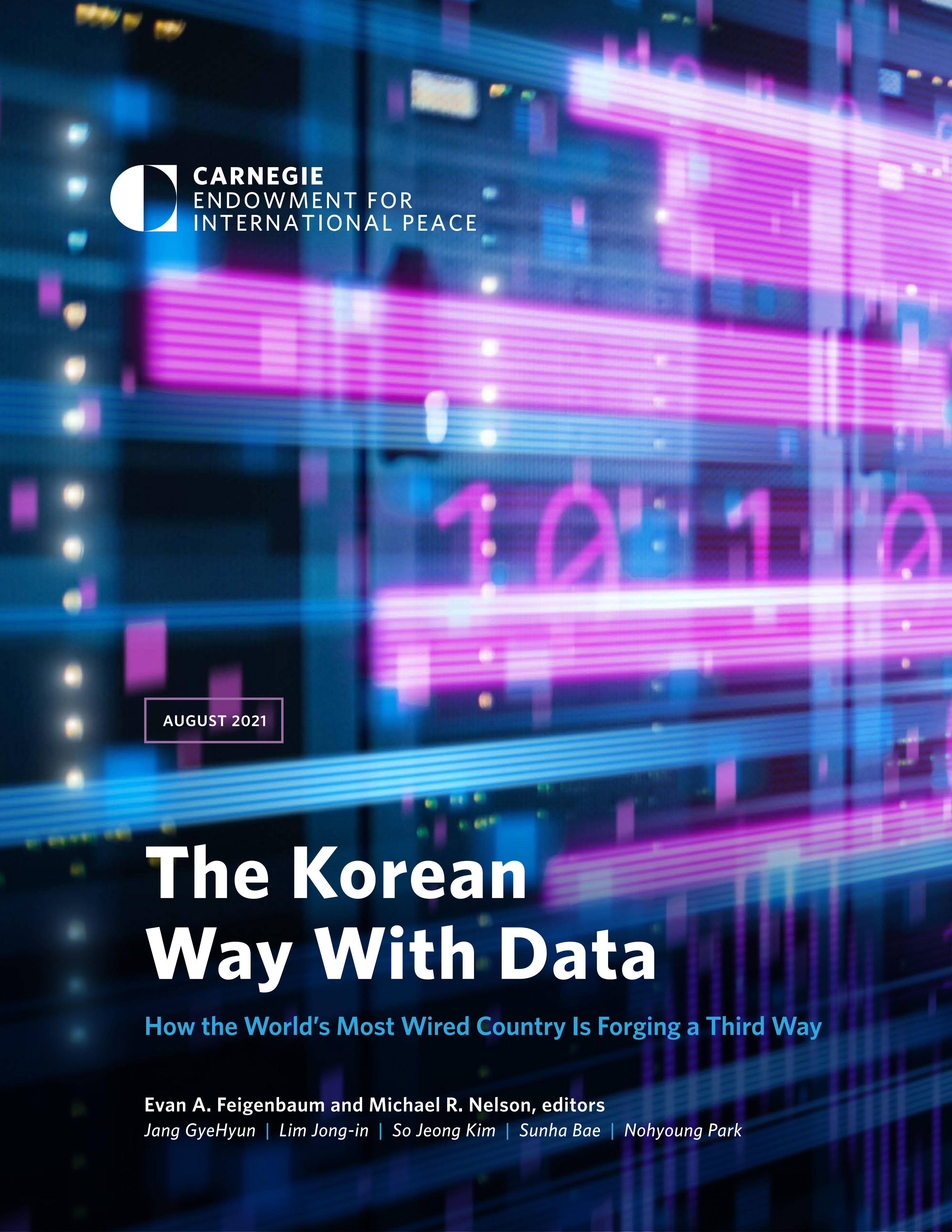


CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

AUGUST 2021

The Korean Way With Data

How the World's Most Wired Country Is Forging a Third Way

Evan A. Feigenbaum and Michael R. Nelson, editors
Jang GyeHyun | *Lim Jong-in* | *So Jeong Kim* | *Sunha Bae* | *Nohyoung Park*

The Korean Way With Data

How the World's Most Wired Country Is Forging a Third Way

Evan A. Feigenbaum and Michael R. Nelson, editors
Jang GyeHyun | *Lim Jong-in* | *So Jeong Kim* | *Sunha Bae* | *Nohyoung Park*

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Project Participants

We are grateful to participants in a transpacific workshop on "Korea and the Future of Data," and especially to those who offered helpful comments on drafts of the chapters in this volume. And we express our thanks to the Korea Foundation for its generous support of this project.

Fiona Alexander
American University

Alexander Botting
Venable, LLP

Andre Boysen
SecureKey

Michael Daniel
Cyber Threat Alliance

Clara Gillispie
National Bureau of Asian Research

Jeremy Grant
Venable, LLP

Minjeong Kim
Korea Foundation

James Larson
Stonybrook University, Korea

Malcolm Lee
Malcolm Lee Associates, LLC

Chung Min Lee
Carnegie Endowment for International Peace

Sarah Mack
Georgetown University

James Miller
American Chamber of Commerce in Japan

Eli Noam
Columbia University

Kyung Sin "KS" Park
Korea University

Samuel Visner
MITRE Corporation

INTRODUCTION

How Korea Can Unleash the Power of Data

EVAN A. FEIGENBAUM AND MICHAEL R. NELSON

The emergence of a deep-seated, multidimensional strategic competition between the United States and China has led many to argue that the world is fracturing into two spheres—a Sinocentric order and a U.S.-centric one. One result of this fragmentation, some suggest, could be that Beijing sets the terms of data and internet governance and technology standards in Asian countries and beyond.[1] As the world moves into the next phase of the digital transformation, what was once viewed as a purely commercial and technological competition is increasingly being framed as an existential geopolitical one.

The fact is, however, that the United States and China are not the world's only major digital players. There has been a proliferation of policy and regulatory models in recent years, and international internet governance is up for grabs as countries, from India to Japan to South Korea, experiment, innovate, and share their policy experiences and practices, successes, and failures.

Data governance is one critical area of contention because it is increasingly central to next-generation industries and the future of rulemaking in the global economy. Countries such as South Korea (hereinafter Korea) and India have developed distinctive national approaches to data governance. Neither country aims to imitate or adopt wholly American, much less Chinese, data policies and practices. They, too, have the potential to drive debates about technology business models and regulatory frameworks.

Korea, in particular, is a digital pacesetter because it is perhaps the world's most connected country. Korea's internet access, according to the Pew Research Center,[2] reached a staggering 96 percent of adults in 2018, and the country boasts the world's highest 4G telecommunications availability and highest fixed broadband upload speed, according to a recently published connectivity index.[3]

Much has already been learned from Korean experiences with technology. Korean consumer electronics companies, such as LG Electronics and Samsung, have grown quickly to become household names around the world. In many areas, from manufacturing to business services, the rest of the world has seen the results of Korean approaches to policy and regulation. Indeed, precisely *because* Korea is such a wired country, much can be learned by examining those policies and regulations in more detail.

Unfortunately, Korea's digital policies are still not widely known, in part because little has been written in English about Korea's distinctive frameworks, standards, and models. In most countries, policymakers tend to look to the United States, Europe, or China for templates as they craft their own digital policies and regulations. Yet Korea has over the past two decades pioneered important approaches to data governance while accumulating a body of experience with best practices—and sometimes not-so-best practices that it has had to tweak, amend, or replace. These experiences provide useful lessons.

This volume digs deeply into what we call "the Korean way with data." It explores in detail Korea's distinctive experiences, successes, failures, and recalibrations. Above all, it aims to address the question of what can and should be learned from innovative Korean policies and practices. The chapters in this study highlight the elements of distinctively Korean approaches, establishing a firm foundation on which to compare and contrast what is emerging there with other countries' experiences and choices.

Korean approaches have demonstrated that persistence, a consistent vision, and innovative policy frameworks can shape a promising digital future. For more than twenty years, policymakers in Seoul have done much to build out national broadband networks and spur the use of digital technologies.

And yet for all of Korea's successes, much work remains to be done if Seoul is to address three critical challenges:

- Intensive commitment to online government, banking, and healthcare services requires an online authentication ecosystem that Korea has struggled to create.

- Intensive digitalization across industries and society makes Korea susceptible to cyber threats and disruptions; several governments and cyber-hacktivist groups have regularly targeted Korea, and will, no doubt, continue to do so.

- Intensive dependence on cross-border flows of goods, capital, people, and technology in one of the world's most trade-dependent economies requires a data regulatory framework that meshes with those of Korea's principal economic partners.

In Korea, as in almost every country, competing ministries with competing priorities often prevent consensus on how best to design policies for the internet and the cloud. This can lead to what could be referred to as "multiple-policy disorder," a pathology that leads to confusion among both technology companies and technology users.

The three chapters in this volume illustrate how the Korean government has tried to craft coherent and consistent policies in three important areas related to data:

- developing effective online authentication systems for protecting data and information technology (IT) systems;
- dealing with cyber threats and improving data resilience; and
- facilitating the free flow of data internationally while protecting the privacy of Korean citizens.

In each case, Korean policies have evolved by trial and error. Different approaches have been tried. When found to be inadequate, more workable approaches were found.

In all three of these areas, executive leadership from the Korean president's office helped to overcome inertia and compel ministries to work together. Further refinement and clarification of policies is needed, especially in the area of data localization rules. But, taken together, the resulting frameworks constitute a Korean way with data that could have broad resonance for countries that are also struggling to address these three issues.

Data-Enabled Online Authentication

The first chapter by Jang GyeHyun and Lim Jong-in of Korea University focuses on online authentication and data access, which are essential for improving cybersecurity. An easy-to-use online authentication ecosystem could provide secure access to e-government services, online banking, and healthcare services—all areas where Korea has excelled. And better authentication could go a long way toward making phishing, spamming, disinformation, malicious hacking, and insider cyber theft more difficult and less profitable.

The authors detail a process of trial and error and persistent experimentation with various online authentication initiatives in Korea over the last twenty years. Initial efforts based on the Resident Registration Number resulted in widespread sharing and disclosure of sensitive, personally identifiable information (PII) and had to be shut down. An alternative, I-PIN Korea, was developed fifteen years ago, but could only be implemented using Microsoft's ActiveX technology, limiting its usefulness. In both cases, it again took intervention by the president himself to stop both efforts and push for better alternatives.

That yields a straightforward lesson: even in an advanced economy like Korea's, presidential leadership can be the prerequisite of progress. It would have taken much longer for the Korean government officials involved in these efforts to admit that changes were needed without the president's intervention.

What resulted, however, was an effort to provide a wider, more flexible range of online authentication approaches: In 2012, the Korean government authorized three mobile network operators to provide authentication services. Five years later, the Korea Communications Commission designated seven major credit card companies as new identity-verification agencies. The solutions they have deployed, which have been much more widely adopted and used than earlier government-led approaches, have facilitated e-commerce, e-government, and mobile applications in Korea.

One conclusion is that the Korean government recognized earlier than almost any other government in the world that e-mail and social media platforms could facilitate defamation, fraud, and doxing. It also recognized that better online authentication could reduce these serious and growing problems. In July 2007, a real-name system was launched to prevent anonymous posts on popular internet websites. This led to complaints by privacy and free speech advocates and a lawsuit claiming that the law was not consistent with the Korean Constitution. What is more, because the law could not be enforced on foreign websites like YouTube, Korean domestic websites argued that the law disadvantaged them. Ultimately, in August 2012, the Constitutional Court ruled this law unconstitutional.

This raucous Korean debate over real-name authentication provides a valuable lesson on the need to design online authentication schemes that can meet the need to improve cybersecurity and data access control while respecting the need of internet users and corporations to protect their private information. Unfortunately, in the Korean case, advocates for privacy and civil liberties were not very involved in designing the specifications and policies for online authentication.

So, as Korea and other countries continue to refine their approaches to authentication, they will need to consider how systems and procedures might enable citizens to verify *what* they are but without providing details on *who* they are. This might mean that internet users can protect their privacy by using a pseudonym or by sharing personal information with a trusted third party: this could verify that particular user's attributes, such as age, income, and nationality, without revealing who they are. A number of cryptographic techniques, including homomorphic encryption, are making such privacy-enhancing techniques more practical and secure.

Another lesson of the Korean experience with schemes for online authentication is that the most successful ones will be those that leverage the infrastructure and business relationships of the private sector, including mobile companies and credit card companies. Developing a system solely for a few government applications is unlikely to be very successful, since not many citizens interact with their government on a weekly or monthly basis. If, on the other hand, governments accept the authentication tools that their citizens are already using for online banking or e-commerce, users are more likely to adopt and trust them. And if these private sector–based approaches are being used in more than one country, the potential applications (and economies of scale) will be much larger.

This is another reason that the latest Korean approach could position the country as a champion of better authentication around the world. Estonia and India, which have invested both money and political capital in their national authentication systems, have demonstrated the benefits that effective online authentication can provide. But their government-led approaches are less likely to lead to third countries embracing their approaches as national, much less global, models. As Jang and Lim note, governments that fail to find international partners will suffer from the so-called Galapagos syndrome because their approach to online authentication will not be interoperable with those used by other countries. If governments cannot overcome this challenge, their citizens might need to rely instead upon authentication services provided by global companies like Apple, Facebook, and Google.

Korea also provides an important set of lessons for the United States. Unlike Korea, Washington has been unable to develop a coherent strategy for online authentication despite trying for more than ten years. The *National Strategy for Trusted Identity in Cyberspace* (NSTIC) announced by former president Barack Obama's administration in 2011 engaged the full range of stakeholders but failed to agree on how to address such key questions as how to protect users' privacy; how to leverage private sector solutions; and how to avoid narrow solutions and ensure interoperability and flexibility?[4] The good news is that the U.S. Department of Commerce's National Institute of Standards and Technology is working to build on the work of NSTIC.[5] As the United States undertakes this and other cybersecurity efforts, it would do well to learn from Korea's experience.

Data Resilience

The second chapter by So Jeong Kim and Sunha Bae of Korea's National Security Research Institute describes in detail how the Korean government has designed a management structure for defining and coordinating cybersecurity policy and improving the resilience of Korean government and corporate information and communications technology (ICT) systems. The chapter documents how the many cyber attacks targeting South Korea over the last twenty years—often originating in North Korea—have triggered a number of narrow policy responses.

But this reactive approach resulted in a patchwork of initiatives rather than the development and implementation of a comprehensive strategy to reduce the number and severity of attacks. So, in 2019, Korea finally adopted a full-blown National Cybersecurity Strategy and an implementation plan.

Today, responsibility for cyber defense is split between the National Cyber Security Center under Korea's National Intelligence Service (for government and public sector data) and the Ministry of Science and Information and Communications Technology (for private sector data). In addition, several agencies run their own response systems, such as the one at the Ministry of National Defense for the military sector's data. Successful implementation of this plan will depend critically on the National Security Council under the Office of the President. It must serve as the control tower for policy coordination across the government and between the public and private sectors.

Yet that is no simple task. It will require a multistakeholder approach that reflects not just the needs of the ministries and offices involved but also addresses the diverse and distinctive needs of Korean companies and Korean citizens. Policies that provide multiple solutions that are flexible, affordable, and easy-to-use will work far better than the kind of one-size-fits-all approaches that some other countries have tried. Korea may well show the way.

