University, Korea Academic Association of Homeland Security (KAAHS)

3.10. Industrial control systems (ICS)

Korea's ICS security market size as of 2020 is estimated to be KRW 91.3bn (GBP 58.2m) and has grown at an average increase of 48.8% per year since 2015.[37] ICS technology was not traditionally considered within the cybersecurity domain in Korea. However, the rapid increase of smart factories, which more than doubled between 2018 and 2020 to almost 20,000, has underscored the importance of ICS technology in the country.

> Industry Insider's Thoughts
>
> Korean companies are increasingly adopting operational technology solutions, but they usually lack awareness and education on potential cyber threats.
>
> Ki Bun Kim, General Manager – Samsung S-1

The 2018 cyberattack on Taiwanese chip supplier TSMC also prompted many Korean companies in the energy, manufacturing, and utility sectors to begin paying greater attention to dedicated protocols and securing equipment through ICS systems. POSCO ICT, the technical solutions arm of the national steelmaker POSCO, announced a jointly-developed ICS solution with Cisco in April

2019.[38] Meanwhile SECUI, one of the leading network firewall companies in Korea, is collaborating with Intel to develop solutions on ICS security monitoring and visualisation systems.

3.11. Supervisory control and data acquisition (SCADA)

The market for SCADA in Korea was worth an estimated KRW 63.7bn (GBP 40.5m) in 2020, growing steadily at an average of 6.3% annually from KRW 50.3bn (GBP 31.9m) in 2016.[39] Government-led SCADA projects are the largest segment of the market, usually related to the conversion of public infrastructure such as power plants, airports, and traffic control centres into smart facilities. Recent purchases of SCADA systems include public utility KEPCO, which installed a KRW 13.2bn (GBP 8.4m) system, as well as Incheon International Airport (KRW 2.7bn or GBP 1.71m).[40]

The SCADA market in Korea began under close collaboration between foreign and domestic companies. Local SI firm Vitzrosys entered a partnership with UK-based EuroTherm, to develop SCADA technology for sale in the Korean market. Vitzro is the market leader with 30% market share, leveraging its broader strengths in delivering complex systems for public customers such as KEPCO, Korea Railroad Corporation and the city of Seoul. Other leading companies in the Korean SCADA market include Hyundai Electric, a spinoff of global shipmaker Hyundai Heavy Industries, as well as LS Electric and Taekwang NC.

3.12. Security consulting

A total of 27 companies in Korea meet KISA's standard for information security consulting.[41] The Information Security Industry Regulations standard requires companies to have competency assessing risk factors and establish protocols to ensure the safety of information and communication facilities. Competency is assessed based on a firm's technical ability, completion of international certifications such as SIS, or PIMS, years of experience in the information security field and the cost of consulting services.

Figure 1: KISA-recognized security consulting firms

3.13. Certifications

A variety of training programmes focused on cybersecurity are run by public agencies and universities, often with financial support from the government. Financial support is expected to accelerate as a result of the Korean New Deal. The MSIT plans to grow the number of graduate schools with security programs from 8 to 12 and to support the existing training programs.

KISA established a cybersecurity professional training centre in 2012, known as K-Shield, offering free month-long training programmes for interested professionals. The Korea Information Technology Research Institute (KITRI) runs the “Best of Best” programme to train and develop young security professionals.

There are five main accreditations offered in the private sector and two types of certifications issued by the Korea Internet & Security Agency.

Table 3: Cybersecurity accreditation programmes in Korea

Certification name	Website	Organisation
Information Security/Industrial Engineer	www.kisq.or.kr	Korea Internet & Security Agency
Information Security Management System (ISMS) Certification	www.isms.kisa.or.kr/main/isms/	Korea Internet & Security Agency
Certified Privacy Protection General (CPPG)	www.cpptest.or.kr/	Korea CPO Forum
Industrial Security Expert	www.license.kaits.or.kr/	Korean Association for Industrial Technology Security
Digital Forensic Expert	www.forensickorea.org/exam/	Korean Institute of Forensic Sciences
Personal Information Protection (PIP)	www.kie.or.kr/kiehomepage/fc/licenceISMG1	Korea Information Evaluation Association

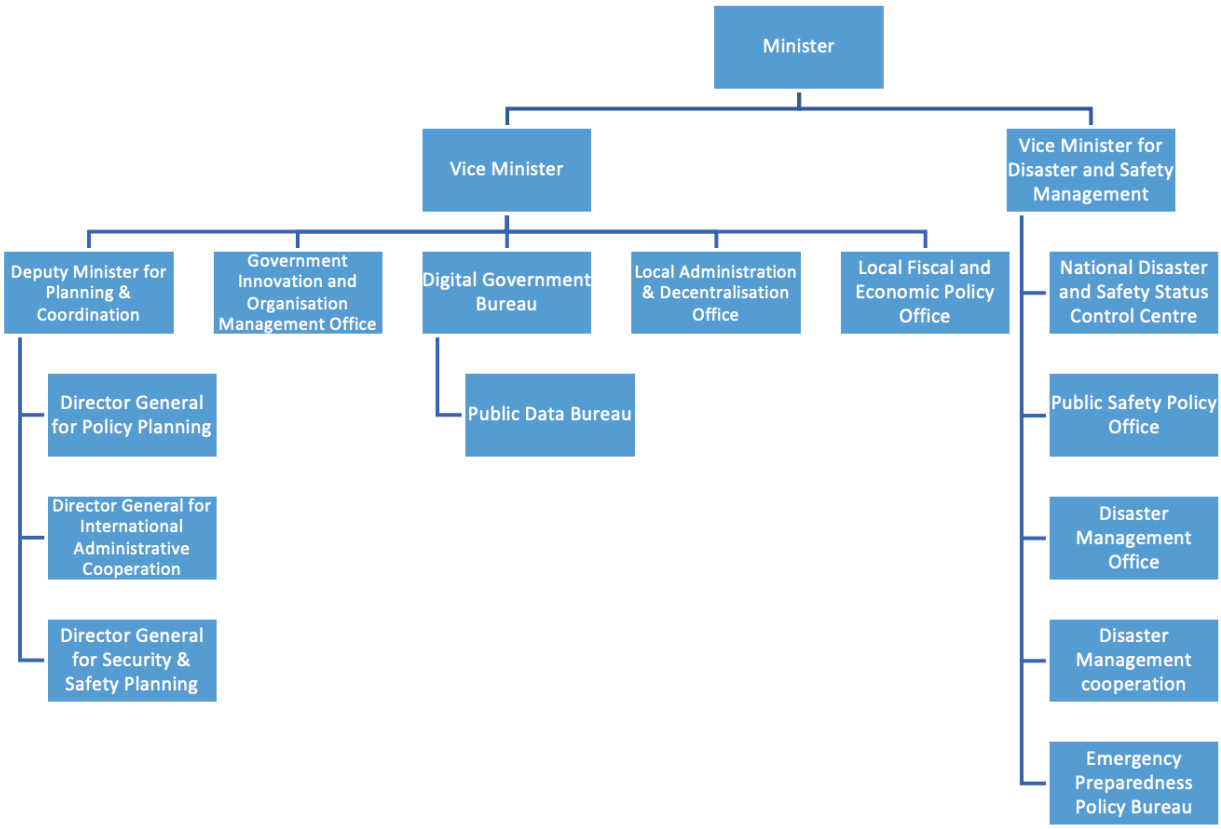
4. Government Customers

4.1. Ministry of the Interior and Safety

209 Sejong-daero, Jongno-gu, Seoul
13, Jeongbu 2cheongsa-ro, Sejong-si
www.mois.go.kr
No. of Employees: 1,472

The Ministry of the Interior and Safety (MOIS) was established in 2017 by combining the former Ministry of the Interior created in 2014 and the Ministry of the Public Safety and Security created in 2013. The Ministry is responsible for planning and operating response measures for national emergencies, civil defence and disasters. It handles general affairs of government organisations, management of public personnel and government properties, as well as government innovation and the digitisation of government services.

Figure 2: MOIS Organisational Chart



Safety and security roles

For disaster and safety management, MOIS focuses on developing response mechanisms, including the precise and timely transmission of information, the establishment of response measures and relief management. The Ministry has an Integrated Disaster Safety Information System, which supports cross-government communication and collaboration for rapid disaster response and collects data on existing disaster management systems using a 3D-geospatial information system (GIS).[42]

MOIS also runs the Public Safety Map Service to provide information on crime, traffic, natural disasters, public health and public facilities, such as police and fire stations.[43] The interactive map also features data on Covid-19, including contact tracing, testing availability and the location of public health facilities. The map has a real-time feed that alerts users of nearby potential threats. The Ministry also maintains Safety e-Report System, the online and mobile platform that enables citizens to report on security threats and accidents.

Budget and projects

MOIS announced its 2021 budget of KRW 57.4tn (GBP 36.6bn). The Ministry intends to focus strongly on disaster management, allocating KRW 520.5bn (GBP 331m) for equipment for high-risk facilities and disaster-prone geographical areas.