The authors of this chapter cite recent surveys showing that Korean businesses and government agencies have accelerated efforts to secure their IT systems, protect against denial-of-service attacks, and install systems to back up data and facilitate recovery after an attack. Over the last few years, this has successfully reduced the amount of *damage* caused by cyber attacks despite a steady increase in the *number* of attacks. One approach that other countries might wish to emulate, then, are Korean regulations that require data backup systems. This effort is supported by Korean policies pushing for more use of cloud storage, particularly in the public sector through Korea's Cloud Service Assurance Program, which parallels U.S. government programs like FedRAMP, the Federal Risk and Authorization Management Program.

Data Localization and Privacy

The third chapter by Nohyoung Park of Korea University Law School examines Korean approaches to data protection and data localization, and especially the framework of laws and treaties that Korean policymakers, legislators, bureaucrats, and negotiators have painstakingly assembled over the last two decades. These related issues—protection and localization—are among the thorniest digital policy issues that national governments everywhere are trying to address. And no country has yet found an approach that works for its citizens and businesses and is also both interoperable and consistent with data policies of other countries. The different, often poorly defined and inconsistently applied rules resulting from the Chinese and Indian approaches to localization and the European Union's General Data Protection Regulation (GDPR) indicate how much work remains to be done.

This is a high bar to clear, but it is especially important for Korea—a country that is incredibly dependent on trade and cross-border economic flows of goods, capital, people, technology, and data—to do so. Despite some slippage during the coronavirus pandemic, Korea's trade dependency index (the total trade volume proportion of gross domestic product) still came in at a whopping 63.51 percent in 2020, according to the Korean Statistical Information Service run by Statistics Korea of the Ministry of Economics and Finance.[6]

As a major trading partner with China, the United States, the European Union, and Japan, Korea has a particularly difficult task. Korean firms are exposed to a variety of emerging global data laws, including the different ways European nations are choosing to enforce the GDPR, as well as the California Consumer Privacy Act (CCPA) and the new Indian data protection law, among others. And they must deal, too, with especially tight controls over the regulation of data in China, the country's largest trading partner.

Yet this is where Korea's opportunity lies: Korea has the potential to be a model for *all* of its trading partners and to shape and harmonize policies for cross-border data flows. If Korea can find ways to demonstrate that it has effective data protection measures, Korean firms can earn the trust of both Koreans and foreign companies, which might then be willing to team up with Korean partners. With new advancements in artificial intelligence, machine learning, the Internet of Things, robotics, and bioinformatics, the free flow of data across international borders will become even more important. For Korea to be well-positioned to capture these innovation opportunities, it needs to actively build on its experiences by helping to shape the evolving global regime on cross-border data flows and access.

Park's chapter lays bare the very real tensions between Korean citizens' desire for privacy—reflected in the strong Korean data protection laws—and the desire of Korean businesses to take advantage of non-Korean online tools and services and partner with foreign companies. There is also a tension between Korean privacy laws, on the one hand, and, on the other, the desire of both the Foreign Ministry and the Office of the President to be able to sign onto several bilateral and multilateral treaties that impose tight limits on how national law can enforce its data localization requirements. One result has been complaints from the United States—its second-largest export partner after China,[7] and second-largest source of foreign direct investment (FDI) stock after Japan[8]—that Korea is not living up to some of its treaty commitments to allow data from Korea to be exported, especially in the case of sensitive data, such as map data.

The coronavirus pandemic has highlighted the benefits of sharing and analyzing both health data and geolocation data. From Taiwan and China to Korea and Israel,[9] major economies have used geolocation data from cellphones for coronavirus-related contact tracing. Data on who has and has not been vaccinated or infected has likewise helped to assess the utility of different types of vaccines and different protection measures.

Park's chapter traces how Korea enacted the Personal Information Protection Act (PIPA) in 2011, which applies to the processing of personal information in both the private and public sectors. This was followed by the so-called Network Act—the Act on Promotion of Information and Communications Network Utilization and Information Protection—which applies to the protection of personal information processed by information and communications service providers. The most recent data protection legislation, Korea's so-called three data laws amendments, were adopted in January 2020, combining the data protection provisions of both of these acts into PIPA.

Park explains how implementation of Korean privacy laws can limit the export of data to countries judged to have less rigorous data protection laws than Korea. An additional constraint on cross-border data transfers is the desire for reciprocal treatment of data. If foreign countries do not allow transfer of their citizens' data to Korea, then Korea may, in turn, block transfer of Koreans' data to those countries to pressure them to lift their data localization requirements.

The collision of these different policy goals will necessitate some new thinking—and perhaps new business models and new technologies.[10] But Korea *has* seen a high-level push to find ways to maximize the potential of data and emerging technologies, such as machine learning and location-based services. This crystallized in President Moon Jae-in's June 2020 announcement of what he calls the Digital New Deal to promote expansion and new uses of Korea's DNA—data, network, and artificial intelligence—ecosystem.[11] Still, the Digital New Deal's ambitious goals to harness digital data for improving health, safety, government services, and business will only be achievable with more consistent and effective data protection regulations and more clear-cut data localization policies.

Korean Policymaking as a Model?

A willingness to shift course after a process of trial and error is not the only reason that Korea has succeeded. The country has also done well with the deployment of specific technologies.

One example is Korea's rollout of broadband internet over the last thirty years. Here again, Seoul made digital policy a presidential priority. And this involvement by the Blue House made a huge difference.

Other world leaders, including U.S. President Joe Biden, have, in the last year or two, accelerated broadband development by making it a priority for their administrations.

Executive leadership at the topmost ranks of government was also important to Korean success because bold-thinking politicians can help to drive or at least entrench broad and consistent political support for a strategic goal. Korea did this by, for example, forging ahead with the ambitious goal of building a national fiber optic network to serve all Korean citizens.

As both the World Bank and,[12] more recently, the Electronic Frontier Foundation,[13] have explained, the result of Korea's push for broadband has been to achieve some of the highest internet penetration in the world and, until a few years ago, low costs per megabit for connectivity. The key to this effort was a decision in 1999 to spur competition among the two telecommunications companies that dominated the Korean network business then. What resulted was a vibrant market with four major players and several smaller ones. And the resulting competition and innovation, when combined with state funding for government networks and subsidies for rural broadband, led to one of the fastest and earliest buildouts of fixed broadband networks in the world. Today, Korean companies are among the world leaders in 5G wireless broadband.

Many challenges remain when it comes to Korea's digital policies. Since early 2016, the Korean telecommunications regulator responded to lobbying from the three largest network services providers, who argued that they were bearing more than their fair share of carrying internet traffic than the smaller networks with whom they interconnected.[14] The rapid growth of video streaming services like Netflix had led to a rapid increase in traffic and necessitated more investment in network infrastructure. So, a complex (and frequently revised) internet interconnection fee structure has been imposed,[15] which favors the three largest Korean network service providers at the expense of smaller players.[16]

The idea of government-mandated interconnection fees runs counter to the norm in almost every other country in the world where there is a competitive broadband market. In those countries, we have seen a preference for negotiated contracts between networks. Recently, Netflix, which has challenged the fees, was sued by the Seoul-based SK Broadband in a Korean court. The court found Netflix liable for unpaid fees that could amount to more than $85 million per year.[17] This may seem like an arcane dispute between telecommunications companies, yet the fact that the Korean government explicitly favors just three such companies will result in less vigorous competition and less investment. Most importantly, several innovative new online services, such as certain content distribution network and cloud computing services, are *not* being offered in Korea because of the dramatic increase in networking costs resulting from these new fees. In an afterword at the end of this volume, Kyung Sin "KS" Park and Michael R. Nelson explain in detail the possible adverse consequences of these Korean efforts to impose interconnection fees.

This is an example of where Korean experiences may have gone awry. It is also an area ripe for the kind of digital leadership by Korea's president that has been such a necessary ingredient of success in the past. From both a political and policy standpoint, such leadership is needed so that Korean internet users and digital innovators are given priority over the interests of just three companies.

These are the choices and trade-offs that face democracies. Korea's democracy, much like the United States, has struggled with other shared challenges, not least how to contain the damage done by disinformation.[18] North Korea has used the internet to deliver disinformation and propaganda to South Korea. But disinformation and rumors generated by South Koreans themselves are also having a major impact, especially on Korean politics.[19] For example, Korean internet companies have aggressively blocked websites that spread rumors and bogus news stories. But free speech advocates in Korea (and elsewhere) have fought against government efforts that could limit discourse online.

Korea has the opportunity to find new approaches, perhaps by using the kinds of authentication technologies that Jang and Lim outline in their chapter to validate social media accounts associated with real people while spotting phony accounts used to amplify posts containing disinformation. Of special concern are so-called deep fakes—deceptive images and video created by machine learning algorithms.[20] Companies like Microsoft and Adobe are hard at work on new approaches to verifying the authenticity and provenance of online content.[21]

Another, even thornier, digital issue that is ripe for Korean leadership is encryption. For more than twenty-five years, the governments of major democracies have struggled to craft policies that would enable the use of strong encryption to protect ICT systems and the data they contain while dealing with the threat from criminals and adversaries who use encryption to conceal their activities. This is made difficult because of the very different priorities of the law enforcement and intelligence agencies that want easy and inexpensive access to data, on the one hand, and the agencies responsible for data protection and cybersecurity, on the other.[22] There has been little public debate over encryption policy in Korea but there *is* a clear understanding of how encryption is an essential tool for protecting privacy. In fact, Korea's Personal Information Protection Act explicitly encourages companies to use encryption to protect sensitive data.

Korea in the Geopolitical Storm

One reason Korean leadership could be so important is that the bifurcation of the world into a Sinosphere or an American sphere would not serve the interests of most countries.

For decades, technology policies have been shaped by two competing approaches: models that empower individual users and innovators (particularly at start-ups) and respect human rights and models designed to give governments more control over what technologies develop, how they are deployed, and which companies profit most (usually large incumbents and national champions).

To some extent, the United States today views itself as the champion of the former. China, by contrast, has both practiced and increasingly argued for elements of the latter.

But many countries, even well-established democracies, are developing a hybrid approach. From Europe to Asia, many democratic governments rely on industrial policies and promote national champion firms. They are taking a strategic approach to the development of technology and the governance of domestic and cross-border data access and transfers, and sometimes disagree on the best path forward.

On data governance, in particular, there has been no putative American-led "Team Democracy" vs. a Chinese-led "Team Autocracy." Indeed, when former Japanese prime minister Abe Shinzo tried to push forward a cross-border data initiative at the 2019 Osaka G20—the so-called Osaka track,[23] which Abe's government based on a concept of "data free flow with trust" (DFFT)[24]—India and Indonesia, two prominent G20 democracies that Washington views as key like-minded partners in Asia, refused to sign up.[25]

Ironically, for all their ideological and strategic differences, Beijing and Washington are approaching the region in similar ways. Both have framed the competition over global rules in increasingly stark terms. Each is suspicious of any regulatory ideas developed by the other. Each is encouraging third countries to accept its preferred norms, standards, and rules. And each has framed the technology challenge, including over data flows, in geopolitical, not just commercial, terms. Each has sometimes coerced others to forestall closer integration with its rival.

Korea could offer a third way—one that relies on practices and experiences developed and incubated in a successful democracy that has also carved out an important role for the state and sought a balance between public and private interests and state and market-based approaches.

The intensifying battle between Beijing and Washington is leading to trade disputes, restrictions on foreign investment, and, increasingly, wholesale bans on the use of foreign web services and apps. Yet as this Carnegie volume clearly demonstrates, countries like Korea have pioneered their *own* unique approaches to technology governance and regulation.

It is important to highlight these alternative models—and to compare and contrast their distinctive features. The chapters in this volume demonstrate that the future will be much more complex than a battle between U.S.- and China-centric approaches.

CHAPTER 1

Technologies of Trust: Online Authentication and Data Access Control in Korea

JANG GYEHYUN AND LIM JONG-IN

Introduction

Information and communications technologies (ICT), particularly the internet and cloud computing, are becoming the substrate for economies and societies. They allow individuals and organizations worldwide to connect, exchange information, and collaborate. They have had a profound impact on industries, politics, and the media. The coronavirus pandemic has only accelerated the shift of business, education, government, and other core activities to the online world, with potentially lasting effects.

Digital technologies provide many conveniences, but they have also enabled crime; disinformation; the theft of private information, confidential business information, and intellectual property; cyber attacks; and cyber espionage. ICT companies are racing to address vulnerabilities in their hardware and software and trying to keep ahead of malicious hackers who are constantly finding new ways to exploit these vulnerabilities.

It is much harder to establish identity and trust online than in a face-to-face environment, resulting in identity fraud and unauthorized access to computer systems and the data they contain. As in other countries, internet users in the Republic of Korea (hereinafter the ROK or Korea) expect and often demand better and easier methods for online authentication and data access control. As a major economy and one of the most "connected" countries in the world,[26] Korea's experience in delivering these services can provide important lessons, both for peer economies and for other countries searching for models they can learn from.

Online authentication is a crucial security measure for identifying users and for validating the online apps they access. Invariably, there is a trade-off between the conflicting goals of usability, innovation, reliability, standardization, and consumer protection. A successful and broad deployment of authentication tools and techniques can lead to greater trust online, enabling user identification, electronic signatures, and nonrepudiation. However, rigorous online authentication may require additional (and sometimes inconvenient) security measures and information such as multifactor authentication.

In Korea—and everywhere else—data access control is a matter of balancing utilization and data protection. The openness and utilization of data improve access to information across society, creating substantial value, such as transparency and data-driven decisionmaking in government, marketing, healthcare, and other areas. However, the collection and sharing of data will inevitably lead to problems such as the misuse of personal data, infringement of privacy, and loss of control by the users, which should also be considered. In addition, there are fears that data transferred abroad will not be properly protected. This is leading to conflicting goals: international data flows, which enable Koreans to use cloud services from hundreds of different providers, conflict with data localization requirements designed to help Korean companies and the government leverage data about Korean citizens and entities.

In developing its strategy for online authentication and data access, the Korean government and the ICT companies operating in the country have had to make several difficult choices, which reflect their conflicting values. This path to a so-called Korean model has not been smooth. And like elsewhere in the world, Korean decisionmakers and stakeholders have had to learn by trial and error.

This chapter explores how the core policies related to online authentication and data access control have been developed and implemented in Korea, focusing on the major changes and the reasons behind them. The chapter first analyzes the drivers of those policies, such as Korea's ICT policy, cybersecurity incidents, cybersecurity policies, and the major actors working to improve cybersecurity. The challenges of online authentication are divided into two parts: *online identification* (user validation) and *authentication online* (activity validation). The challenges of *data access control* are likewise divided into two parts: public data and private data.

The Origins and Evolution of a Korean Approach to Online Data

Korea's approach to online authentication and data access control reflects several unique characteristics of the country's economy, infrastructure, and development. For one, Korea has invested heavily in ICT infrastructure as a national priority, building broadband networks and extending their reach into almost every home. With an average of more than 200 megabits per second for fixed broadband speed,[27] the country's broadband networks have created a powerful platform for innovation.

Korea has been a divided country for more than sixty years, and the Republic of Korea's neighbor, North Korea, is known as a major malicious actor online worldwide. This has made ROK's online authentication and data access control policies and implementation even more important.

Of course, Korea is not alone in facing a hostile external environment. Other countries, like Estonia and Taiwan that face acute cyber threats from threatening neighbors, have also invested heavily in cybersecurity.

However, Korea's experience is also anchored by historical experiences and practices that are unique to the country's development trajectory since the 1960s. During that decade, Korea launched its drive for rapid industrialization, which included a national-level personal identification system that became especially important as the country's economy began to move online in subsequent decades. Moreover, Korea established and enforced a national-level authentication infrastructure superior to many other certificates called the National Public Key Infrastructure-based Authorized Certificate (NPKI-based AC). Unfortunately, several problems have emerged with the certificate because it is difficult to use and dependent upon a single technology platform. As a result, the use of these identification and authentication methods has been limited, and the government has had to introduce alternative methods.

In the main, Korea's approach to data accessibility has been conservative. Yet, that is changing today due to a clear recognition by government officials, corporate leaders, and citizens alike of the need for a more flexible, open policy to reflect social demands and changes in the business environment.

The Information and Communications Technologies Environment of Korea

Korea is recognized as having one of the most advanced ICT infrastructures in the world,[28] and it has become a testing ground for leading-edge applications. The country has consistently ranked first or second among 176 countries on the International Telecommunication Union ICT Development Index since 2009 and also ranked second in 2017, the most recent survey.[29] Korea is also among the world's top in terms of internet and smartphone penetration as of 2020.[30] In addition to the ICT infrastructure, it is also top-notch in utilization and service. In the UN E-Government Development Index, Korea is consistently near the top, ranking first three consecutive times (2010, 2012, 2014) and second in the most recent announcement in 2020.[31] Moreover, Korea's proportion of e-commerce transactions has reached 30 percent,[32] and the proportion of online banking has reached 66 percent.[33]

In addition to Korea's rapid economic growth and so-called "*ppalli ppalli*" (faster, faster) culture, geographic and demographic advantages and its government-driven policies have been major factors in its ICT development (see table 1). In the 1970s, a national public administration initiative led to the establishment of a resident registration system and computerization of administrative information. In the 1980s, policies for the spread and expansion of telecommunication networks were implemented in earnest. In the 1990s, ultra-high-speed information communication networks were developed. And in the 2000s, the change to an information society led to the development and dissemination of internet-based technologies, laying the foundation for e-government services and improving information security.

Table 1. Major Data and Informatization Policies in Korea

Paradigm	National policies of Korea
Computerization: Public Administration 1975–1985	Computerize public administration ▪ President Park Chung-hee's order to computerize public administration (1975) ▪ First Master Plan for Computerization of Public Administration (1978–1987)
Computerization: Expansion 1986–1995	Expand national basic information system ▪ Act on Computer Network Expansion and Usage Facilitation (1986) ▪ First Master Plan for National Basic Information System (1987–1991) ▪ Second Master Plan for National Basic Information System (1992–1996)
Informatization: Internet 1996–2005	Promote national and social informatization ▪ Framework Act on Informatization Promotion (1995) ▪ First Informatization Promotion Master Plan (1996–2000) ▪ Cyber Korea 21: Second Master Plan (1999–2002) ▪ Comprehensive Plan for Super High-Speed Information Infrastructure (1995) ▪ E-Government Project (2001) ▪ IT 839 Project (2004)
Informatization: Mobile 2006–2013	Establish a knowledge information society ▪ E-Korea Vision 2006: Third Master Plan (2002–2006) ▪ Fourth National Informatization Master Plan (2008–2012) ▪ Broadband IT Korea Vision 2007 (2003–2007)

Korea's ICT policy was implemented under a clearly defined, government-driven strategy, which was effective in terms of infrastructure construction and foundation building. However, one limitation of this approach was that technology was often developed according to government specifications rather than market demand. For instance, the WiBro wireless broadband technology that was developed, generously funded, and promoted by the Korean government failed. This technology could not succeed in the market and failed to compete against the LTE (Long-Term Evolution) in 4G network.

Korea's geographic and demographic advantages were also important factors. In evaluating the ICT development environment of states, factors like population, gross domestic product, area, and particularly population density affect the availability of broadband and mobile networks. Korea ranks twenty-third in terms of population density, but fourth among countries with an area of over 2,000 square kilometers and first among the Organisation for Economic Co-operation and Development (OECD) countries. In addition, Korea is highly urbanized: 47.5 million people (91.8 percent of the country's 51.8 million population) live in cities as of 2020.[34] This has clear advantages for ICT development, deploying online services, and addressing the connectivity divide and other types of digital divides.

Entities and Laws Related to Trust in Online Services

A number of government entities have shaped Korea's efforts to foster trust online (see table 2). An important factor in the study of Korean public administration is the analysis of the relevant ministries and the legal system under their jurisdiction. In Korea, for each issue, the law stipulates in detail which ministries have roles and responsibilities for them, and how they are regulated and responded to. In areas of online authentication and identification, the Ministry of Interior and Safety is a key organization and oversees the Resident Registration Act, the E-Government Act, and the Information Disclosure Act. In the past, it was also in charge of the Personal Information Protection Act, which was changed to the jurisdiction of the Personal Information Protection Commission in 2020. Another major entity is the Ministry of Science and ICT, which is in charge of Korea's most important security-related law, the ICT and Security Act. It deals with various internet-related issues such as online security, protection of personal information, and countermeasures against illegal information. In addition, the Ministry of Science and ICT is also in charge of the Electronic Signature Act, which is the core of online authentication. In the financial sector, the Financial Services Commission deals with electronic financial transactions and credit information protection.

Table 2. Korea's Major Entities and Laws Related to Trust in Online

Law	Related entities	Major issues related to online authentication and data access control
Resident Registration Act	Ministry of the Interior and Safety	• Issuance of the personal identification number given to all citizens on a 1:1 basis, the Resident Registration Number (RRN) • Issuance of the national ID card, the Resident Registration Card
Electronic Signature Act	Ministry of Science and ICT	• Regulates detailed requirements of the National Public Key Infrastructure-based Authorized Certificate
Electronic Government Act	Ministry of the Interior and Safety	• Regulations on the e-government service • Requirements for authentication measures to use the service
Electronic Financial Transaction Act	Financial Services Commission	• Regulation of authentication methods required for electronic financial transactions
Act on Promotion of Information and Communications Network Utilization and Information Protection (ICT and Security Act)	Ministry of Science and ICT	• Overall online service providers' personal data protection, including online identification measures • Alternative identification measures of the RRN • Designation and operation of the identity verification agencies
Personal Information Protection Act	Personal Information Protection Commission	• Regulations on overall personal information protection • Restriction on collection of unique identification numbers, including RRNs • Data access control issues such as overseas data transfer and use of personal information
Credit Information Use and Protection Act	Financial Services Commission	• Regulations on the protection of the personal credit information • Provision of requirements for using personal credit information
Official Information Disclosure Act	Ministry of the Interior and Safety	• Guarantee the right to know about public data • Regulations on the information disclosure claims

Major Cyber Incidents

Although Korea has succeeded in deploying a highly developed, digital infrastructure, the country still faces many difficulties in terms of cybersecurity. In particular, North Korea has launched frequent major cyber attacks against both government offices and corporations in ROK. And precisely because Korea is highly dependent on ICT, the resulting damage has amounted to billions of dollars as well as widespread disruption of key services. Microsoft estimates that Korea's economic loss from cyber threats amounted to $72 billion in 2017 alone.[35] And the damage to Korea's economy caused by a distributed denial-of-service (DDoS) attack in 2009 and the March 20 and June 25 cyber terrorism attacks in 2013 was estimated to $746 million.[36]

Korea has experienced cyber attacks continuously since 2009, including DDoS attacks and cyber terrorism (see table 3). Most of these cyber attacks are presumed to originate in North Korea, but that is not always the case. For example, in the case of the 2018 PyeongChang Olympics cyber attack, Russia was suspected of retaliating for its punishment by the International Olympic Committee for a national doping scandal. After experiencing such cyber incidents, the Korean government established new policies and countermeasures to identify problems, improve response time, and reduce the damage these attacks cause.

Table 3. Major Cyber Incidents in Korea

Year	Incidents
2009 July 7 DDoS attack	Three distributed denial-of-service attacks from July 7 to July 10 paralyzed major government websites, including that of the Office of the President.
2011 March 4 DDoS attack	DDoS attacks on forty local websites, including those of major portals, government offices, the Ministry of National Defense, and financial institutions.
2011 NH Bank incident	NH Bank's internal data and server system were damaged. Service access was paralyzed entirely or partially.
2013 March 20 cyber terror	Major local broadcasters and six financial institutions' information technology systems went down due to destructive malware.
2013 June 25 cyber terror	The Office of the President website, major government websites, media, and political parties' websites were under cyber attack.
2014 KHNP incident	Korea Hydro and Nuclear Power was blackmailed by the so-called Group Against Nuclear Power Plants. The blackmailers threatened that, if KHNP power plants were not stopped, the group would destroy them.
2018 PyeongChang Winter Olympics incident	On the day of the opening ceremony, hundreds of International Olympic Committee computers were hacked, causing connection failures on its websites.

Korea has also experienced several major, personal data breaches in the private sector. After the Auction incident in 2008, when millions of users' personal data records, including real names and encrypted Resident Registration Numbers (RRNs), were revealed by a security breach,[37] efforts to improve protection of personal data and reduce the damage caused by data breaches became a major focus of public and regulatory attention. Since then, Korea has experienced many large-scale incidents, such as breaches of SK Communications in 2011, of major credit card companies in 2014, and of Interpark in 2016. One response was the Personal Information Protection Act, which became a general law in 2012, prohibiting the collection of RRNs online and strengthening the right to self-determination of personal information.

Online Identification

The system of online identification in Korea has centered, in the first instance, around a range of government initiatives.

Resident Registration Number

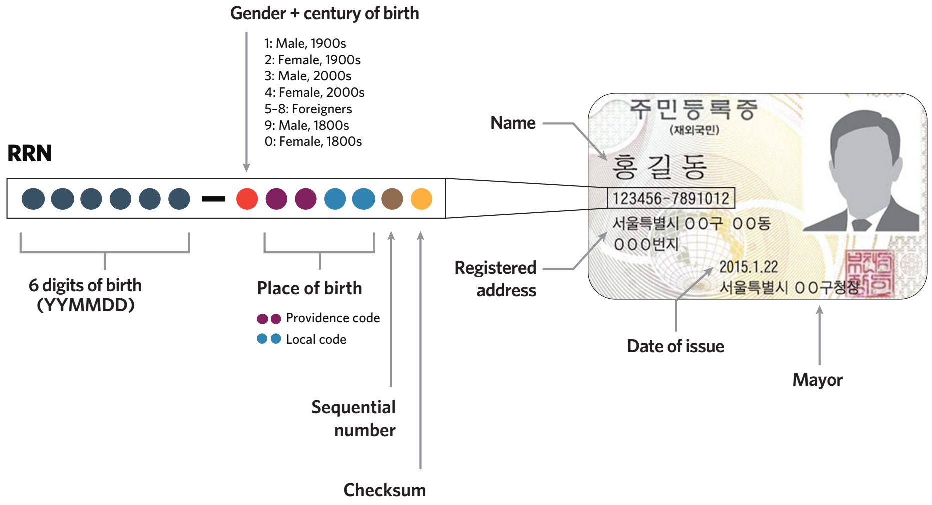
Korea's identification online was centered on the RRN until the mid-2000s. The RRN is a unique lifelong identification number given to all Koreans at birth, much like the Social Security number in the United States and is used for a wide range of government and private-sector purposes. The Korean RRN and Resident Registration Card (RRC), a nationally recognized identification card that includes the RRN, were established by the enactment of the Resident Registration Act in 1962 (see table 4).

Table 4. The Enactment and Major Revisions of Korea's Resident Registration Act

Date	Law No.	Outline
May 1962	(Enactment) Law No. 1067	• Enactment of Resident Registration Act • Municipality certificate system
May 1968	(Revised) Law No. 2016	• Introduction of the twelve-digit Resident Registration Number (RRN) system • Issuance of Resident Registration Cards (RRCs) for those over eighteen years old
January 1970	(Revised) Law No. 2150	• Issuance of an RRC became mandatory
July 1975	(Revised) Law No. 2777	• Revised to provide for a thirteen-digit RRN system • Mandatory issuance of an RRC for those over seventeen years old • Renewal of all existing RRCs
January 2001	(Revised) Law No. 6385	• Prescribe the basis of issuing RRN in the law • Establish a system to manage and access resident registration information online
May 2016	(Revised) Law No. 14191	• Permission to change the RRN of a person affected by personal information leaks, identity exposure, and so on

This act was amended in 1968 to establish a twelve-digit Personal Identification Number (PIN) system, the predecessor of the RRN system. In addition, an RRC was issued to citizens over the age of eighteen. Later, in 1975, this obligation was changed to seventeen years of age, converted to the RRN's current thirteen-digit number system, and the RRC was updated (see figure 1). The RRC has been maintained until now after the second renewal in 1983 and the third renewal in 1999.

Figure 1. Resident Registration Number and Resident Registration Card of Korea



Source: Lim Jong-in et al., *A Study on the Technical Improvement Plan of the Resident Registration Number-Based Authentication for Personal Information Protection* (Korea Local Information Research & Development Institute, 2014).

Because the RRN is a unique identification number assigned to each citizen of Korea, it was widely used for identification online in the early 2000s. Private websites that are not legally mandated to collect and verify the RRN also requested the RRN when individuals signed up. They could not verify the legitimacy of the RRN, but they performed verification using the RRN checksum algorithm. Moreover, most of them used the RRN as the key value for identification for their website database.[38]

After 2004, as the internet was expanding, the problem of excessive collection of RRNs and the theft of personal data increased. A survey conducted by the country's top certification body, the Korea Internet and Security Agency (KISA), in 2003 found that out of 448 websites, 447 had requested the collection of RRNs.[39] This was done to discourage illegal activities, but RRN data was excessive, making them vulnerable to theft and abuse. The National Public Key Infrastructure-based Authorized Certificate was launched in 2004 as a way to enable substitutes for the RRN identification (for example, the I-PIN) and began to be discussed as a way to limit the collection of the RRNs online.

After the 2008 Auction personal data leak, several provisions related to personal information were revised in the Act on Promotion of Information and Communications Network Utilization and Information Protection, and associated legislation. In Article 23-2 of this amendment to the act, a new provision was adopted that obliges Korea's online service providers with more than a specified number of page views to introduce a means of replacing the RRN.

In August 2012, the collection of the RRNs online was prohibited outright, and in August 2014, the so-called RRN collection legalism was introduced to prohibit collections of RRNs except where specific laws require them to be collected, such as for e-government services, financial transactions, contract signings, and medical information verification.