In March 2021 MOIS started the operation of the Korea Safe-net, the world's first LTE-based disaster and safety communications network connecting the police, fire rescue and other public agencies in cases of national-scale disasters such as forest fires, major fires in urban areas and maritime disasters. The project began in 2018 to find a higher-quality solution to real-time communication in national disasters. Connected parties will be able to transmit details (i.e. messages, photographs, videos, etc.) and updates through the network in real time to collaborate with each other. The network will be implemented throughout the police force in 2021 and extend to all relevant disaster respondents in 2022. The Ministry also plans to evaluate the network for a possible 5G convergence.[44]

4.2. National Counter-Terrorism Centre

97 Tongil-ro, Seodaemun-gu, Seoul
http://www.nctc.go.kr/nctc_en/index.do
No. of Employees: 32

The National Counter-Terrorism Centre (NCTC) was established in June 2016 under the Office of Government Policy Coordination within the Prime Minister's Office. The NCTC is the central entity in charge of Korea's national counter-terrorism activities and establishes counter-terrorism policies, operations, and safety measures. The legal basis for the Centre's establishment and its role can be found in the Act on the Counter-Terrorism for the Protection of Citizens and Public Security, Korea's first counter-terrorism law, enacted in 2016.

Roles

The NCTC assumes three main functions – prevention, response and strengthening of capabilities against terror attacks. Prevention mechanisms include the operation of terror-related information sharing systems, elimination of human and material terrorist risks and provision of protection for overseas citizens and facilities. The NCTC's rapid response system aims to respond immediately to terror-related emergencies and work closely with international partners. The Centre also works to strengthen counter-terrorism capabilities by training on-site agents, increasing the availability of personnel and equipment, as well as providing safety guidelines for the public.

The NCTC is home to the bureaux in charge of counter-terrorism activities: the Information Integration Centre, Regional Counter-Terrorism Council, and the Counter-Terrorism Council for Airport and Harbour Security.

Projects

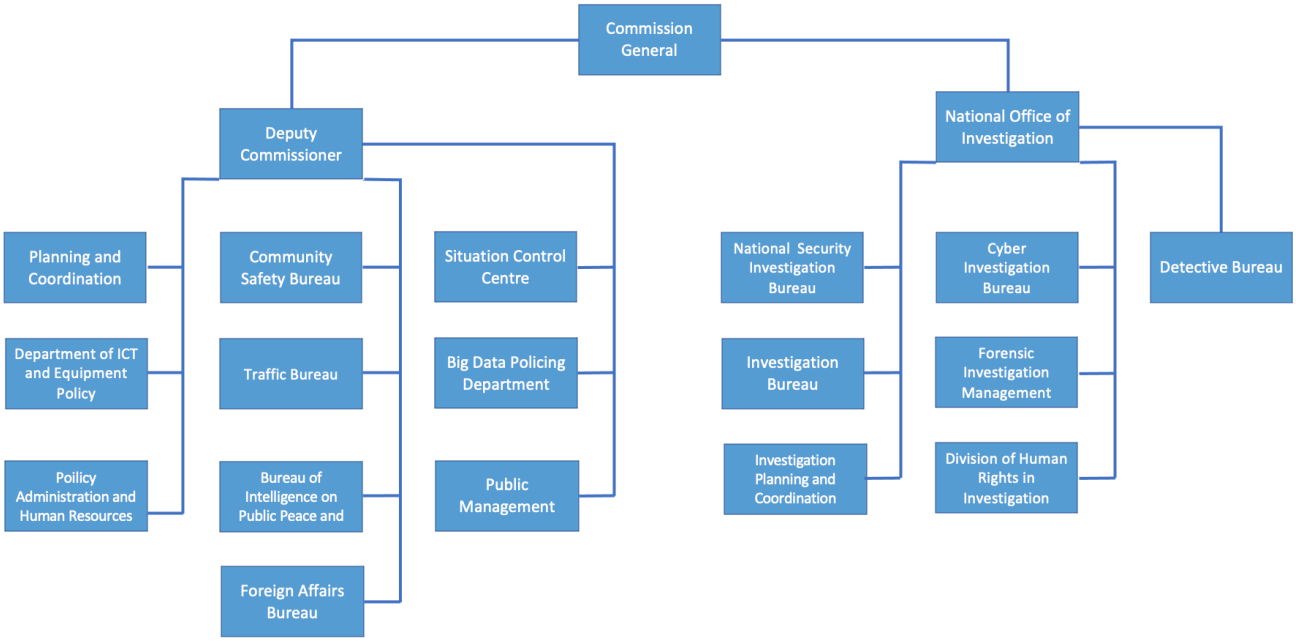
Korea continues to expand its counter-terrorism infrastructure, adding special counter-terrorism forces within regional police forces in Sejong, North Jeolla and North Gyeongsang in 2020. The NCTC stated its plans in 2021 to adopt AI and extended reality (XR) technology, as well as drone detectors and legal guidelines for anti-drone technology.[45]

4.3. Korea National Police Agency

Tongil-Ro 97, Seodaemun-gu, Seoul
www.police.go.kr
No. of Employees: 142,108

The Korea National Police Agency (KNPA) operates under the MOIS. KNPA is present in over 18 metropolitan cities and provinces with 257 stations, 585 precincts and 1,437 police boxes.

Figure 3: KNPA Organisational chart



Security roles

The Department of ICT Management and Equipment plans the adoption of ICT equipment, maintains information security and conducts research on relevant laws. It also operates and manages the agency's information network and engages in R&D for network-related programmes.

The Cyber Investigation Bureau leads cybercrime investigations, establishes and amends cybersecurity-related laws and plans prevention measures. It operates the Digital Forensic Centre which leads and promotes digital forensics while coordinating with relevant organisations when necessary.

The Big Data Policing Department establishes and implements policies on the use of big data in the security field. It trains personnel on the use of big data for preventive measures and cooperates with domestic and foreign institutions on the application of big data to policing.

The Counter-terrorism Division is responsible for terror responses. It handles personnel affairs and provides training and guidance for the SWAT team. It also operates a hostage negotiation team for terror attack incidents and conducts research on equipment for terror attack response.

The Protective Service Division establishes security plans for high-level government officials, both domestic and from overseas, including heads of state. It assesses the quality of security service at high-profile events and works to improve police security service methods and systems.

Budgets and projects

KNPA's total budget for 2021 is KRW 11.97tn (GBP 7.6bn), an increase from the 2020 budget of KRW 11.36tn (GBP 7.2bn).

Within the 2021 budget, KNPA plans to spend KRW 221.2bn (GBP 141m) on criminal investigations, which includes a budget of KRW 18.4bn (GBP 11.8m) for cybersecurity infrastructure and cyber investigation. The agency also plans to spend KRW 79bn (GBP 50m) on national security, which includes counter-terrorism measures and investigations.

KNPA has also newly allocated R&D budgets for anti-drone technology and autonomous vehicles. The budgets are KRW 1.3bn (GBP 830,000) and 16.2bn (GBP 10.3m), respectively.[46]

In March 2021 KNPA began its trials for a pre-detection system for crimes (pre-CAS). The system runs on an AI-based programme that analyses big data including public records of police cases and civilian reports to predict the crime rate in different areas. Through such analyses, it is hoped that KNPA will be able to take prevention measures such as tighter surveillance of high-risk areas. KNPA plans to officially implement the system in April 2021 throughout the entire nation.[47]

4.4. National 119 Rescue Headquarter

1, Gujiseo-ro, Guji-myeon, Dalseong-gun, Daegu
www.rescue.go.kr
No. of employees: 360

The National 119 Rescue Headquarter operates under the National Fire Agency, which is under MOIS. It supervises response measures and provides technical support for national-scale disasters and major disasters beyond local rescue forces' capabilities.

The 119 Rescue Headquarters takes prevention and response measures for disasters on both land and sea, including in mountainous regions and urban areas. It also manages equipment purchase plans to improve its capabilities. Equipment used include protective clothing, hazardous material detectors, leakage prevention equipment and neutralizing or detoxifying agents.

Divisions

The National 119 Headquarters is divided into four main divisions but also maintains special rescue forces deployed at regional centres throughout the country. The following are the significant branches within the organisation.

The Planning and Cooperation Division conducts research on rescue techniques and manages the operation of Hazmat. It also plans the Rescue Headquarters' international rescue efforts.

The Special Equipment Aviation Team is responsible for researching and deploying new technologies for search and rescue operations, such as innovative vision and sonar. It also oversees

victim search and safety management at disaster sites on both land and water, such as in earthquake sites or collapsed buildings.

The Special Fire Terror Response Division is responsible for CBRN disasters. The Rescue Headquarters maintains seven chemical disaster centres throughout the country and operates prevention and response measures for CBRN disasters.

The National Search and Rescue Headquarters establishes search and rescue operation plans, coordinates and supervises search and rescue plans for local rescue centres and makes the final decision to suspend or resume search and rescue efforts. The division cooperates with both domestic and foreign forces relevant to search and rescue operations.

The Special Aviation Rescue Division deploys search and rescue forces using helicopters, commands response measures to forest fires, transfers emergency patients and organ donations and engages in R&D for aviation-based rescue technologies.