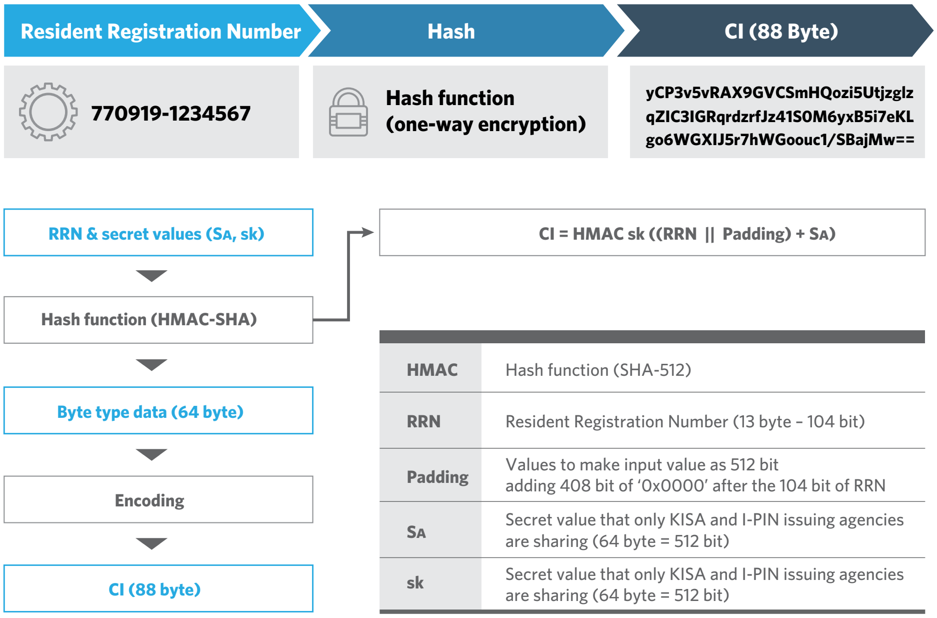
With the introduction of the RRN collection legalism and the implementation of alternative identification measures, there was a demand for changes in the RRN system itself. Discussions emerged around how to solve chronic problems with the current RRN system, such as the possibility of exposure of personal information and the fact that it is impossible to change a permanent identity number that is meant to be used throughout a citizen's lifespan. Ultimately, the RRN system was revised to allow for the reissue of a new RRN in cases of possible exposure of personal data and to protect victims of domestic violence and sexual violence. Thus, the RRN, in thirteen-digit form, was revised in 1975 and has been maintained to this day, but it is used today as a means of identification online only in limited circumstances.

I-PIN

Due to the risk of data breaches and the reckless collection and use of RRN data, the Korean government established and distributed an Internet Personal Identification Number (I-PIN) system as an alternative means of identification. The I-PIN is an alternative means to identify individuals on the internet. Credit bureau companies such as the Korea Credit Bureau, National Information and Credit Evaluation, and SCI Information Service were designated by the government in October 2006 as official I-PIN issuing entities. When identification is requested at a specific site, the result is delivered by verification using the information they have, including the RRN.

In June 2010, the Korean government introduced the I-PIN 2.0, which added functions such as connecting information (CI), a connection value of different services, and duplicated joining verification information (DI), to prevent duplicate subscription. The core of the I-PIN 2.0 system is the CI that creates a unique universal key value for online identification, which replaces the RRN for a specific individual. The CI is a unique value that corresponds directly with the RRN. It is made into 88-byte through a SHA-512 hash function of the RRN and several paddings and key values that are shared by the KISA and I-PIN issuing entities (see figure 2). The CI is used not only for the I-PIN but also for the public identification services established later in 2012. And the DI is a 64-byte number generated from the RRN and the information of the internet service provider (ISP), providing a unique value linked to each ISP.

Figure 2. The Process of Issuing Connecting Information in Korea


Resident Registration Number
Hash
CI (88 Byte)
770919-1234567
Hash function
(one-way encryption)
yCP3v5vRAX9GVCSmHQozi5Utjzglz
qZIC3IGRqrdzrfJz41S0M6yxB5i7eKL
go6WGXIJ5r7hWGoouc1/SBajMw==
RRN & secret values (SA, sk)
Hash function (HMAC-SHA)
Byte type data (64 byte)
Encoding
CI (88 byte)
CI = HMAC sk ((RRN || Padding) + SA)

HMAC	Hash function (SHA-512)
RRN	Resident Registration Number (13 byte – 104 bit)
Padding	Values to make input value as 512 bit adding 408 bit of ‘0x0000’ after the 104 bit of RRN
SA	Secret value that only KISA and I-PIN issuing agencies are sharing (64 byte = 512 bit)
sk	Secret value that only KISA and I-PIN issuing agencies are sharing (64 byte = 512 bit)

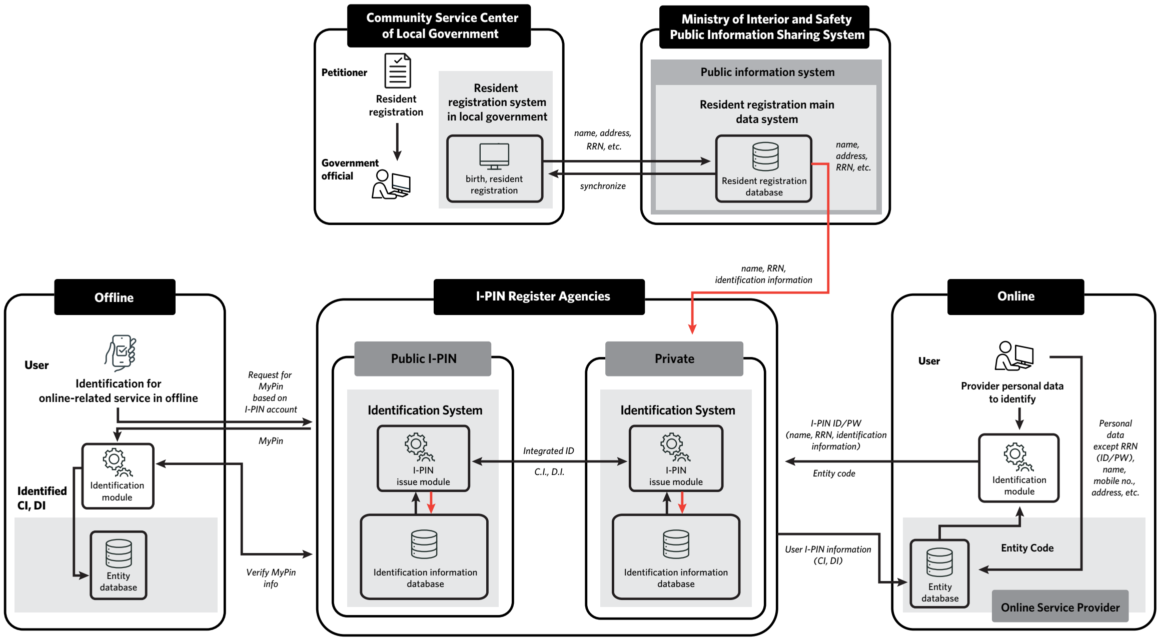
Source: Korea Internet and Security Agency, “Information on Opinion Gathering Meeting on CI (Connecting Information)” (in Korean), July 17, 2019, https://www.kisa.or.kr/notice/notice_View.jsp?mode=view&p_No=4&b_No=4&d_No=2441&ST=total&SV=.

With the implementation of the RRN collection legalism, the demand for I-PINs that can replace it also increased. In addition, MyPin, formed with a thirteen-digit random number derived from the I-PIN (see figure 3), was introduced in the case that identity verification and linkage are required offline.

However, because the I-PIN adopted ID/password-based authentication, it required additional forced security measures, such as CAPTCHA and installation of ActiveX to prevent keylogging. These complementary security measures caused great inconvenience. Despite these security measures, in early 2015, a public I-PIN operated by the Korea Local Information Development Institute was hacked, resulting in 750,000 fraudulent issuances.[40] In response to this, in May 2015, all existing I-PINs were reissued, and an expiration date was introduced so that each I-PIN must be renewed every year. Also, it was changed to require an additional authentication measure such as a secondary password, key pattern, and biometric authentication.

These additional security measures made it more inconvenient to use I-PIN compared to private identification services, slowing adoption of I-PIN. According to a survey by the Ministry of Science and ICT and the Korea Internet Promotion Agency, 37.7 percent of websites (2,783 of 7,371 websites surveyed) that provided I-PIN based identification reported that no website visitor had used it in over a year.[41] This reduction in the use of I-PIN led to the government’s decision to abolish the I-PIN system.

Figure 3. The Architecture of I-PIN and MyPin


Community Service Center of Local Government
Petitioner
Resident registration
Government official
Resident registration system in local government
birth, resident registration
name, address, RRN, etc.
synchronize
Ministry of Interior and Safety Public Information Sharing System
Public information system
Resident registration main data system
Resident registration database
name, address, RRN, etc.
name, RRN, identification information
Offline
User
Identification for online-related service in offline
Identification module
Identified CI, DI
Entity database
Request for MyPin based on I-PIN account
MyPin
Verify MyPin info
I-PIN Register Agencies
Public I-PIN
Private
Identification System
I-PIN issue module
Identification information database
Integrated ID
C.I., D.I.
I-PIN ID/PW (name, RRN, identification information)
Entity code
User I-PIN information (CI, DI)
Online
User
Provider personal data to identify
Identification module
Personal data except RRN (ID/PW), name, mobile no., address, etc.
Entity Code
Entity database
Online Service Provider

Source: Lim Jong-in et al., *A Study on the Technical Improvement Plan of the Resident Registration Number-Based Authentication for Personal Information Protection* (Korea Local Information Research & Development Institute, 2014).

New issuances and renewals were stopped in October 2018, and a decision was made to terminate the program in 2021 when the last public I-PINs, which were valid for three years, will expire.[42]

Private Identification Services

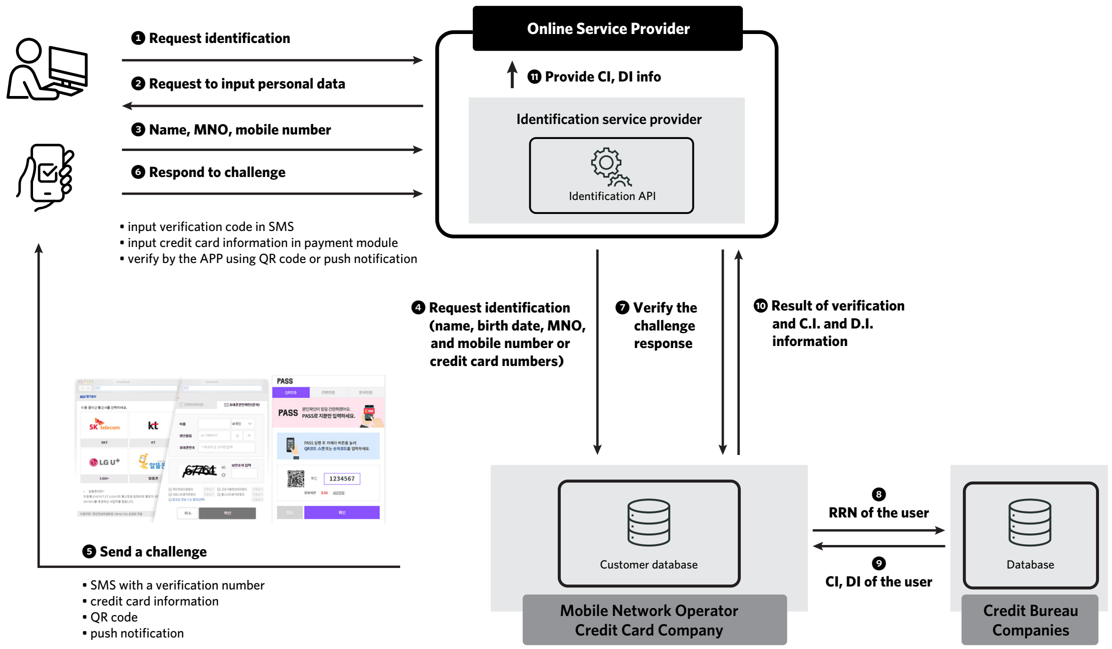
Since August 2012, online identification through the RRN has been prohibited in Korea, and the I-PIN and the NPKI were not widely used, so the government considered other alternative means that can be used easily and inexpensively. In August 2012, the government established rules for identity verification agencies, and in December 2012, the Korea Communications Commission (KCC) determined that three mobile network operators (MNOs) could be designated as identity verification agencies in the private sector.[43] Identity verification by the MNOs was initially conducted in the form of a challenge and response through text messages.

The online service provider (OSP) handles the user's request for identity verification through the verification agencies designated by the MNOs. The agency transmits a challenge to the user's mobile phone using the personal information stored by the MNO, and the user sends a response to the verification entity. The verification entity provides the personal information of the identity verification requester and the CI and DI that were provided by the credit bureau companies to the OSP to verify the identity. As the use of smartphones spread, app-based authentication methods, such as QR code and biometric authentication, were added.

At the end of 2017, the Korea Communications Commission designated seven major credit card companies as new identity verification agencies, and they started their identification operations in April 2018.[44] These credit card companies, like MNOs, are allowed to collect and retain personal data, including RRNs. They offer identification in three forms: mobile card application payment, automated response system authentication, and verification through card company website access, providing personal information, CI, and DI to the OSP (see figure 4). These credit card companies are reliable and secure entities, so they could be expanded as identity verification agencies.

Such private identification services will be expanded further when the I-PIN expires. In March 2021, major OSPs, such as Naver, Kakao, and the fintech company Toss, applied for status as identity verification agencies but were rejected by the KCC due to concerns about account and identity theft.

Figure 4. The Architecture of Private Identification Service in Korea



❶ Request identification
❷ Request to input personal data
❸ Name, MNO, mobile number
❻ Respond to challenge
• input verification code in SMS
• input credit card information in payment module
• verify by the APP using QR code or push notification
Online Service Provider
⓫ Provide CI, DI info
Identification service provider
Identification API
❹ Request identification (name, birth date, MNO, and mobile number or credit card numbers)
❼ Verify the challenge response
❿ Result of verification and C.I. and D.I. information
❺ Send a challenge
• SMS with a verification number
• credit card information
• QR code
• push notification
Customer database
Mobile Network Operator
Credit Card Company
❽ RRN of the user
❾ CI, DI of the user
Database
Credit Bureau Companies
SK telecom
kt
LG U+
PASS
1234567

Source: Ministry of the Interior and Safety, “Introduction to Public Website Authentication Methods” (in Korean), 2018, https://www.mois.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_00080432Bs0st7I&fileSn=0.

Identity Verification of Users of Online Message Boards

Since 2003, Korean society has discussed the introduction of an internet real-name system to address many problems with internet and online services, and in 2004, an amendment to the Public Official Election Act included a provision for real-name verification for internet media sites to prevent false slander during the election process. As the use of the internet expanded, the former Ministry of Information and Communication (MIC), the agency in charge, worried about how the anonymity of internet users could facilitate defamation, fraud, and doxing—all of which were already happening in Korea, in sometimes highly publicized cases.

In January 2007, the government of Korea proposed an amendment to the ICT and Security Act, which included the so-called limited identity verification provision, which required users of some large online services to verify their real names. Despite some opposition from civic groups and the public, this amendment eventually was enacted by the National Assembly, resulting in the launch of an internet real-name system in Korea in July 2007.