Budget

The Rescue Headquarter announced its 2021 budget of KRW 88.8bn (GBP 56.8m), a 0.6% increase from 2020. This includes KRW 43.5bn (GBP 27.9m) for the special rescue forces and KRW 11.1bn (GBP 7.1m) for chemical disaster centres' facilities and equipment.[48]

4.5. Presidential Security Service

Cheong-wa-dae-ro 1, Jongro gu, Seoul
www.pss.go.kr
No. of Employees: 395

The Presidential Security Service (PSS) is an independent agency responsible for the protection of the president, their families, dignitaries and the Blue House, Korea's presidential residence. PSS protects former presidents and their immediate families for ten years after leaving the office. PSS is also typically deployed at large international events and took part in providing security at the 2018 Pyeongchang Winter Olympic Games and the subsequent Paralympic Games.

PSS was expanded significantly in 1974 after the assassination of Yuk Young Soo, the wife of the former President Park Chung Hee. The organisation gained greater authority over presidential security operations, including the mobilisation of the military and the police force.

Divisions

The Planning and Management Bureau is responsible for development plans, budgeting, external affairs, judicial affairs, public relations and communications. It also collects intelligence and conducts analysis regarding security threats.

The Protection Bureau is responsible for security at presidential events as well as visits of foreign leaders.

The Security and Safety Bureau provides safety in the Blue House. It commands the military and police units in charge of the Blue House and collects information from both domestic and international sources regarding security. The Bureau also establishes safety protocols for former presidents.

The Communication and Logistics Bureau manages facilities and transportation services. It also develops and operates secure communications networks, as well as related equipment.

The PSS Training centre develops security education programs and trains personnel for the field.

Budget and projects

Table 4: Presidential Security Service 2021 Budget (GBP)

Categories	2019	2020
Total	56.4m	58m
VIP special guard	10.4m	10m
Equipment and facility enhancement	4.8m	4.6m
Digitisation of security services	1.7m	2.2m
Operation of the security and safety education centre	1.3m	1.5m

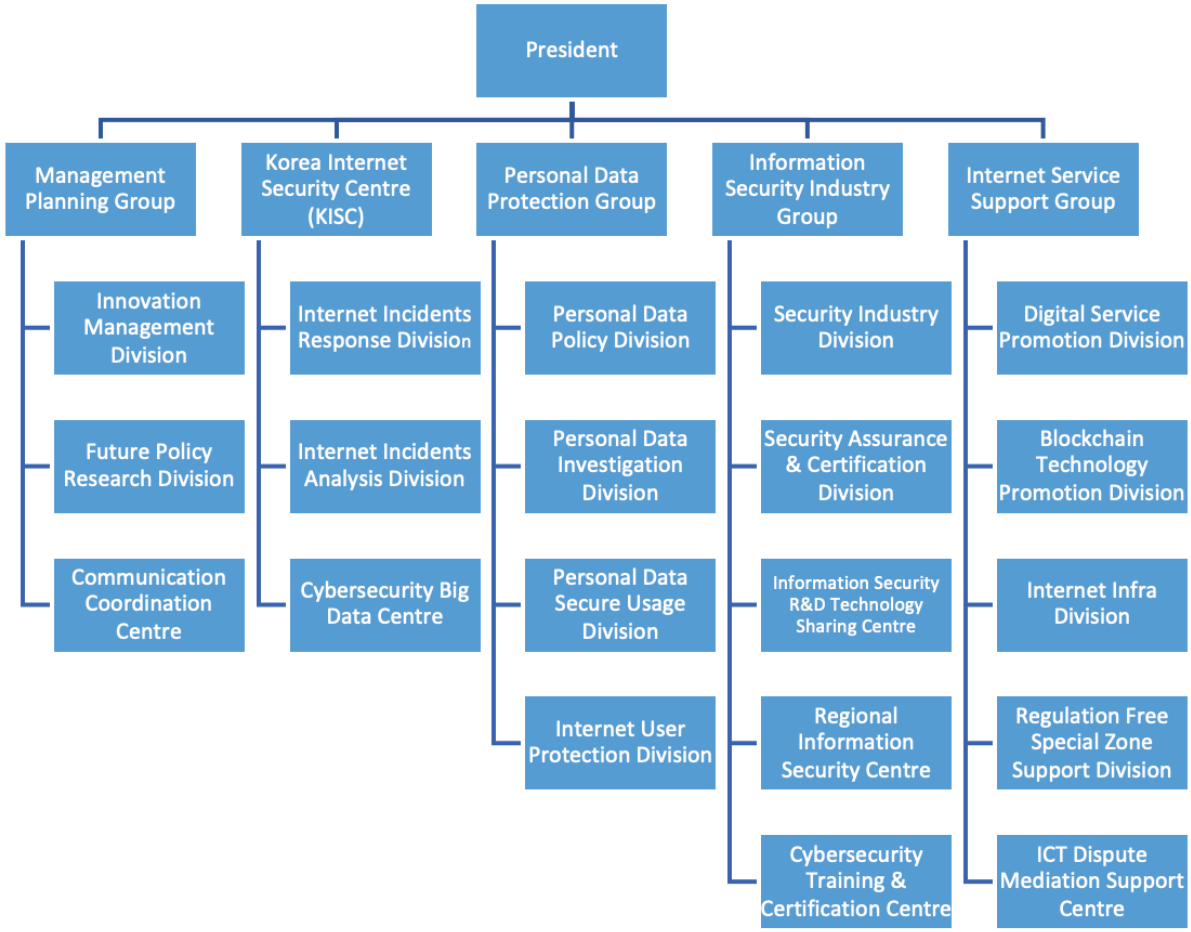
In 2019, PSS began cooperation with MSIT, research institutes and universities to open the National Technology Cooperation R&D Workshop. The participants agreed to collaborate to develop drones, smart CCTVs, wearables and cybersecurity solutions.[49]

4.6. Korea Internet and Security Agency

IT Venture Tower, 135 Jungdae-ro, Songpa-gu, Seoul
www.kisa.or.kr/
No. of Employees: 757

The Korea Internet and Security Agency (KISA) is a quasi-governmental organisation formed in 2009 under MSIT. KISA manages the operation of Korean Internet, including IP addresses and the .kr country code top-level domain (ccTLD). The organisation is also responsible for the security of Korea's Internet and is often the designated agency that evaluates and certifies cybersecurity and information protection standards of information and communication service providers.

Figure 4: KISA Organisational chart



Security roles

The Korea Internet Security Centre (KISC) plans cybersecurity polices. The Centre detects and responds to security incidents, analyses security breaches and assesses vulnerabilities. It also provides security for critical infrastructures and e-government systems.

The Personal Data Protection Group provides measures to prevent privacy breaches by maintaining a secure personal data infrastructure.

The Security Assurance and Certification Division runs physical security performance evaluations and issues certifications such as the Korea-specific Information Security Management Systems Certifications (ISMS), which larger information and communication service providers must attain to operate in Korea. Within the division is the Information Security R&D Technology Sharing Centre that develops security technology, threat response and cyber defence. The division also has a cryptography and electronic signature team.

Budget

KISA's 2020 overall budget was KRW 199.1bn (GBP 128m). Within the total budget, KRW 81.2bn (GBP 53.3m) was allocated for information security, which includes countermeasures for hacking and viruses, and promotion of the information security industry.

A budget of KRW 14.2bn (GBP 9.1m) was set for software business promotion and KRW 24.6bn (GBP 15.8m) for support for the Internet-based industry, which includes establishing infrastructure for fintech and blockchain and promoting the use of HTML5. A budget of KRW 11.2bn (GBP 7.2m) was set for R&D.

4.7. National Cybersecurity Centre

Naegok-dong, Seocho District, Seoul
https://eng.nis.go.kr/EID/1_7_1.do
No. of Employees: Classified

The National Cyber Security Centre (NCSC), established in 2004, sits under the National Intelligence Service (NIS), Korea's central intelligence agency. NCSC is responsible for identifying, preventing and responding to cyber-attacks and threats. The centre works closely with the private sector to disseminate alerts, respond to security incidents and to protect critical national infrastructure in Korea.

Roles

NCSC establishes and implements national cybersecurity policies and prepares guidelines to protect the nation's major information and communication networks.

NCSC manages cyber crisis prevention and detection by inspecting major national information and communication networks and conducting cyber mock drills. The centre detects signs of cyber threats and issues alerts by grade.

The centre also carries out cyber infringement investigations and threat analysis for national and public institutions by working with related domestic and foreign organisations.

4.8. Incheon International Airport Corporation

47 Gonghang-ro 424beon-gil, Unseo-dong, Jung-gu, Incheon
https://www.airport.kr/co/en/index.do
No. of employees: 1,774

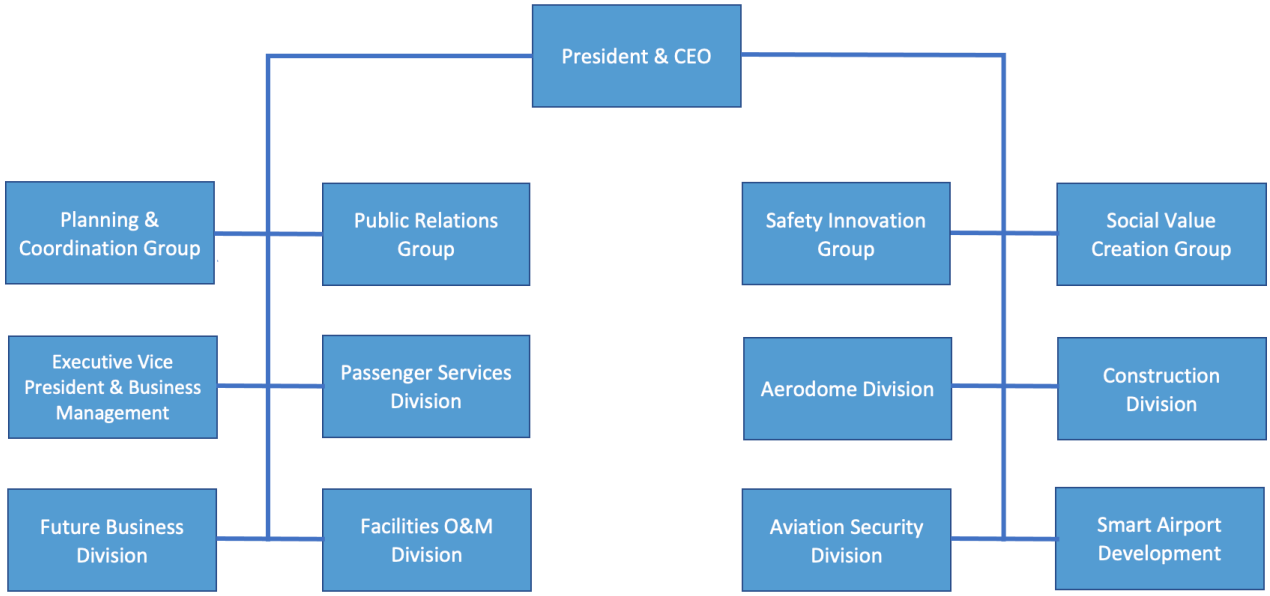
Incheon International Airport Corporation (IIAC) manages Korea's largest airport, Incheon International Airport. IIAC was established in 1999, prior to the completion of the state-owned airport in 2001, replacing the Gimpo International Airport as Korea's primary international airport.

Located 70km west of Seoul, the Incheon Airport is consistently ranked among the top airports globally and has been ranked first by the Airport Service Quality (ASQ) programme for 12 consecutive years.

IIAC's business areas include construction, management and operation of the Incheon International Airport, development of surrounding areas and government-commissioned projects. The corporation also engages in research and survey on airport construction, management and operation.

The Incheon Airport opened its second passenger terminal in January 2018, a major expansion project that began in 2013 with a KRW 4tn (GBP 2.54bn) investment. The second terminal increased the airport's passenger capacity from 44 to 62 million and cargo capacity from 4.5 to 5.8 million tons per year. In 2019, the airport accommodated 71 million passengers, 400,000 flights and 2.76 million tons of cargo.[50]

Figure 5: Incheon Airport Corporation Organisational chart



Security roles

For operations safety, the airport maintains skyway safety through pre-emptive measures and crisis control. The Incheon Airport introduced Airport Collaborate Decision Making (A-CDM) to Korea for the first time in 2017, allowing air transit management, airlines and other stakeholders to share real-time aircraft transit and preparation time information among themselves.

The airport also oversees its safety management system, which includes aims to minimise aircraft collisions, ground collisions and interference to aircraft operation caused by mismanagement. The airport uses vehicle detecting system (VDS) and advanced surface movement guidance and control

system (A-SMGCS) for the safety of the airport grounds. Future incorporation of AI and big data analysis to monitor aircraft navigation is a major area of interest.

IIAC is aiming to develop a comprehensive passenger-friendly security and counter-terrorism process. Major areas of focus are relieving passenger congestion through efficient security screening procedures, pre-emptively identifying security threats through advanced technology and improving capabilities through using AI and biological recognition.

The Incheon Airport also has a disaster response system overseen by its safety innovation team. A future benchmark for the response system is to implement airport-customised protocols for infectious diseases and disasters.[51]

Budget and projects

The official budget for the Incheon International Airport Corporation is not published to the public. However, the estimate of the total budget acquired from a direct source is KRW 1.24tn (GBP 794.6m). A budget of KRW 250bn (GBP 160m) is allocated for security including KRW 7.5bn (GBP 4.8m) for cyberterrorism response. The cumulative budget for R&D, airport expansion and a new runway is KRW 974bn (GBP 624.2m).

In 2019, Incheon Airport announced a KRW 4.8tn (GBP 3.1bn) "Phase 4" project. The plan includes expanding Terminal 2, establishing a fourth runway and increasing the number of aprons from 210 to 285 by 2024. Terminal 2 will increase the airport's capacity to accommodate up to 160 million passengers per year, making Incheon the first airport in the world with two terminals that can each accommodate more than 50 million passengers per year. The airport is planning to incorporate 4IR technology and use of big data, IoT and virtual reality to improve its service. The establishment of a fourth runway will also increase the capacity of flights per hour from 90 to 107.[52]

The airport also plans to expand its use of 4IR technologies for safety and security. In November 2020 the airport successfully used drones for utility infrastructure inspections. IIAC stated its intention to engage with more smart technology for both the operation and safety of the airport.[53]

4.9. Korea Coast Guard

130 Haedoji-ro, Yeonsu-gu, Incheon
http://www.kcg.go.kr/english/main.do
No. of Employees: 13,661

Founded in 1953 as part of the Korean National Police Agency, the Korea Coast Guard is now an independent and external branch of the Ministry of Maritime Affairs and Fisheries. After the 2014 Sewol ferry disaster that resulted in over 300 deaths, the organisation was disbanded and its responsibilities were given to the National Police Agency. In 2017 the Coast Guard was re-established under the MOIS and later in the same year became a branch of the Ministry of Maritime Affairs and Fisheries.

Security roles

The Korea Coast Guard's duties can be broadly divided into safety and security missions.

For safety, the Coast Guard is responsible for maritime disaster management. This includes rescue measures in vessel incidents in coastal sea, response to natural disasters and safety control for leisure activities. The KCG also establishes maritime traffic order by providing vessel traffic service and controlling port access and oversees the safety measures for various types of vessels, from general ships to leisure vessels, especially high-risk vessels with oil tankers or hazardous and noxious substances. Prevention and response measures to marine pollution are also established by the Coast Guard.

For security the Korea Coast Guard protects maritime territory and sovereignty which involves response to illegal fishing by foreign vessels, protection of critical marine infrastructure, implementation of marine anti-terrorism activities and prevention of the proliferation of weapons of mass destruction. The Coast Guard also investigates maritime crimes. This includes investigations of crimes related to the fishing industry as well as international crimes such as smuggling, illegal entry and exit and piracy.

Budget and projects

The following are the Korea Coast Guard's budget for 2021. The table includes the total budget as well as areas significant to safety and security.

Table 5: Korea Coast Guard 2021 Budget (GBP)

Category	GBP
Total	981.9bn
Coastal safety prevention activities	3m
Search and rescue enhancement	5.8m
Coastal rescue equipment	2.5m
Vessel traffic service operations	19m
Satellite equipment maintenance	11.2m
Counterterrorism enhancement	5.8m
Information network security	480,000
"Golden hour" search and rescue technology R&D	4.9m

The Korea Coast Guard announced in November 2020 its plan to establish a disaster safety communication network that connects marine and land organisations including police, fire departments, military and local governments to enable rapid joint response in the event of a disaster. Through 2021, the Coast Guard plans to add 1,300 control terminals to establish control

centres and recording servers.[54] The KCG plans to expand LTE-M-based communication up to 100km from the coast and link satellite communication networks beyond the area.

The Korea Coast Guard is actively seeking to improve both its safety and security maintenance abilities. From November 2020 the Coast Guard incorporated 3D-printing to produce vessel parts such as drainage pumps with more resilient materials at a lower cost. Also in late 2020, the Coast Guard made a much-needed improvement of its vessel traffic service (VTS) system, which can now transmit alerts when vessels move off their route or exceeded the speed limit. This involved cooperation of outside sources such as the port management information system to more accurately detect vessel activities.[55]

The Korea coast Guard also anticipates new security threats from new 4IR technologies such as drones and autonomous surface ships. In December 2020, the Coast Guard announced an amendment to the Marine Security Act, which it oversees and plans to revise the Maritime Counterterrorism Basic Plan every five years. The Coast Guard also plans to engage in R&D developments for counterterrorism technology.[56]

4.10. Korea Airports Corporation

78, Haneul-gil, Gangseo-gu, Seoul
https://www.airport.co.kr/wwweng/index.do
No. of Employees: 2,650

The Korea Airports Corporation operates three major regional airports, Gimpo, Busan and Jeju, and a host of smaller ones. The Airport Corporation is also responsible for the construction, management and operation of airports, including development and maintenance of areas surrounding airports as well as airport and airfield facilities.

The corporation is a state-owned corporation established in 1980 and is an affiliate of the Ministry of Land, Infrastructure and Transport (MOLIT). MOLIT and the Ministry of Economy and Finance each own just under half the shares of the Corporation. The legal basis for the corporation's role and its scope of business is the Korea Airports Corporation Act.