Article 44-5 of ICT and Security Act stipulated that the entity operating an open message board should take measures to verify users' identities on boards that have a large impact on Korean society. Initially, according to Article 30 of the ICT and Security Act, online service providers such as portal sites and user-generated content service providers with more than 300,000 page views per day and internet media sites exceeding 200,000 page views per day were targeted.[45] Later in January 2009, this regulation was revised, and the target was expanded to all websites exceeding 100,000 daily page views (see table 5).[46]

Table 5. Websites and Internet Service Providers Regulated by the Mandatory Identity Verification Rules

Year	Covered websites (ISPs)	Criteria specified in laws and enforcement decree
2007	35 (22)	Portal sites and user-generated content service providers with more than 300,000 page views per day and internet media sites exceeding 200,000 page views per day
2008	37 (33)	
2009	153 (138)	All websites and ISPs exceeding 100,000 page views per day
2010	167 (157)	
2011	146 (133)	
2012	131 (123)	

Source: Korea Internet & Security Agency.[47]

After the implementation of the limited identity verification rules, malicious content was reduced on internet bulletin boards as well as comment and reply sections, but the effect was not large. According to the results of a 2007 survey led by the MIC and the KISA, the proportion of malicious comments on these boards decreased from 15.8 percent to 13.9 percent.[48] In addition, according to a 2010 study by Woo, a professor at Seoul National University, who compared the ten-day periods before and after the implementation of the limited identity verification rules on July 27, 2007, found that slanderous posts decreased slightly from 13.9 percent to 12.2 percent. However, the number of internet protocol addresses significantly decreased from 2,585 to 737 during the same time.[49] This suggests that although the regulation had no significant effect on the type of comments posted, it adversely impacted internet participation.

In addition, some overseas service providers refused to abide by the new regulations. In 2009, the YouTube website in Korea recorded more than 100,000 average page views per day and became the target of the identity verification rule. In response, Google, which runs YouTube, decided to bypass the regulation by restricting YouTube video uploads in Korea and closing the comment feature.[50] As a result, Korean users had to change their country settings to use YouTube sites of other countries. Since then, the Korea Communications Commission, which oversaw the identity verification system, decided to exempt overseas websites.[51] This decision, however, led to complaints of reverse discrimination against domestic sites.

In August 2012, the Constitutional Court of Korea unanimously ruled that the internet real-name system was unconstitutional in a ruling on a lawsuit filed by internet media companies, civic groups, and some users.[52] The court ruled that it was not in the public interest to limit freedom of expression, particularly considering that illegal postings did not decrease significantly after the implementation of the internet real-name system. The court also noted adverse side effects, such as users fleeing to overseas sites and reverse discrimination against domestic companies. As a result of this court decision, the limited identity verification was abolished in Korea.

In addition, in January 2021, the Constitutional Court ruled as unconstitutional the provision for real-name verification on internet media sites, which had been enacted to prevent false slander during elections since 2004, under Article 82-6 of the Public Official Election Act. Accordingly, the regulations on websites related to the two major internet real-name systems in Korea have been abolished. As a result, the game shutdown law, which restricts teenagers from accessing online games from midnight to 6 a.m., is the only law in Korea related to the online real-name system.[53]

Authentication Online

National Public Key Infrastructure-Based Authorized Certificate (NPKI-based AC)

In the late 1990s, with the progress of information technology, it became necessary to prepare an infrastructure to implement social activities in traditional social activities in non-face-to-face electronic environments for e-commerce, e-government, and similar services. These activities included financial transactions, contracts, and identity verification online. In response to this need, internationally, the

Working Group on Electronic Commerce of the United Nations Commission on International Trade Law conducted standardization studies related to online authentication.

This was both timely and useful because high-speed communication network technologies such as ISDN and ADSL quickly spread through Korea during the late 1990s, and policymakers recognized the necessity of creating a foundation for e-commerce and other services, which were growing very rapidly. Annual growth of e-commerce-based transactions was 400 percent from 1997 to 1999.[54]

To meet this growing need, Korea enacted an array of laws, such as the Electronic Signature Act and the Basic Act on Electronic Transactions, promulgated as Act Nos. 5792 and 5834, respectively, in February 1999 and taking effect in July 1999. Subsequent legislation included the Act on Promotion of Electronic Administration for E-Government Realization of 2001 (E-Government Act), ensuring the legal status of electronic signatures, seals, and stamps. Under this provision, an authentication function is provided for electronic signatures to assess the authenticity of documents and electronic transactions.

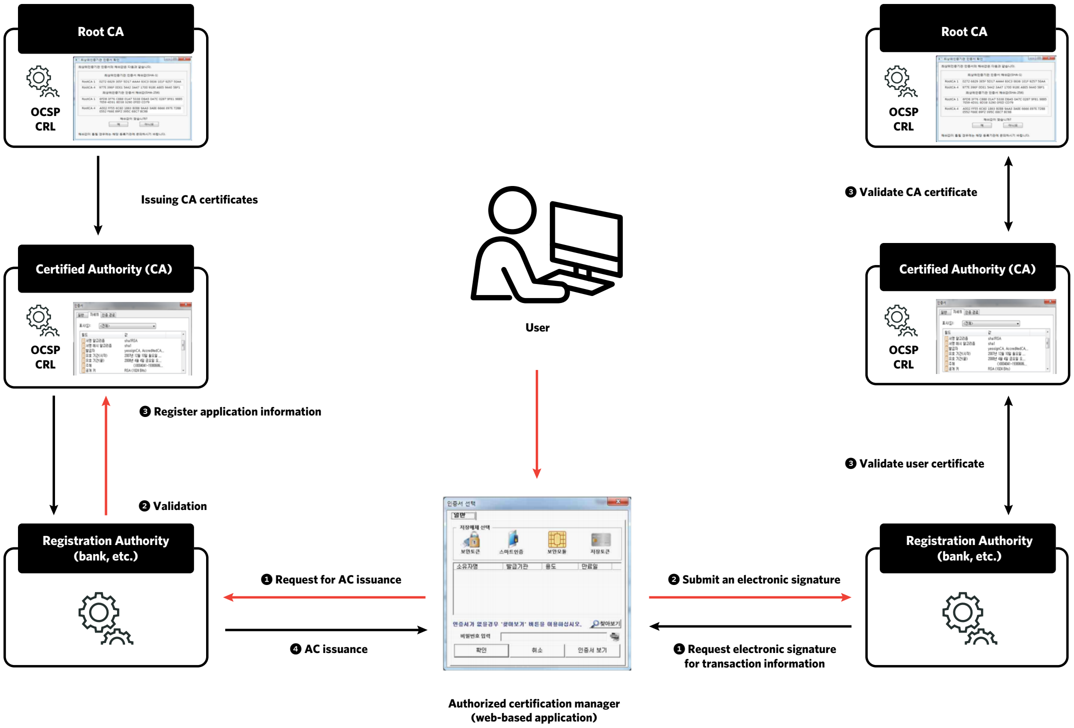
The institutional basis for digital signatures was established in Korea in 2001, and the NPKI-based AC system has been implemented in earnest since then. Architectures, technical specifications, and so on had already been discussed in 1999, focused on the government and financial sectors separately and were integrated into the current NPKI system in 2001.

Public key infrastructure (PKI) is a technology used for digital certificate implementation or public key encryption in an online environment. In ITU-T, the PKI standard is specified in the X.509 standard and is used for secure sockets layer encryption or the implementation of electronic certificates. PKI is a widely used technology, but Korea built a PKI at the national level to provide a robust authentication technique that could be used in a wide range of situations. It is characterized by mandatory use in electronic financial transactions and e-government-related activities.

Korea's NPKI system issued certificates through the KISA and five private organizations designated as certificate authorities (CAs).[55] In the issuing process, when a user requests certificate issuance to a registration authority (RA), such as a bank that generally performs certificate issuance, the RA makes a request to the CA for validation and certification issuance. The CA verifies whether the user is legitimate based on the personal information it holds. Based on the certificate granted by the root CA to the CA, the user's authorized certificate is issued by the CA and delivered to the user through the RA. The verification and signing process is undertaken in reverse order. When the OSP requests the user to sign through the RA, the user signs the certificate with a private key and sends it. The RA verifies it by the CA, and the CA verifies it by the root CA (see figure 5).

When the NPKI-based AC is issued, it is saved as files such as signCert.der and SignPri.key in the NPKI folder on the user's computer. If a site requires an AC, a certificate in the form of these files is loaded through the AC Manager, and authentication is performed through a signature act in which the user inputs a private key. In addition, since the certificate is managed in the form of files, it can be copied and used on other computers or smartphones.

Figure 5. The Architecture of NPKI-Based AC



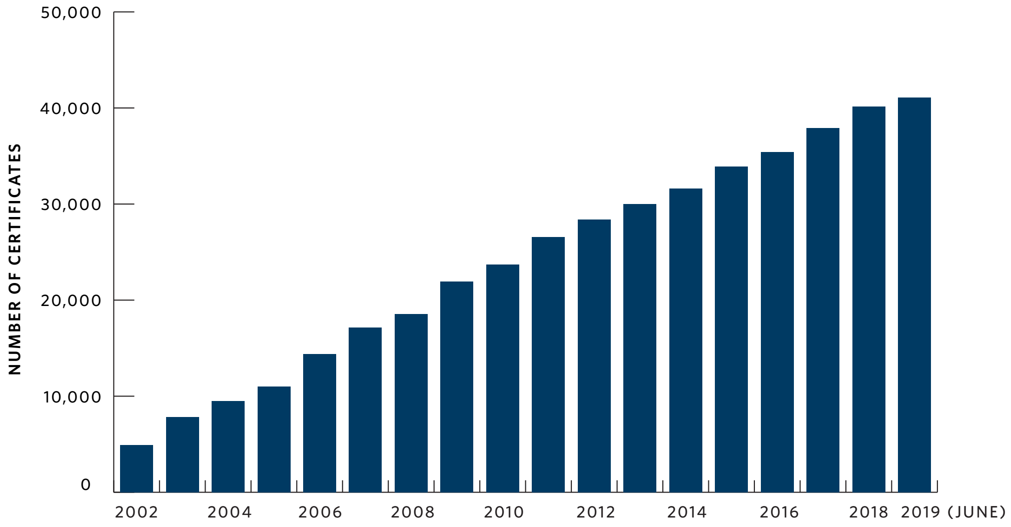
Source: Korea Internet and Security Agency, “Authorized Certificate SW” (in Korean), http://www.rootca.or.kr/kor/accredited/accredited06_01.jsp.

Here, the Korean model provides a lesson for other countries because its authorized certificate system may have several advantages as a national-level infrastructure, and is mandated for use in online transactions, such as online banking, payments over 300,000 Korean won (about $265), and e-government-related services.[56] In addition, the AC is widely used as a means of online identification. Thus, by 2010, the AC had come to dominate the online authentication market (see figure 6), and other types of certificates were rarely used in Korea. Still, some problems cropped up that those who seek to emulate Korea’s example can learn from.

Specifically, the idea of establishing an NPKI system and the AC may have several advantages, and there were no issues with designing the architecture and technical specifications. However, in implementing and developing an actual system for specific online applications, several security vulnerabilities or useability problems emerged.

The essence of this problem is that the implementation relied on ActiveX, a plug-in for Internet Explorer (IE) provided by Microsoft. The NPKI system itself is technology neutral, but it was implemented by security companies using ActiveX, which works only in Windows and IE environments. In the early

Figure 6. Amount of NPKI-Based AC Issuance



Source: Korea Internet and Security Agency and Hu-Seop Lee, "The Monopoly of Authorized Certificates Disappeared in 21 Years…Civil Service With Simple Passwords" (in Korean), Edaily, May 19, 2020, https://m.edaily.co.kr/news/Read?newsId=03857286625770560&mediaCodeNo=257.

stages of NPKI, Korea's standard encryption algorithm called SEED was used, and most Korean users at that time used Windows and IE environments. To improve ease of use, the encryption algorithm was changed to one based on AES, but ActiveX continued to be used.

The first problem with this is the dependence on a specific computing environment. In many other operating systems or web browser environments, where ActiveX did not work, AC was impossible to use. This issue became even worse with the advent of the smartphone environment and Microsoft's decision to remove ActiveX from its browsers in 2015.

The second problem is the security problem of ActiveX itself. To implement ActiveX requires that the certificate authority be granted operating system administrator privileges. This makes it easy to install capabilities, including a keylogging prevention tool, which can be implemented only with ActiveX and was widely adopted and used in Korea. However, this meant that many people at the CAs and solution providers had access to internal computer files, resulting in many security vulnerabilities.

Due to growing antipathy against the NPKI-based AC, in March 2014, then president Park Geun-hye proposed abolishing the mandatory use of AC for payments. Afterward, mandatory AC use for payments over 300,000 Korean won was abolished, and the mandatory provisions for AC in internet banking were also abolished in March 2015. Nevertheless, the NPKI-based AC and the ActiveX-based security measures were used continuously given path dependence and legacy software.

In 2017, presidential candidate Moon Jae-in proposed abolishing NPKI-based AC as part of the ICT pledge, and the majority of the public and relevant civic groups supported the proposal.[57] After Moon took office in May 2017, his government promoted the withdrawal of AC, which led to a complete amendment to the Electronic Signature Act, abolishing the mandate for use of the NPKI-based AC.

Mixed Online Certification Environment

In its place, in December 2020, the government adopted a joint certificate environment, enabling various authentication means to be used together (see table 6).