Security roles

The Airports Corporation has a Safety and Security Division which is comprised of safety and security office, operations control centre, emergency planning office and cybersecurity centre. The safety and security office has four subdivisions – safety planning department, disaster prevention department, security planning department and counter-terror response department. The division plans comprehensive airport safety management plans and is responsible for implementing policies and guidelines for flight safety and security. It also maintains and updates security equipment and provides technical support for regional offices.

Aviation Security Training Centre (ASTC)

ASTC was established in 2003 by the government and is overseen by KAC. The centre is a specialised aviation security training centre that trains experts in security scans, aviation security and explosive ordnance disposal. ASTC is a member of the International Civil Aviation Organisation (ICAO) network along with 34 other centres and has been operating ICAO aviation security training courses since 2008. ASTC currently has four instructors with one of them being ICAO-certified and 17 assistant instructors among which three are ICAO-certified.

Budget and projects

KAC's 2020 budget was KRW 1.13tn (GBP 720bn) with KRW 598bn (GBP 382m) for facility maintenance and operations, KRW 25bn (GBP 16m) for R&D and KRW 335bn (GBP 214m) for construction projects. KAC does not publicly disclose more specific breakdowns of its budget.[57]

The corporation reportedly suffered a loss of KRW 200bn (GBP 127m) in 2020 from the steep drop in air travel and duty-free purchases caused by the COVID-19 pandemic. KAC has announced plans it will issue public bonds worth a total of KRW 400bn in 2021 to support airports' economic recovery.[58]

KAC has also formed a four-way partnership in January 2021 with Hanwha Systems, SK Telecom and the Korea Transport Institute to drive the commercialisation of flying cars or air mobility vehicles (UAM). With the goal of executing commercial air taxi trials by 2025, KAC will contribute by building and operating vertiports and traffic control for UAM vehicles.[59]

4.11. Korea Customs Service

Building 1, Government Complex-Daejeon, 189, Cheongsa-ro, Seo-gu, Daejeon
https://www.customs.go.kr/english/main.do
No. of Employees: 349

The Korean Customs Service (KCS) is responsible for processing customs clearance and regulating all goods entering and exiting the country in accordance with Korea's laws. KCS was established in 1970 and is overseen by the Ministry of Economy and Finance.

KCS's role broadly splits into two. The first is to assist passengers and freight through customs, facilitating international travel and trade. The second is to protect public order and the national economy by prohibiting the entry of smuggled goods, drugs, terror-related items, counterfeits and pollutants.

Security roles

KCS has three divisions involved in security measures.

The Investigation and Surveillance Bureau is responsible for prohibiting the entry of smuggled or counterfeit goods that harm the domestic economy and fair global competition. It also prohibits the entry of weapons and drugs.

The Main Customs oversees the five regional customs offices in Incheon, Seoul, Busan, Daegu and Gwangju and may participate in each region's internal administrative duties.

The Customs Border Control Training Centre trains professional personnel in customs border control, including import and export businesses on FTAs and clearance. The centre also breeds and trains detector dogs to search for explosives and drugs.

Budget and projects

KCS announced its total budget of KRW 596.2bn (GBP 379.5m) for 2021. This includes a budget of KRW 33.2bn (GBP 21.1m) for clearance facilities and equipment, KRW 49.6bn (GBP 31.6m) for anti-smuggling control and KRW 69.8bn (GBP 44.4m) for informatisation, which focuses on big data and digitalisation of customs service.[60]

From 2020, KCS's budget for anti-smuggling control has increased by 12.9% and informatisation by 4% as the organisation increasingly invests in innovative solutions. In November 2020, KCS held a presentation targeting telcos and tech companies to discuss plans and budget for the adoption of 4IR technologies and further digitalisation of its service. Among many items, KCS's plan includes an update of its big data system and AI X-rays with investments of KRW 6.3bn (GBP 4m) and KRW 700m (GBP 442,000), respectively.[61]

4.12. National Intelligence Service

Naegok-dong, Seocho District, Seoul
https://eng.nis.go.kr/
No. of Employees: Classified

The National Intelligence Service (NIS) is Korea's chief intelligence agency, reporting directly to the president. It assumed its current name in 1999 after its establishment in 1961 as the Korean Central Intelligence Agency. The NIS provides intelligence, maintains security and conducts criminal investigations. Some of its major duties are collecting domestic and overseas intelligence, with a specific emphasis on North Korea, overseeing defence technology, as well as handling counterterrorism and cybersecurity measures.

Centres within NIS

NIS has four different centres – National Cyber Security Centre, National Industrial Security Centre, Transnational Crime Information Centre and Terrorism Information Integration Centre.

NIS established the National Cyber Security Centre (NCSC) in 2004 after the country's internet was paralysed by the Slammer Worm in 2003. The centre plans and coordinates national cybersecurity polices, as well as facilitating information-sharing among the public, private and military sectors. It also operates cyber crisis prevention activities and continues to develop detection technologies for new hacking methods.

NIS also operates the Terrorism Information Integration Centre, which collects, analyses, prepares and distributes domestic and foreign intelligence on terrorism. The centre is responsible for tracking down terrorists both domestically and internationally and cooperating with other foreign intelligence services.

Budget

The Korean media reports estimate NIS 's 2021 budget for both security and special activities to exceed KRW 1tn (GBP 631m).[62]

4.13. Defence Acquisition and Program Administration

Building #3,4, Government Complex-Gwacheon, 47, Gwanmun-ro, Gwacheon-si, Gyeonggi-do
http://www.dapa.go.kr/
No. of Employees: 1,130

The Defence Acquisition Program Administration (DAPA) handles procurement for all branches for the Korean military, including the Army, Navy and Air Force. DAPA was established as a branch of the Ministry of National Defence (MND) in 2006 with the goal of centralising procurement in a single agency. Prior to the establishment of DAPA, defence acquisitions was run through its own procurement offices at each military branch under MND's administrative oversight. In addition to procurement, DAPA is also involved in development projects related to vehicles, vessels and aircrafts.

DAPA manages defence contracts and runs technology transfers from research labs to production and exercises authority over budget allocations for acquisitions on domestic and foreign suppliers. DAPA's Foreign Purchase Bid and Information Service to set out bids.[63]

DAPA runs the Integrated Project Teams (IPTs) organised to manage defence acquisition programs with centralized planning, budgeting, quality assurance, and technology management. DAPA's Contract Management Agency houses the International Contract Department that executes contract on defence equipment from local and foreign suppliers.

Budget and projects

DAPA manages approximately 30% of the total defence budget – dedicated to defence improvement costs, with the remaining 70% allocated to the MND for troop operation costs and

force maintenance costs. This figure reached 33.3% this year, representing KRW 15.8tn (GBP 10bn) of a KRW 47.6tn (GBP 30.3bn) budget, the highest since DAPA's establishment.

Table 6: DAPA 2020 Budget

Type	GBP
Aircrafts	3.9bn
Ships	1.7bn
Guided weapons	1.6bn
Defence business policy support	1.1bn
Mobile firepower	1.1bn
Command reconnaissance	678m
Defence business establishment support	98.3m
Internal transaction expenditure	5.5m

5. Opportunities and Analysis

5.1. Future outlook

Korea has won praise for its management of the COVID-19 pandemic and more than a year since the virus hit Korea, the total number of cases remains less than 100,000.[64] Authorities were able to control the pandemic through widespread testing, contact-tracing and quarantines to limit outbreaks, avoiding lockdowns and allowing daily life largely to continue as normal. As a result, Korea's economy shrank by just 1.1% in 2020, outperforming other OECD member countries that saw much larger contractions, including the UK (9.9%), US (3.6%) and Germany (5%).[65] The Korean economy is expected to remain among the strongest worldwide, with the IMF forecasting 3.1% growth in 2021.[66]

Government strategy to generate growth in the post-pandemic years will revolve around the Korean New Deal, a KRW 160tn investment in large-scale digitisation and decarbonisation of the economy, government and society.[67] Over one-third of the public funding (KRW 44.8tn or GBP 28.5bn) will focus on the development and utilisation of technologies such as AI, big data platforms and 5G connectivity. Approximately KRW 1tn (GBP 640m) in cybersecurity funding will improve the defensive capabilities of small and mid-sized businesses, while also seeking to incubate an ecosystem of 100 cybersecurity startups.

> Industry Insider's Thoughts
>
> The Korea New Deal and broader digital transformation underscore the need for new cyber solutions as cyber threats and attacks become increasingly sophisticated.
>
> General Manager – Information Protection Bureau, KISA

Another key issue over the long term is the low birth rate and rapidly aging population. Korea has the lowest birth rate in the world at 0.84 as of 2020 and the population began dropping in 2020, a year earlier than expected.[68] Approximately 14% of Koreans are currently over the age of 65, but this figure is expected to more than triple over the next 20 years.[69] Companies are beginning to respond by investing in automation, often with government support such as a KRW 100bn (GBP 64m) joint fund to support the adoption of robotics in manufacturing.[70] Korea has the highest robot density of robot workers of any major economy, its 868 robots per 10,000 workers trailing only Singapore's 918.[71]

5.2. Emerging technologies

Korea invests heavily across its public and private sectors in the development of new technologies, ranking fifth amongst OECD countries for R&D spending as a percentage of GDP [72] and fourth

worldwide in the number of international patent filings.[73] There is strong demand from various government agencies for innovative technologies that can increase their defensive, surveillance or protective capabilities. These technologies include mobility, cloud, AI and big data, with applications in multiple security sectors.

Major automotive OEMs such as Hyundai and KIA are investing in mobility applications such as autonomous and airborne vehicles. Other companies, such as major defence contractors LIG Nex1 and Hanwha, are seeking future growth by exploring the development of unmanned aerial and underwater vehicles, as well as related systems. For example, the Korea Airport Corporation is working with SK Telecom, Hanwha Systems and the public Korea Transport Institute on a long-term project to commercialise air taxis. The project is in its early stages and is expected to enter a trial phase by 2025.

The development of new cybersecurity technologies is an area of strategic interest for government, network operators and hardware manufacturers alike. Government funding is supporting the development of detect and response capabilities as part of an existing push to secure digital infrastructure, as well as to prepare for the coming increase in digitisation through the Korean New Deal. Major telecommunications operators are leading a push towards commercializing quantum cryptography, including SK Telecom's partnership with Swiss ID Quantique to develop quantum key distribution (QKD), as well as KT's locally developed quantum encryption for 5G data.[74]

> Industry Insider's Thoughts
>
> As COVID-19 continues and untact services grow, the government has announced the Digital New Deal strategy. In 2021, in order to support this ICT strategy, the MSIT has allocated KRW 670bn in budget for cybersecurity projects. One of the areas of interest is international cooperation. The Korean government welcomes and encourages foreign companies with advanced technology to form partnerships for cooperation with local companies.
>
> Deputy Director – Information Security Planning Division, Ministry of Science and ICT (MSIT)

AI and big data have played a major role in Korea's largely successful containment of the COVID-19 pandemic, allowing for the rapid development of test kits in the early stages and then helping make sense of the tremendous amounts of information collected in contact tracing.[75] The role of AI in other security applications is likely to grow as part of the October 2019 National AI Strategy, which seeks a 90% crime clearance rate through the use of AI.[76] The KNPA and the Korea Coast Guard are also investing in data analytics to identify and respond to emergencies faster. The ability to read and analyse CCTV footage will aid police, as will other advanced vision systems. Incheon Airport, for example, is already using an AI-based X-ray image reading system.[77]

The Korean market for cloud computing services is growing rapidly, expanding 25% in 2019 to an estimated KRW 1.3 trillion (GBP 830m). The market is increasingly controlled by a small number of global players such as Amazon, Google, and Microsoft, who can deliver market-ready solutions to meet growing demand from customers. Major Korean tech companies Kakao, Samsung SDS and

Naver have entered the cloud business, as have leading telecommunications operators KT and SK Telecom. Naver and Kakao are in the process of building additional data centres to add capacity, with an eye on the Korean government's plans to run via cloud by 2030, as well as the government's goal of achieving national self-sufficiency in this sector.

5.3. Market opportunities

UK companies will find opportunities across Korea's various security sectors in areas where domestic firms are not yet capable of producing high-quality solutions, as well as security-specific applications of technologies such as AI and data analytics. Innovative technologies and solutions that can help government customers achieve their policy goals will also receive interest from government customers, as well as Korean companies capable of building complete systems for delivery to those customers.

Advanced AI solutions and data processing capabilities with security applications will find broad interest from multiple sectors in the security industry, including surveillance, disaster response and threat recognition. Incheon Airport, for example, has a specific interest in the use of data analytics for monitoring aircraft navigation, while the Korea Coast Guard is seeking to build predictive models for identifying accidents through the collection and analysis of data from vessels. Vision systems, such as those capable of analysing or searching CCTV footage, will find public security applications, including for post-pandemic protocols.

Advanced cybersecurity solutions, as well as specialized professional services, will be in demand as Korea undertakes further digitisation of its economy and particularly its government. The continued threat of cyberattacks from North Korea and elsewhere will put a premium on the ability to protect major companies, public institutions, banks and other sensitive targets from intrusion. The drive towards cloud autonomy, where Korea's tech companies seek to develop domestic cloud computing infrastructure, will further create opportunities for UK companies able to secure this infrastructure.

> Industry Insider's Thoughts
>
> On any given day, many actors attack Korean society. Those entities could be North Korean, Chinese, or other actors looking to steal money, information or to cause harm. The UK is a natural partner for Korea to defend itself against these kinds of intrusions.
>
> In-Bum Chun, Retired Lieutenant General

Urban air mobility (UAM) is an area of interest for automotive OEMs such as Hyundai, all three telecommunications service providers and public organisations such as the Korea Airport Corporation. Many projects are in the planning stage over the next year or two, with trial deployments set to begin as early as 2023 and projected to continue for multiple years. Companies with technology capable of enabling UAM or securing its infrastructure will be in high demand, though regulatory or standards issues across countries could be an obstacle.

Aviation security will also be an important source of opportunities for international firms. There continues to be strong demand for conventional technology such as airport security tools, aircraft components, avionics and sensors, although Korean firms are improving their competitiveness in these areas. Anti-drone solutions and systems are increasingly an area of interest across multiple sectors, including airports, critical infrastructure sites, transportation hubs and public spaces in Seoul. A number of major Korean groups such as Hanwha and SK are seeking to develop this technology, but for the time being, the industry is dominated by international players in the absence of domestic competition.

5.4. Challenges

UK companies seeking to sell into the Korean security market may face a number of obstacles, such as the complexity of the public sector procurement process, disadvantages due to the lack of a local presence, as well as regulatory differences between the UK and Korean markets. Korean customers may be price sensitive but are willing to pay for high-performance solutions that meet their needs. However, UK companies may find that there is a preference in the public sector for comparable local suppliers.

In certain cases, a UK company's technology or solution may be integrated into a complete system by an in-country partner, customer or systems integrator, who would then deliver a product to the Korean government agency that is the end user. This scenario is much simpler as the local company would take responsibility for dealing with the Public Procurement Service (PPS), avoiding issues relating to the preparation and submission of bid documents. However, other UK firms may prefer to engage in direct sales to a Korean government customer through the PPS, a far more challenging task.

The ability to provide local support for both hardware and software solutions is important as Korean customers prefer to have local support teams in Korea that can provide real-time Korean-language support. International firms unable to offer this may be perceived as less reliable despite superior technical performance, making it potentially advantageous for UK firms to consider working with a local partner that can offer frontline support. After service is a critical component of building trust with Korean customers.

Issues related to regulations, as well differing industry or government standards, may also pose an obstacle for UK companies seeking to do business in the Korean public sector. For example, innovative telecommunications, IOT or connective solutions may run into regulatory issues around the usage of frequency bands. Overseas firms with cybersecurity solutions tend to use the global Advanced Encryption Standard (AES), but the Korean public sector requires agencies to use the locally developed ARIA and SEED algorithms. This makes it difficult to sell to Korean government customers, making greater flexibility in cybersecurity standards an area of interest for the UK government.

6. Procurement Process

6.1. Background

The Public Procurement Service (PPS) is the central public procurement agency that manages the purchase of goods, equipment and services on behalf of Korean government agencies. Public procurement of goods and services exceeding the value of approximately USD 85,000 (GBP 61,000) and construction projects exceeding USD 2.54m (GBP 1.83m) are typically made through PPS. The role of PPS in public procurement varies among different organisations and industries.

Aside from overseeing public procurement, the PPS's range of responsibilities includes standardisation of procurement procedures and provision information on bidding contracts, specified products, pricing, suppliers and government customers. PPS also manages stockpiling of raw materials and construction projects concerning real estate owned by the Korean government.

Table 7: Total value of completed public procurement contract by the PPS (GBP)

Type of procurement	2018	2019	2020
Total	37bn	41.5bn	44bn
Domestic	17bn	20.4bn	22bn
Construction	19.5bn	20.5bn	21.4bn
Foreign	288m	363m	362m
Stockpile	164m	105m	170m

Source: Intralink research

6.2. Registration

Bidders must register with PPS at least one day before their bid. Late registration may be permitted for foreign bidders as long as registration is complete before entering into a contract. To register, a foreign bidder must be a manufacturer, a wholesaler or a retailer of the tendered goods and must provide its business registration or certificate as a proof. All documents must be issued by the relevant public authority of the applicant's country or be publicly notarised to be deemed valid.

Public procurement bids are typically made online through PPS's Korean Online E-Procurement System's (KONEPS) single window — an online portal where bidders can submit their bids and track the entire procurement process.[78] After a one-time registration with the portal, potential suppliers can bid through the KONEPS and all their bids will be published in the portal.

6.3. Bidding process

For a tender to be disclosed by PPS, procuring public entities i.e., customers can submit purchase requests through the KONEPS portal. After receiving a request, PPS prepares the preliminary terms and conditions for the invitation to bid. The preliminary invitation is disclosed to the public on KONEPS for seven days to receive feedback from relevant industries to ensure fair competition for the bid. PPS then consults on the feedback to finalise the bid invitation and publishes it on KONEPS at a designated time. The opening of the bid can also be held offline in the presence of the bidders.