Table 6. Online Certifications in Korea as of March 2021

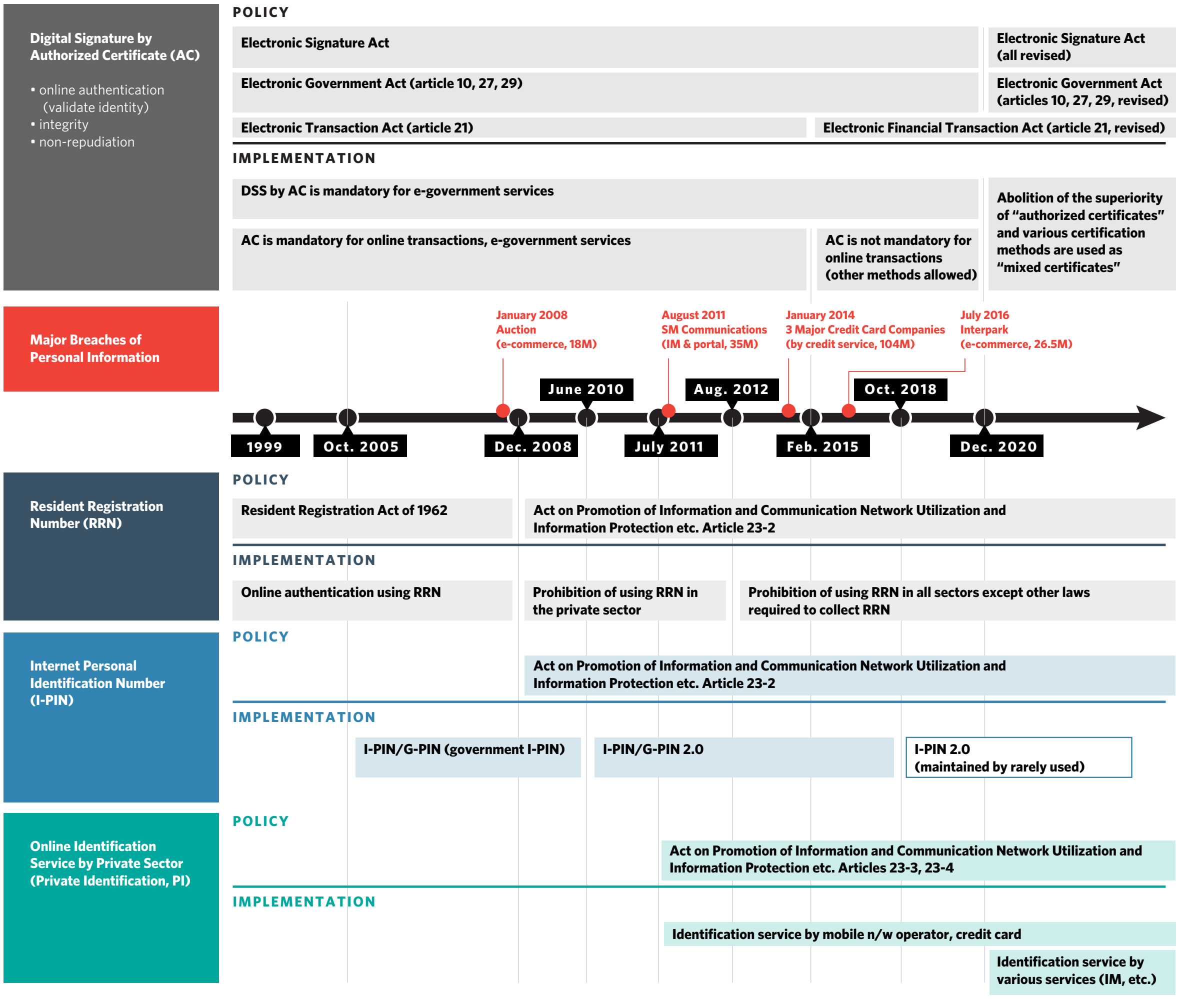
Sector	Certificate	Issuance	Characteristics
Government	Joint certificate	Korea Financial Telecommunications and Clearings Institute, Koscom Corporation	Used in the same way as existing National Public Key Infrastructure-based Authorized Certificate (NPKI-based AC)
Finance	Finance certificate Service	Korea Financial Telecommunications and Clearings Institute	Available from twenty-two banks and credit card services
	KB mobile	KB Bank	Available for each financial service through each bank's app
	NH OnePass	NH Bank	
	Hana 1Q Mobile	Hana Bank	
ICT	Pass	Mobile network operators	Certificates are issued by individual service apps and can be used in related services

Source: Financial Services Commission of Korea.[58]

The joint certificate enables secure communications and is also used in identity verification services and provides personal information, such as CI, DI, and birth date, after verification. Although the joint certificates are no longer the sole means of government-endorsed authentication, cases exist in many high-level authentication environments where it is still the only authentication method in use, for example, certificate issuances, such as registration and social insurance verification. Even the private sector still requires the joint certificate, and it is requested often, such as for self-certification of online education.

Financial institutions jointly issued a financial certificate, a cloud-based certificate authenticated with six digits or biometric authentication in device level, which is valid for a three-year period and has an automatic renewal function. In addition, major banks provide their own certificates. Various private individual certifications have also been released, used, and adopted in many services, including e-government services. The MNOs' Pass service was used as an existing identity verification. Moreover, Kakao and Naver (representative OSPs in Korea) and Payco and Toss (fintech companies) also provide authentication services.

Figure 7. Online Authentication Policies and Implementation in Korea


Digital Signature by Authorized Certificate (AC)
• online authentication (validate identity)
• integrity
• non-repudiation
POLICY
Electronic Signature Act
Electronic Signature Act (all revised)
Electronic Government Act (article 10, 27, 29)
Electronic Government Act (articles 10, 27, 29, revised)
Electronic Transaction Act (article 21)
Electronic Financial Transaction Act (article 21, revised)
IMPLEMENTATION
DSS by AC is mandatory for e-government services
Abolition of the superiority of "authorized certificates" and various certification methods are used as "mixed certificates"
AC is mandatory for online transactions, e-government services
AC is not mandatory for online transactions (other methods allowed)
Major Breaches of Personal Information
January 2008 Auction (e-commerce, 18M)
August 2011 SM Communications (IM & portal, 35M)
January 2014 3 Major Credit Card Companies (by credit service, 104M)
July 2016 Interpark (e-commerce, 26.5M)
June 2010
Aug. 2012
Oct. 2018
1999
Oct. 2005
Dec. 2008
July 2011
Feb. 2015
Dec. 2020
Resident Registration Number (RRN)
POLICY
Resident Registration Act of 1962
Act on Promotion of Information and Communication Network Utilization and Information Protection etc. Article 23-2
IMPLEMENTATION
Online authentication using RRN
Prohibition of using RRN in the private sector
Prohibition of using RRN in all sectors except other laws required to collect RRN
Internet Personal Identification Number (I-PIN)
POLICY
Act on Promotion of Information and Communication Network Utilization and Information Protection etc. Article 23-2
IMPLEMENTATION
I-PIN/G-PIN (government I-PIN)
I-PIN/G-PIN 2.0
I-PIN 2.0 (maintained by rarely used)
Online Identification Service by Private Sector (Private Identification, PI)
POLICY
Act on Promotion of Information and Communication Network Utilization and Information Protection etc. Articles 23-3, 23-4
IMPLEMENTATION
Identification service by mobile n/w operator, credit card
Identification service by various services (IM, etc.)

Source: Authors' research.

Data Access Control

Korea has also pioneered several methods of access control for public databases under an architecture of open government data policies.

Increasing the accessibility of public data can be advantageous, not least by meeting right-to-know requirements, enabling better analysis, and fostering new services that lead to job creation and add value to the economy. But as Korea, like many countries, has discovered, excessive public information disclosure can have several adverse effects. These include the infringement of rights (such as privacy), fraud, and unfair and deceptive sales techniques. As a robust democracy with extensive platforms for citizen engagement, Korea has had to address such issues as data management, access-related systems, and guaranteeing the availability of data and services when the government put the regulations and policies in place.

Public Data

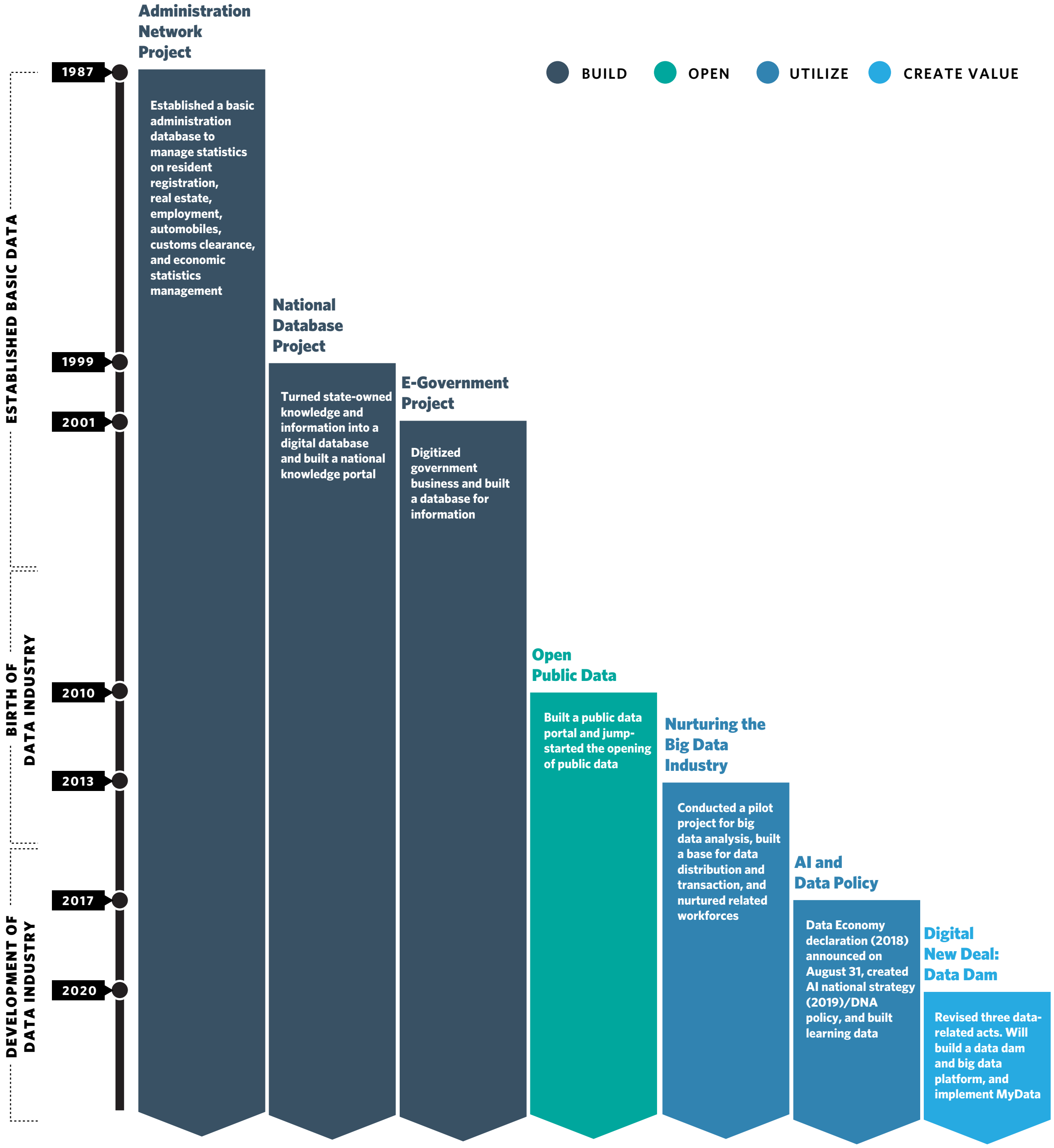
In the past, public data in Korea was processed and managed by the government, which guaranteed the public's right to know through information disclosure requests. In 1996, the Act on the Disclosure of Information by Public Organizations was enacted to stipulate the rights and forms of public requests for disclosure of information held by public institutions and stipulated matters necessary for the disclosure obligations of public institutions. This act has aimed to ensure the public's right to know, citizen participation in national affairs, and government transparency.

Requests for disclosure of information in public institutions were processed by the National Archives of Records starting in 2004, and requests for disclosure of information have increased every year, showing steady growth from 104,024 in 2004 to 756,342 in 2016.[59] On average, the information disclosure acceptance rate is maintained at around 95 percent every year.[60] However, there are criticisms that this figure is overinflated, since the government agencies often partially disclose information excluding crucial data for reasons such as invasions of privacy or damage to public interests.[61]

The paradigm of public information also changed dramatically due to the introduction of smartphones in 2010 and the flood of data and new apps that resulted. Restrictions on public information became a problem due to the increase of applications accessing information on a smartphone. For instance, a simple bus location app required real-time government data. To cope with issues like these, Korea established a plan to promote the private use of public information in 2010. In 2011, guidelines for the provision of public information and public data portal services were established, which led to the Government 3.0 Basic Plan and the Act on Providing and Utilizing Public Data in 2013.[62]

In 2016, the government established the E-Government 2020 Basic Plan, as well as five strategies to reflect the social demands due to the advent of a hyperconnected society.[63] Better access to public data was enabled by increased funding for government IT systems and a shift to cloud-based administrative information infrastructure. In February 2021, the government established the Data 119 Project and announced a data strategy to revitalize the digital economy by promoting open data utilization.[64] The strategy called for amending and updating the so-called three data laws' amendments and launching nine new data services and outlined eleven action tasks, including the establishment of a special data committee. The three data laws' amendments refers to amendments to the Personal Information Protection Act, the ICT and Security Act, and the Credit Information Protection Act. These laws were promoted to meet the needs of industry, by introducing the concept of pseudonymous information and helping certify adequacy with the European Union's General Data Protection Regulation (EU GDPR).

Figure 8. Paradigm of Public Data in Korea



Administration Network Project

Established a basic administration database to manage statistics on resident registration, real estate, employment, automobiles, customs clearance, and economic statistics management

National Database Project

Turned state-owned knowledge and information into a digital database and built a national knowledge portal

E-Government Project

Digitized government business and built a database for information

Open Public Data

Built a public data portal and jump-started the opening of public data

Nurturing the Big Data Industry

Conducted a pilot project for big data analysis, built a base for data distribution and transaction, and nurtured related workforces

AI and Data Policy

Data Economy declaration (2018) announced on August 31, created AI national strategy (2019)/DNA policy, and built learning data

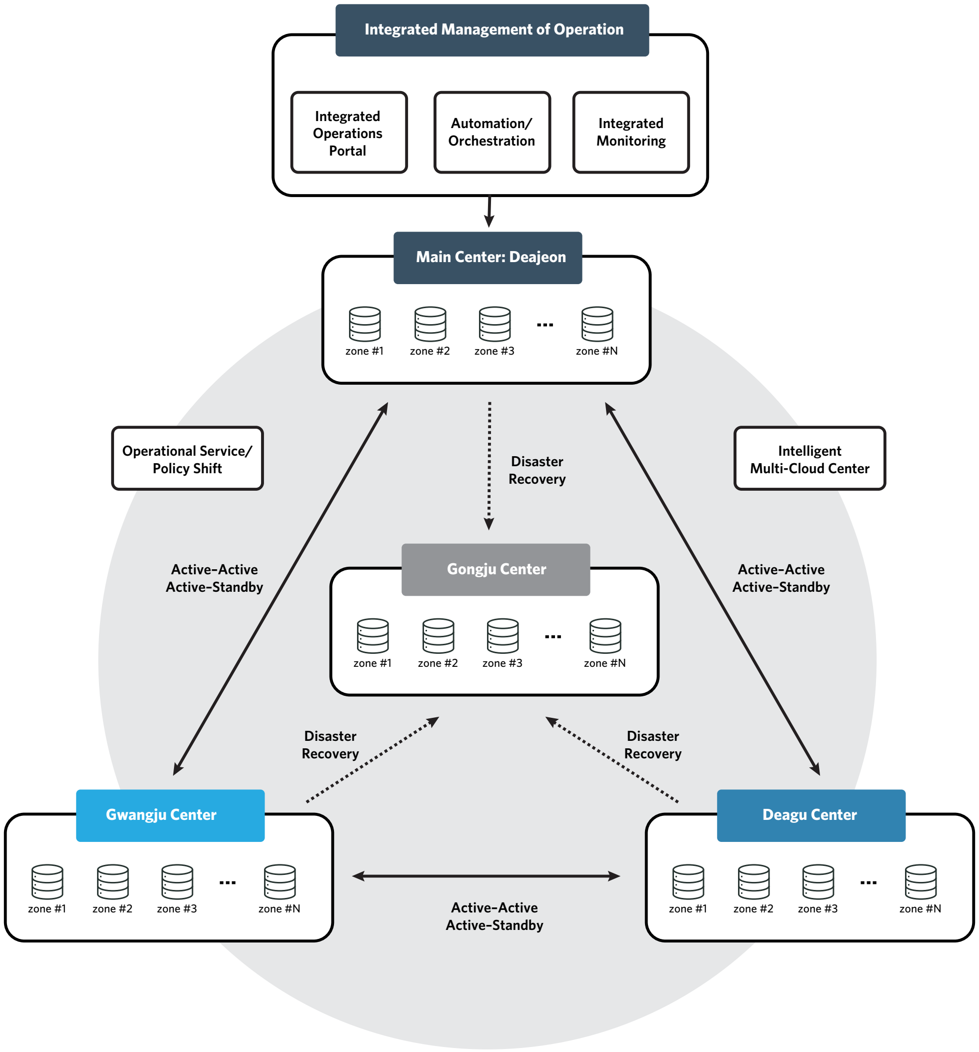
Digital New Deal: Data Dam

Revised three data-related acts. Will build a data dam and big data platform, and implement MyData

Source: Korea Data 119 Project, "Presidential Committee on the Fourth Industrial Revolution of Korea," 2021.