Several types of bidding and contracting processes exist. Customers can set forth different competition schemes by allowing all qualified suppliers to make their bids or allowing only those it nominates to make bids or directly negotiating with the candidate it selects.

Customers can also establish a contract through a supply scheme in which they can agree on procurement by the total contract amount or by unit-price, the latter being commonly used by procuring entities that make frequent purchases.

Some bids may require a two-track process with separate commercial and technical submissions. In such cases the customer will first select their preferred technology then select a supplier in consideration of the price.

Bid bonds worth 5% of the total bid price may be required, but can be waived with the submission of a memorandum of bid bond payment.

6.4. Bid evaluation

The technical review of bids is conducted by the customers, but PPS and customers may collaborate if necessary. Three different results may come of the review – acceptable, conditionally acceptable and not acceptable. Acceptable bids are expected to be superior to others in meeting the specifications in the bid invitation and supplemented by the required documentation.

Conditionally acceptable bids are often those that comply with bid specifications but lack the appropriate documentation. Unclear indication of equipment models or minor non-compliant parts can also ensure that a bid's acceptance remains conditional.

Bids that are deemed 'not acceptable' do not comply with the bid invitation to a substantial degree. Customers may also not accept bids with insufficient documentation, including catalogues, drawings, outlines of structural designs and descriptions. Documentation discovered to be copied from another company can also lead a customer to refuse to accept a bid.

When a bid is selected, the successful bidder will receive written notification of award and the contract will come into effect.

6.5. Payment and delivery

After the contract is awarded and goes into effect, PPS applies to an authorised foreign exchange bank in Korea for the issuance of an irrevocable, without-recourse and non-transferable commercial letter of credit (L/C). The bank will then notify the beneficiary.

Upon notice of the L/C issuance, the successful bidder, now the supplier, must deposit the performance bond, a minimum of 10% of the contract amount, to the bank. The bank will release the bond back to the supplier upon completion of the contract.

After receiving the L/C, the supplier must perform its contractual obligations according to the L/C and the contract i.e., make the shipment by the specified delivery date. Upon a supplier's failure to comply, its performance bond may be confiscated, and it may be banned from contracting with PPS and other public entities in the future.

In cases of loss or damage to goods, including no-shows, shortage of supply, breakage and discrepancies with the agreed specifications, PPS may take the necessary action to replace, repair or acquire compensation from the liable party. If necessary, PPS may select an inspector to perform an inspection of the supply prior to delivery.

When the delivery arrives at the designated port, the regional PPS office nominates a stevedoring firm to unload. The regional PPS office completes customs clearance in cooperation with the purchaser and the former delivers the goods to the latter. If the purchase has been contracted under FCA or FOB terms, the transport operator nominated by the PPS must deliver the goods to the place designated by the customer.

When the shipment is complete and all shipping documents are presented by the supplier, the bank releases the payment to the supplier under L/C. Upon the purchaser's notice of receipt and confirmation that the contract terms have been completed, PPS instructs the issuing bank to close the L/C and release the performance bond to the supplier.

[1] 원병철, 보안뉴스, “2021 년 대한민국 보안시장 규모, 6 조 414 억원 전망”, 2021/03/03, (https://www.boannews.com/media/view.asp?idx=94940)
[2] 경찰청, “2019 경찰범죄통계”, 03/04/2021, (https://www.police.go.kr/www/open/publice/publice03_2019.jsp)
[3] OECD, “OECD Better Life Index – Safety”, (http://www.oecdbetterlifeindex.org/topics/safety/)
[4] Ibid.
[5] 김은경, 연합뉴스, “강남 묻지마 살인, 정신질환자 전형적 범죄…'女가 괴롭혀' 망상(종합)” 2016/05/22 (https://www.yna.co.kr/view/AKR20160522012651004)
[6] 장선, 인천일보, “불법촬영 범죄, 지난 5 년간 86% 증가 피해 심각”, 2020/10/28, (http://www.incheonilbo.com/news/articleView.html?idxno=1064356)
[7] 국토교통부, “2019 년 교통사고 사망자 3,349, 전년 대비 11.4% 감소”, 2020/03/08 (https://www.korea.kr/news/pressReleaseView.do?newsId=156378977)
[8] 이병준, 중앙일보, “9 일째 이어진 폭우, 사상자 속출…30 명 숨지고 12 명 실종”, 2020/08/09, (https://news.joins.com/article/23844172)
[9] Andrew Freedman, The Washington Post, “Typhoon Maysak strikes South Korea, while a second storm gains strength just behind it”, 2020/09/03, (https://www.washingtonpost.com/weather/2020/09/02/typhoon-maysak-korea-haishen/)
[10] 김기훈, 연합뉴스, “국내 재난안전산업 시장 규모 47 조 3 천억원…전년보다 8% 증가”, 2021/02/24, (https://www.yna.co.kr/view/AKR20210224049300530)
[11] Elizabeth Shim, UPI, “South Korea develops new maritime surveillance radar for ships, aircraft”, 2019/10/30, (https://www.upi.com/Top_News/World-News/2019/10/30/South-Korea-develops-new-maritime-surveillance-radar-for-ships-aircraft/3551572450288/)
[12] 정민하, 조선비즈, “LIG 넥스원, ‘함정 원격정비지원체계’ 공개”, 2020/12/11 (https://biz.chosun.com/site/data/html_dir/2020/11/12/2020111200801.html?utm_source=naver&utm_medium=original&utm_campaign=biz)
[13] 박미영, 보안뉴스 “해양경찰청, 해양 대태러 역량 강화 제도적 기반 마련” 2020/12/15 (https://www.boannews.com/media/view.asp?idx=93410&page=1&kind=2)
[14] 국토교통부, "국내 인증을 통한 항공보안장비 생산의 길 열려”, 2019/09/05, (http://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?lcmspage=1&id=95082252)
[15] 홍찬선, 뉴시스, “인천공항 3km 드론 출현→軍출동…"뮤비 찍어" 주장”, 2020/12/24, (https://www.donga.com/news/Society/article/all/20201224/104620594/1)
[16] 인천국제공항공사, “International Freight Network”, (https://www.airport.kr/co_cnt/en/majbus/logistic/logcom/logcom.do)
[17] Ibid.
[18] 김기훈, 연합뉴스, “국토부, ‘가덕도 신공항 예산 28 조대…안던사고 환경훼손 우려” 2021/02/24, (https://www.yna.co.kr/view/AKR20210224080552001?input=1195m)
[19] 곽래건, 조선일보, “조종사협회 ‘가덕도, 김해공항과 착륙경로 겹쳐 안전에 문제’”, 2021/04/03, (https://www.chosun.com/national/transport-environment/2021/03/04/NG3Y2SBOZ5BY3NXGY4RHCOU2Q4/)
[20] 경찰청, “의무경찰 연혁”, (https://ap.police.go.kr/ap/main/contents.do?menuNo=200003)
[21] 설성인, 조선비즈, “[구멍 뚫린 원전]② 한수원 해킹, APT 공격 가능성”, 2014/12/19, (https://biz.chosun.com/site/data/html_dir/2014/12/19/2014121902619.html)

[22] 김소연, 원자력신문, “국가보안시설 ‘가급’ 원사력 시설 ‘테러로부터 안전한가”, 2019/10/02, (https://www.knpnews.com/news/articleView.html?idxno=17379)
[23] 김소연, 원자력신문, “국가보안시설 ‘가급’ 원전…’드론테러’ 대책마련 시급”, 2019/09/17, (https://www.knpnews.com/news/articleView.html?idxno=17295)
[24] 차근호, 연합뉴스, “국가보안시설 고리원전 드론 무단비행…10 개원새 14 명 적발”, 2020/06/18, (https://www.yna.co.kr/view/AKR20200618155100051?input=1195m)
[25] 최다현, 아주경제, “통신재난관리, 기본부터 다시 세운다”, 2019/01/30 ,(https://www.ajunews.com/view/20190130093200062)
[26] LG CNS, (https://lgcns.com/EN/Industry/e-Government)
[27] 대한민국 정책브리핑, “국가 사이버보안 전략”, (https://www.korea.kr/archive/expDocView.do?docId=38501)
[28] Yunwhan Chae, Yonhap News, “S. Korea to spend 670 bln won on cyber security by 2023”, 2021/02/18, (https://en.yna.co.kr/view/AEN20210218006100320)
[29] Ibid.
[30]원병철, 보안뉴스, “2021 년 과기정통부 정보보호 예산 2,400 억원 확정, 지난해보다 540 억원 늘었다”, 2020/12/3, (https://www.boannews.com/media/view.asp?idx=93128)
[31] 권준, 보안신문, “[2021 년 공공부문 정보보호 수요 분석-1] 네트워크 보안 예산 기관·기업 TOP 10”, 2021/03/18, (https://www.boannews.com/media/view.asp?idx=95723)
[32] United States Trade Representative, “2020 National Trade Estimate Report on Foreign Trade Barriers”, (https://ustr.gov/sites/default/files/2020_National_Trade_Estimate_Report.pdf)
[33] 박남수, 정보통신신문, “디지털 인증 본격화…전자서명 시장 재편”, 2020/12/21, (https://www.koit.co.kr/news/articleView.html?idxno=80395)
[34] Kyoung-Son Song, Korea JoongAng Daily, “Mobile carriers make app registration easier with Pass”, 2020/03/25, (https://koreajoongangdaily.joins.com/2020/03/25/industry/Mobile-carriers-make-app-registration-easier-with-Pass/3075346.html)
[35] Woo-hyun Shim, The Korea Herald, “Revenues of Korean IoT firms surpass W10tr in 2019”, 2020/02/26, (http://www.koreaherald.com/view.php?ud=20200225000865)
[36] Korea JoongAng Daily, “Nearly 20,000 smart factories are now operating in Korea”, 2021/01/14, (https://koreajoongangdaily.joins.com/2021/01/14/business/tech/smart-solutions-smart-factories-smart-factory/20210114182800459.html)

[37] Ibid.
[38] POSCO, ”POSCO ICT Joins Hands with CISCO to Reinforce Industrial Security Business”, 2019/04/04 (https://eng.ixotive.com/customer/news/1572)
[39] 한국 IR 협의회, “기술분석보고서”, (https://kirs.or.kr/information/tech2020_2.html)

[40] Ibid.
[41] 한국인터넷진흥원, “정보보호 전문서비스 기업 지정 제도 해설서” (https://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=259&dno=61&fseq=1)
[42] Ministry of the Interior and Safety, “Integrated Disaster and Safety Information System”, (https://www.mois.go.kr/eng/sub/a03/bestPractices1/screen.do)
[43] 행정안전부, 생활안전지도, (http://www.safemap.go.kr/main/smap.do)
[44] 행정안전부, 보도자료, “정부, 세계 최초 LTE 기반 재난안전통신망 구축…사진, 영상 전송도 가능해” 2020/01/15, (https://www.mois.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000911727PtP1Md&fileSn=0)

[45] 대한민국정책조정실, “제 12 차 국가테러대책위원회 보도자료”, 01/19/2021, (https://www.korea.kr/news/pressReleaseView.do?newsId=156434480&call_from=rsslink)
[46] 경찰청, “경찰청 2021 예산 개요”, (https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1023&q_bbscttSn=20201207103005327)
[47] 경찰청, 보도 “인공지능으로 범죄예방의 첫걸음 대디딘다 – 경찰청, 법죄위험도 예측분석 시스템 (Pre-CAS) 시법운영 실시”, 2021/03/01, (https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20210302161224662)
[48] 소방청, “2021 년도 세입세출예산 각목명세서”, (https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000031&nttId=82156)
[49] 신희강, 뉴데일리, “과기정통부·대통령경호처, 경호 분야 R&D 협력방안 논의”, 09/27/2019, (http://biz.newdaily.co.kr/site/data/html/2019/09/27/2019092700096.html)
[50] 박미영, 보안뉴스, “첨단 ICT 기술을 활용한 경호 분야 R&D 협력 방안 논의” 09/28/2019, (https://www.boannews.com/media/view.asp?idx=83333)
[51] 인천국제항공공사, (https://www.airport.kr/co_cnt/en/intro/general/iianum/iianum.do)
[52] 인천국제항공공사, “인천공항 4 단계 건설사업 기공식('19.11.19) [2024 년 세계 3 대 공항으로 도약하겠습니다!]” 12/31/2019, (https://www.airport.kr/ai/ko/cmm/cmmBbsView.do?FNCT_CODE=258&NTT_ID=24338)
[53]박미영, 보안뉴스, “인천공항공사, 공항시설 안전점검에 드론 활용한다”, 2020/11/06, (https://www.boannews.com/media/view.asp?idx=92393&page=1&kind=2)
[54] 해양경찰청, “해양경찰청, 바다와 육지를 연계한 재난안전통신망 구축”, 2020/11/10, (http://www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?nttSn=26112)
[55] 박미영, 보안뉴스, “해양경찰청, 항로 이탈, 과속 선박경보 정확도 높인다”, 2020/12/11, (https://www.boannews.com/media/view.asp?idx=93335&page=1&kind=2)
[56] 박미영, 보안뉴스, “해양경찰청, 해양 대테러 역량 강화 제도적 기반 마련”, 2020/12/15, (https://www.boannews.com/media/view.asp?idx=93410&page=1&kind=2)
[57] 공공기관 경영정보 공개시스템, “한국공항공사 주요사업 현황 2020 젼 1/4 분기”, (http://www.alio.go.kr/popReportTerm.do?apbaId=C0157&reportFormRootNo=31501)
[58] 홍성환, The Guru, “한국공항공사, 올해 공사채 4000 억 발행 계획…’코로나 대응’”, 2021/03/08, (https://www.theguru.co.kr/news/article.html?no=19430)
[59] 지용준, Money S News, “2025 년 UAM 상용화…한국공항공사 등 4 개사 ‘플라잉카’ 어벤져스 구성”, 01/28/2021, (https://moneys.mt.co.kr/news/mwView.php?no=2021012809308032796)
[60] 관세청, “2021 년도 관세청 세입, 세출 예산 개요”
[61]관세청, “2021 년도 관세청 정보화사업 통합 설명회 개최 안내”, (https://www.customs.go.kr/kcs/na/ntt/selectNttInfo.do?mi=2889&bbsId=1341&nttSn=10054376)
박미영, 보안뉴스 “관세청, 2021 년 추진 모든 정보화 사업 온라인 설명회 개최” 2020/11/3 (https://www.boannews.com/media/view.asp?idx=92287&page=1&kind=2)
[62] 정혜인, 아주경제 “국정원 2021 년도 안보비, 특활비 예산 1 조원 이상” 2020/11/16 (https://www.ajunews.com/view/20201116082540160)

[63] DAPA, “Procedure for DAPA-RFQ”, (http://www.d2b.go.kr/fbis/rfq/engRfqProcedure.do?md=221)
[64] YTN, “[속보] 어제 하루 환자 465 명 추가...국내 확진자 94,198 명으로 늘어”, 3/11/2021, (https://www.ytn.co.kr/_ln/0103_202103110934108738)
[65] 김수진, 연합뉴스, “[팩트체크] 작년 한국 경제성장률 "OECD 최상위권" 사실?”, 01/18/2021, (https://www.yna.co.kr/view/AKR20210118157900502)
[66] 기획재정부, “IMF “올해 한국 경제 3.1% 성장…2 년간 성장률 11 개 선진국 중 1 위”, 2021/01/21, (https://www.korea.kr/news/policyNewsView.do?newsId=148883178)
[67] 기획조정부, “한국판 뉴딜”, 07/14/2020, (https://www.moef.go.kr/nw/nes/detailNesDtaView.do?searchBbsId=MOSFBBS_000000000028&searchNttId=MOSF_000000000040637&menuNo=4010100)
[68] Eun-Young Jeong, The Wall Street Journal, “South Korea’s Population Falls for First Time, Likely Worsened by Covid-19”, 01/04/2021, (https://www.wsj.com/articles/south-koreas-population-falls-for-first-time-likely-worsened-by-covid-19-11609767528)
[69] Ibid
[70] Sam Kim, Bloomberg Businessweek, “South Korea’s Robots Are Both Friends and Job Killers”, 11/11/2019, (https://www.bloomberg.com/graphics/2019-new-economy-drivers-and-disrupters/south-korea.html)
[71] International Federation of Robotics, “Robot Race: The World´s Top 10 automated countries”, 1/27/2021, (https://ifr.org/ifr-press-releases/news/robot-race-the-worlds-top-10-automated-countries)
[72] Yunwhan Chae, Yonhap News, “S. Korea's R&D spending 5th largest among OECD members in 2019”, 12/9/2020, (https://en.yna.co.kr/view/AEN20201209003800320)
[73] Suhyun Song, The Korea Herald, “Korea rises to 4th place in international patent filings”, 03/04/2021, (http://www.koreaherald.com/view.php?ud=20210304001050)
[74] Jun-Ho, Jung, Korea IT Times, “KT succeeds in sending 5G data with native quantum cryptographic technology”, 02/04/2020, (http://www.koreaittimes.com/news/articleView.html?idxno=97418)
[75] MyITU, “COVID-19: How Korea is using innovative technology and AI to flatten the curve”, 02/04/2020, (https://www.itu.int/en/myitu/News/2020/05/06/11/53/COVID19-How-Korea-is-using-innovative-technology-and-AI-to-flatten-the-curve)
[76] Ministry of Science and ICT, “National Strategy for Artificial Intelligence”, 03/23/2020, (http://english.msip.go.kr/cms/english/pl/policies2/__icsFiles/afieldfile/2020/03/23/National%20Strategy%20for%20Artificial%20Intelligence_200323.pdf)
[77] LG CNS, “AI and Big Data“, (https://www.lgcns.com/en/Platform/AIBigdata-DAP)
[78] UNCTAD, 2018 KONEPS Presentation

This document is also available on our website at gov.uk/dit-ukdse

Published March 2021 by UK Defence & Security Exports

UK Defence &
Security Exports

Part of

Department for International Trade