To implement public data access control, meanwhile, the government has pursued various lines of effort, such as establishing a management system, managing accessibility, and securing availability. In 2002, the E-Government Special Committee was established to research policies and implementation to establish e-government services. An Innovation Plan for Efficient Operation of the Pan-Government Computer Environment was later selected as one of the thirty-one tasks in the E-Government Roadmap in 2003. In 2004, a plan for establishing and promoting an integrated computing environment-related ISP project was prepared. In 2005, the Government Integrated Computing Center was established in Daejeon under the Ministry of Information and Communication (MIC). The Government Integrated Computing Center was renamed the National Information Resource Management Service in 2017 and is currently in operation. Since 2007, the Gwangju Center has been the core of this architecture, and a Gongju Center for backup and Daegu Center for Cloud have been under construction since 2019 (see figure 9).

Figure 9. Architecture of the Government Integrated Computing Center



Source: National Information Resource Service of Korea.

Private Data

The most complex issue regarding data access in the private sector is the use of personal information, and Korea has had to find and adopt a pathway that reflects its national conditions. Today, Korea's personal data-related regulations are like EU-style regulations emphasizing protection in the form of detailed provisions limiting the collection and unauthorized use of personally identifiable information.

But in the early days of its ICT development, Korea did not have regulations related to personal information protection at all. It addressed the problem in earnest only in 2001 by revising the ICT Promotion Act, which is now called the Act on Promotion of Information and Communications Network Utilization and Information Protection. Chapter 4 of the revision stipulated various provisions related to personal information protection. And in a 2008 revision, after the Auction incident, regulations related to personal information protection were reinforced, by, among other things, introducing the concept of a conforming business operator to stipulate entities other than OSP.

With the enactment of the Personal Information Protection Act (PIPA) in 2011, Korea established a regulatory system for personal information. The PIPA is a general law regulating overall subjects and personal information protection in Korea, and the ICT and Security Act specifically regulates OSPs. The Credit Information Protection Act specifically regulates financial institutions.

The PIPA broadly defined personal information as information that, by itself or in combination with other information, could be used to identify the person linked to the information. Accordingly, various types of information, such as the Internet Protocol address and media access control address, are recognized as personal information; therefore, their use is restricted. Adoption of big data tools by Korea's companies is only 7.5 percent, putting it fifty-sixth out of sixty-three countries in 2017, according to a study by the International Institute for Management Development.[65] Also, according to the Korea Data Industry Promotion Agency, the size of the Korean data markets as of 2017 was $443 million, which was only 0.25 percent of the U.S. market ($177 billion).[66]

In response to the EU GDPR and in preparation for the Fourth Industrial Revolution, there have been demands for improvements to Korean privacy regulations. Accordingly, in January 2020, the government revised the so-called three data laws' amendments to improve protection of personal information. By revising these three laws, the government introduced the possibility of using nonidentifying personal information and enabled social access to data with the expectation that new commercial services would be established, such as MyData. This is a one-stop service relying on data portability that was created by an industry-university consortium to provide various financial-related information and is expected to launch by August 2021.

Data Localization

Another major issue regarding personal data access in Korea concerns cross-border access and transfers. Korea had earlier provisions covering personal information abroad in its ICT and Security Act, but this didn't respond to questions about overseas transfers, and individual consent was required. In the PIPA, Article 17 also only allows transferring personal data outside of Korea in provisional cases.

Due to Korea's conservative regulatory environment, Article 17 only stipulates that the consent of the data subject must be obtained when transferring data about them to other countries. It does not specify in detail the level of protection that must be provided by data processors in other countries or additional protection measures that must be implemented. This is due to Korea's conservative regulatory environment. The Asia-Pacific Economic Cooperation forum established the Cross-Border Privacy Rules System in Asia, which is different from the EU's Adequacy and Safe Harbor (Privacy Shield) provisions established under the GDPR (see table 7).

A gap also exists in the regulations related to cross-border transfer in the revision of the three data-related laws. Discussions on this continue between Korea and other major economies, and the cross-border transfer using a mutual-adequacy approach, such as EU GDPR's adequacy and other options, will need to be continually reviewed.

Table 7. Differences Between the Two Approaches to Cross-Border Data Transfer

	Adequacy	Accountability
Model	EU General Data Protection Regulation	APEC's Cross-Border Privacy Rules
Objectives	Protect with the same level of protection	Complemented with different levels of protection
Unit	State (geographical)	Organizational
Characteristics	High barriers, low risk	Low barriers, high risk
Regulatory Model	Public authority	Self-regulation

Source: Kim KyungHwan, *Issues of Cross-Border Data Transfer and the Countermeasures* (PIS Fair, 2013).[67]

Conclusion

The importance of the internet, cloud computing, and other information technologies is increasing rapidly due to the coronavirus crisis and the Fourth Industrial Revolution transformation. As business activities, financial transactions, and education continue to shift online, security measures related to online identification, authentication, and nonrepudiation will become even more important. In addition, access to information is contributing a large part of new value creation in almost every sector of the economy. Furthermore, if Korea is to fully leverage data-centric services developed elsewhere, data localization and cross-border data flow issues will need to be better addressed in a consistent manner.

Korea has one of the most advanced ICT infrastructures in the world. Both government and industry have worked hard to make that infrastructure (and the applications that rely upon it) more secure and reliable. Korean efforts to improve online authentication can provide useful case studies that can inform many other countries facing similar challenges.

Korea has a unique political system characterized by a government-driven, conservative process for making and implementing policy that reflects the peculiar character of its bureaucracy. This resulted in the establishment of national-level infrastructure such as NPKI-based AC in Korea, while other countries entrusted ICT policies and security measures, including online authentication, to the market.

The history of online authentication in Korea began with the use of RRNs, which were used for online authentication without adequate privacy safeguards. As e-commerce and e-government developed, Korea experienced various personal data breaches, leading to limits on the number of cases where RRN collection and processing is allowed. The government introduced the I-PIN to replace the RRN, but it was not adopted in the market because it was difficult to deploy and use, and it was ultimately abolished. In contrast, online identification through mobile phones and credit cards has become mainstream due to their convenience.

Between 2001 and 2015, online authentication in Korea focused on a government-mandated NPKI-based AC system, a national PKI-based digital signature system. Although it had the advantage of providing a national-level authentication infrastructure, one disadvantage was that the government required use of specific technologies, and that policy probably held back progress of online authentication by five years or more.

In addition, during the implementation process, the contractors and security solution vendors forced a specific technology, the NPKI-based AC system, that did not meet users' needs. Users thus faced problems such as being reliant on Microsoft Windows and IE or being required to use ActiveX. This resulted in complaints from the public, who wanted more options and flexibility. Eventually, the mandate requiring use of the NPKI-based AC was abolished and changed to a joint certification, and the environment changed to the mixed use of various authentication methods. Unfortunately, the development and introduction of other authentication methods such as browser SSL certificate and FIDO have been relatively delayed in Korea, and they are still not mainstream in the market.

Korea's data access policy has also changed from the initial conservative approach to a more open, innovative approach. Access to public data was limited in the past by a cumbersome request process, but new approaches have led to the expansion of public data access and an open application programming interface and the establishment of a public data portal service, enabling access to much more data, sometimes on a near-real-time basis. Although it is not as developed as Estonia's Data Embassy, the Korean government is preparing to move key government resources to a cloud-based data repository, using a national convergence network design and a recovery system through the Daegu and Gwangju centers.

Until just a few years ago, Korea's online authentication and data access control–related policies and implementations were conservative. New market demands, especially users' expectation of new online services, and the changing business environment are gradually pushing policy in the direction of increasing usability and openness. This is one of the most important lessons that digital policymakers in other countries can learn from both Korea's successes and failures.

Another key lesson is that trust is one of the most important ingredients for successful policies for the internet. Developing standards or technologies for securing trust benefits from sustained, consistent, high-level, political leadership. In the early days of internet development, Korea built a platform for online authentication and identification by the government that played a key role in the development of the Korean internet environment, such as e-government services, online transactions, and other services. However, the dissemination of trust-related technologies led by the Korean government also had obvious problems, resulting in an iterative, trial and error process that created the current environment. This history can provide other countries lessons on the merits and limits of government-centered dissemination of trust-related technologies.

The national approach to online authentication demonstrates the clear benefits of economies of scale and rapid adoption. If a well-designed technology or platform is developed by key government agencies, it can accelerate adoption cost-effectively at the national level. In the case of Korea, as the state established an online authentication system and mandated it for many public sector and online transactions, it could quickly enable better authentication for much of the Korean internet environment. However, Korea's state-led online trust technologies were developed for a unique Korea system, failing to secure interoperability at the international level, and resulting in an isolated system—an example of the so-called Galápagos syndrome.

Even if the policy and architecture are well designed, it is also necessary to carefully monitor issues that may arise in the process of development, implementation, and use. In the case of Korea's online authentication-related technologies such as NPKI-based AC and I-PIN, the architecture itself did not have any problems, but security issues appeared in the process of implementing and managing them by the responsible agencies or security solution contractors. Therefore, the state should carefully establish the specifications of security- and privacy-related technologies, and continuously supervise (and adjust) the process of implementation and operation.

In the processes of policy and technological decisionmaking, arbitrary government decisions can be dangerous. Although civic groups, industries, and users expressed concerns about NPKI-based AC, RRN, I-PIN, and data access control in Korea, they did not significantly influence decisionmaking. Korea's internet real-name system is a representative example of a controversial policy that was later restrained when the judiciary ruled it was unconstitutional. Even if the government leads certain policies and technologies, it needs to gather opinions from all stakeholders and address them as much as possible.

A key lesson in Korea's online authentication is that government-led policies and implementations can be effective, but government mandates can have side effects. In Korea, specific online authentication and identification methods were deployed by the government, mandated in some areas, and therefore given priority over other authentication methods. As a result, the overall online environment depended on the public authentication methods, and development of the authentication industry was stymied. Eventually, a pivot to various authentication methods, including private certifications and a focus on evaluating the security of authentication methods, made government efforts to increase trust online much more effective.

In hindsight, it is clear that the Korean government should have pursued a different path. If, from the beginning, it had distributed and utilized the NPKI-based AC but used it as just one of various authentication methods and allowed users to choose one of several authentication methods, a sounder internet trust environment would have been created. Rather than mandating one solution, it is best practice to set general standards for online authentication, which could be met by various services, giving companies and users options and flexibility.

Key factors to consider in this process are usability and listening to the opinions of all the stakeholders of the internet. No matter how good the security of a specific authentication method, if its usability is poor, it may not be used widely, and technologies dependent on the certain environment, specific operating system, or browser, it may be neglected by users. To avoid this, it is necessary to listen to the opinions of internet service providers who need to introduce these technologies and the security companies that actually implement them. Most importantly, it is necessary to engage with the users themselves and use their feedback to set the direction of security and data related policies and their implementation.

CHAPTER 2

Korean Policies of Cybersecurity and Data Resilience

SO JEONG KIM AND SUNHA BAE

Introduction

South Korea is one of the most digitally connected countries in the world. Like other digital societies, it is vulnerable to cyber attacks. These attacks can wreak havoc on institutions, disrupt the economy, and erode social trust. Cyber attacks suspected of originating from North Korea, in particular, have become increasingly sophisticated. North Korea has used cyber attacks to achieve its political goals in South Korea (hereinafter Korea or the Republic of Korea—ROK) by stealing information and millions of dollars, sowing a sense of vulnerability in Korean society. Attacks from North Korea and other malicious actors have disrupted information and communications technology (ICT) systems in the ROK government and the country's private sector. In response, over the last three decades, Korea has developed better and more comprehensive cybersecurity policies aimed at ensuring the capability to prepare, respond, and recover in both the public and private sectors. However, much more remains to be done.

Korea's cybersecurity effort began in earnest in the 1980s when the government first began to actively promote informatization of the economy, government, and society.[68] Until the early 2000s, this effort was primarily focused on document security and physical security, aimed at providing a blanket of information protection or information security. These cybersecurity-enhancing goals were defined by Korea's National Intelligence Service (NIS) for the public sector and by the Ministry of Science and ICT (MSIT) for the private sector. But rather than developing a proactive, comprehensive, and nationwide cybersecurity policy or strategy, these agencies mostly limited themselves to responding to malicious activities and working to develop practical countermeasures.

However, the cyber threat had grown exponentially. Actors supposedly associated with Pyongyang had become capable of routinely launching successful attacks on information technology (IT) systems in South Korea. As the damage and disruption from these attacks intensified, public awareness of the need to improve cybersecurity put new pressures on both government and the private sector to develop a more robust set of tactics and tools.[69]

In 2009, the government at last made its first attempt to publish a national cybersecurity countermeasure. Three subsequent attempts followed, but these were more like lists of policy action items rather than strategic vision documents. By this point, however, Korea was also engaging in international efforts to address cyber threats and joining intergovernmental partnerships in cybersecurity. For example, South Korea participated in the first and second United Nations (UN) Groups of Governmental Experts (GGE) on information security, was part of the London Process, and hosted the Organisation for Economic Co-operation and Development (OECD) Ministerial Meeting on the Future of the Internet Economy in 2008, which produced the Seoul Declaration.[70] Particularly, because of the links between cyber threats and national security, the government in Seoul held discussions with other countries through the framework of both ad hoc multinational and bilateral mechanisms and channels. One result was the Seoul Conference on Cyberspace, held in 2013, which was an important opportunity to reflect on the importance of digital issues in the diplomatic and security fields. The Seoul Framework and Guidelines for an Open and Secure Cyberspace and Best Practice was produced by that conference.[71]

An attempt *was* made in 2009 to establish a single, national cybersecurity countermeasure, and cyber attacks were identified as a serious threat in the National Security Strategy published in July 2014.[72] It was not, however, until 2015 that the government announced comprehensive measures to strengthen Korea's cybersecurity posture and appointed a cybersecurity officer in the National Security Council directly under the president of Korea. With this position, the government tried to provide a focal point for better cybersecurity policymaking and coordination. However, three consecutive officers were not fully effective in that role for varying reasons: from their expertise with cyber issues to political differences on who should have overarching authority on cyber-related matters. In the years since 2015, the role of the independent presidential officer of cybersecurity has been merged with that of the secretary of information convergence.

Despite increased awareness of the importance of cybersecurity, there has been very little research by Korean social scientists about how institutions and practices related to cybersecurity have evolved in the country. Instead, the research on cybersecurity has been mostly limited to the writings of a few jurists on narrow legal aspects and the highly technical discussions of cybersecurity practices shaped by engineers, technologists, and security practitioners. This narrow focus on technological solutions has meant that much policy work needs to be done to ensure that such solutions will be effectively deployed and managed.

Different Korean agencies have pushed different messages and competing tools and programs to address cybersecurity. The result has, until very recently, been a lack of effective strategy and institutionalized policy practice. The Korean-convened Global Cyberspace Peace Regime (GCPR), a major platform facilitating highly professional track 1.5 discussions, embracing academic and governmental experts from the Asian region and around the globe, is a step in the right direction.[73] Still, contributions from the social science community are lacking. This chapter aims to fill that gap and share lessons learned from Korea's more recent experience.

Interministerial competition for cybersecurity oversight has been an additional challenge in Korea. Government policies have helped make Korea a high-growth, high-income economy, so the economic ministries have a good deal of clout. But their views of digital issues and particularly cybersecurity are very different from the security agencies. Their priorities and even their cybersecurity language sometimes differ. That said, it is encouraging that internal efforts have started to develop a common terminology or lexicon in this field. It should lead to more coordinated policymaking and action in the future.

The evolution of Korean institutions, policies, and practices and the country's experience as a target of malicious cyber activity can inform an understanding of its own experiences with cyber defense and data resilience. It can also aid other countries in their approach to cybersecurity.

For more than two decades, major cyber attacks have triggered new initiatives meant to reduce the likelihood of future attacks and reduce the damage and disruption they can cause. After attacks such as the distributed denial-of-service (DDoS) attack in 2009, the attack on broadcasting systems in 2013, and the ransom attack on Korea Hydro and Nuclear Power in 2014, the Korean government responded by announcing new comprehensive measures.[74]

Table 8. Response to Critical Cyberattacks by the Republic of Korea Government

Year	Cyber attack	Preventative measures or countermeasures	Institutional measures
2000		Establish National Security Research Institute (NSR)	
2001			Enact the Act on the Protection of Information and Communications Infrastructure (Act on the PICI) Enact the Electronic Government Act (E-Government Act) Enact the Act on Promotion of Information and Communications Network Utilization and Information Protection, so on.
2003	January 25 internet disruption		

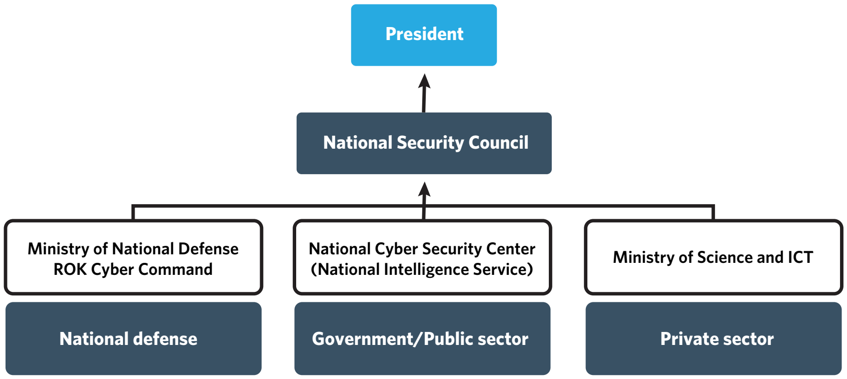
2004		Establish the National Cybersecurity Center (NCSC) under the National Intelligence Service (NIS)	Enact the National Crisis Management Basic Directive (presidential directive) Create the National Cyber Crisis Management Manual
2005			Enact the National Cybersecurity Management Directive (presidential directive)
2007			Revise the E-Government Act Revise the Act on the PICI
2009	July 7 DDoS	National Cyber Crisis Comprehensive Countermeasure	
2010		Establish Cyber Command	Revise the E-Government Act
2011	March 4 DDoS NH Bank hacking	National Cybersecurity Master Plan	
2012		Build Private-Public-Military Joint Cyber Threat Response Team	
2013	March 20 cyber attack March 25 cyber attack	National Cybersecurity Comprehensive Countermeasure	
2014	KHNP hacking	Establish Cybersecurity Training and Education Center (CSTEC) of NSR	
2015		Designate a Cybersecurity Adviser in the Office of the President Establish the Financial Security Institute (FSI) Establish the National Cybersecurity Status Building Measures	Enact the Act on the Promotion of Cybersecurity Industry
2016	Interpark hacking	K-ICT Convergence Security Strategy	
2017	WannaCry ransomware attack Nayana ransomware attack		
2018	PyeongChang Olympic Games hacking		
2019		National Cybersecurity Strategy National Cybersecurity Basic Plan	
2020			Revision of the National Intelligence Service Act

Source: NIS et al., "White Paper on Information Security 2020" (in Korean), 2020.

Cybersecurity Governance

Over the years, the Korean government's statements about cyber attacks raised awareness among policymakers and the public about the need for more government action to address the threat. Cybersecurity governance was composed of three agencies: the National Cybersecurity Center (NCSC) under the National Intelligence Services for the government and public sector; the Ministry of Science and ICT for the private sector; and then individual response systems for a diverse group of agencies, such as the one at the Ministry of National Defense for the military sector. The NCSC, established in 2004, was named as a general manager, and the National Cyber Safety Management Regulations enacted in 2005 defined each organization's roles (see figure 10).[75]

Figure 10. Cybersecurity Governance of the Republic of Korea


President
National Security Council
Ministry of National Defense
ROK Cyber Command
National Cyber Security Center
(National Intelligence Service)
Ministry of Science and ICT
National defense
Government/Public sector
Private sector

Source: NIS et. al., "White Paper on Information Security 2018" (in Korean), 2018, p. 52.

Korea has, in recent years, made significant changes to its framework for cybersecurity. The National Security Council (NSC), which reports directly to the president, has been coordinating cybersecurity since 2015.[76] Under the NSC, the NCSC leads practical efforts for cybersecurity across the national government and the public sector where more than 70 percent of the nation's critical information infrastructure facilities are located.[77] Within the NCSC, the Ministry of Science and ICT and the Cyber Command of the Ministry of National Defense are responsible for the private sector and the military sector respectively.

This system has made a positive contribution to the overall improvement of the initial cybersecurity capabilities. There is no doubt as to the effectiveness of many of the measures that were first introduced by public institutions. The state and public sectors actively led the cybersecurity technologies policies and expanded the application to the private sector, supporting the improvement of technical and managerial capabilities. For example, Korea has cybersecurity regulations that provide the basis for strengthening cybersecurity for both the central government and public institutions. With that, for example, collecting and sharing information needed to strengthen cybersecurity is specified as a unique duty of the NIS. The NCSC is establishing and operating a National Cyber Threat Information–sharing system for incident investigation and information sharing in public institutions.[78] But some have pointed out that a reexamination of the effectiveness of the existing system is necessary due to the recent technological development and expansion and convergence of cyberspace.

To protect critical information infrastructure from cyber threats and attacks, Korea enacted the Critical Information Infrastructure Protection Act (hereafter CIIP Act) in 2001, which has been subsequently amended. Under the CIIP Act, Korea established a Critical Information Infrastructure Protection Committee under the Office of the Prime Minister to coordinate CIIP-related activities among several governmental authorities. The CIIP Act mandates that the NCSC, for the government and public sector, and the Ministry of Science and ICT, for the private sector, have key roles in CIIP activities in each sector. The NCSC, which has developed advanced technologies and trained experts, has taken the lead in the government's CIIP-related activities and coordinated the activities of other ministries.[79] As a result of the CIIP Act, more than 400 facilities, including nuclear power plant systems, transportation systems, and commercial bank networks, have been designated as critical information infrastructure (CII).[80]

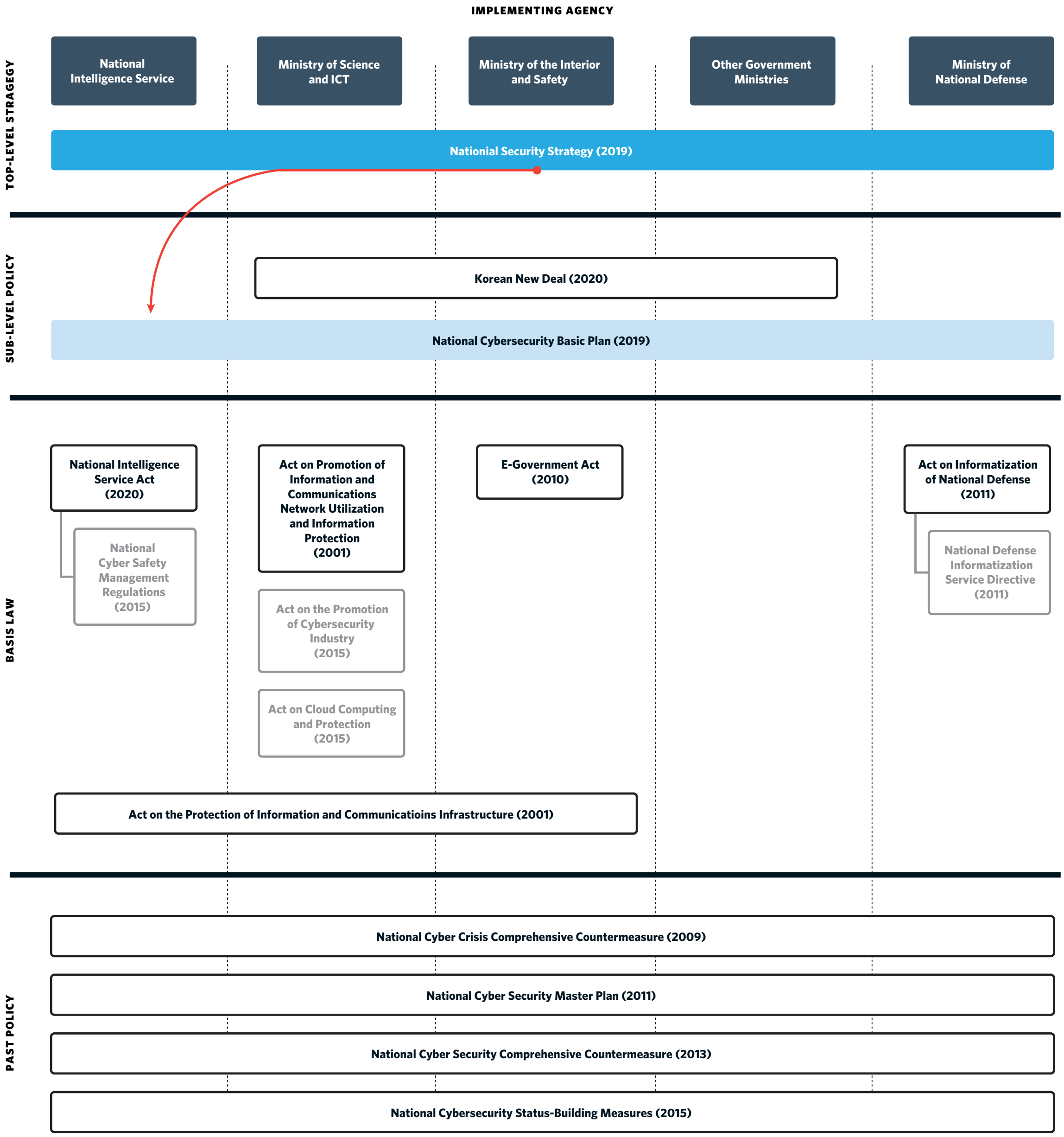
National Cybersecurity Strategy and National Cybersecurity Basic Plan of 2019

In 2019, the publication of a new National Cybersecurity Strategy by the presidential National Security Office was widely regarded as the most important and effective policy document on cybersecurity produced in more than thirty years in Korea.[81] It led to redoubled efforts to strengthen the resiliency of Korea's digital infrastructure and was followed by the establishment of a basic plan and an implementation plan. The strategy identified 5G design and deployment and anti-drone measures as the most critical areas of government focus, both of which were new issues for priority emphasis in Korean cybersecurity and national security.

The goals of this 2019 strategy are to ensure stable operations of the state, respond to cyber attacks, and build a strong cybersecurity foundation in Korea. For this purpose, the strategy sets out three basic principles: balance individual rights with the need for better cybersecurity, conduct security activities based on the rule of law, and build a system of participation and cooperation among domestic stakeholders and foreign counterparts. The strategy encourages individuals, business, and the government to participate in cybersecurity activities, and pursue close cooperation with the international community. It outlines how Korea will ensure it can continue reaping the benefits provided by ICTs while minimizing risks. The strategy is built around six strategic pillars: secured national critical infrastructure, enhanced cyber attack defense capabilities, trust- and cooperation-based governance, cybersecurity industry growth, fostering a cybersecurity culture, and strengthened international cooperation.

The strategy was followed by the National Cybersecurity Basic Plan, which outlines 100 tasks to be accomplished over the next two to three years.[82] The strategic tasks and detailed tasks of the strategy are included in the 2019 National Cybersecurity Strategy. Those 100 tasks have, in turn, been categorized as either policy tasks or technological tasks. Policy tasks make up almost 70 percent of the whole plan and

Figure 11. Status of Cybersecurity Policy in Korea


IMPLEMENTING AGENCY
National Intelligence Service
Ministry of Science and ICT
Ministry of the Interior and Safety
Other Government Ministries
Ministry of National Defense
TOP-LEVEL STRAGEGY
Nationial Security Strategy (2019)
SUB-LEVEL POLICY
Korean New Deal (2020)
National Cybersecurity Basic Plan (2019)
BASIS LAW
National Intelligence Service Act (2020)
National Cyber Safety Management Regulations (2015)
Act on Promotion of Information and Communications Network Utilization and Information Protection (2001)
Act on the Promotion of Cybersecurity Industry (2015)
Act on Cloud Computing and Protection (2015)
E-Government Act (2010)
Act on Informatization of National Defense (2011)
National Defense Informatization Service Directive (2011)
Act on the Protection of Information and Communicatioins Infrastructure (2001)
PAST POLICY
National Cyber Crisis Comprehensive Countermeasure (2009)
National Cyber Security Master Plan (2011)
National Cyber Security Comprehensive Countermeasure (2013)
National Cybersecurity Status-Building Measures (2015)

Source: NIS et al., “White Paper on Information Security 2020” (in Korean), 2020.

include international collaboration, international norm setting, CIIP, crisis management, and information sharing. In addition to the National Cybersecurity Basic Plan, each agency contributes to an annual National Cybersecurity Implementation Plan.

It is very encouraging that various efforts are being made to achieve the vision presented by the strategy through the basic plan and implementation plan. However, revising and refining the plans will require more research in some key areas. For instance, it is necessary to develop deterrence strategies to discourage cyber attacks, but the strategy does little to make headway in this area. In particular, in-depth discussions with the national security agencies should reflect the scope, intensity, and impact of the increasingly serious cyber attacks—in both military and economic terms. In this regard, the strategy needs to more clearly articulate goals and define terms, as well as explain how responsibilities are assigned to government agencies as well as to private sector organizations. An improved strategy should start with a thorough threat analysis, which would be then be updated as necessary, to enable well-informed, data-driven decisionmaking.

Revision of the National Intelligence Service Act

Since 2006, the ROK has worked to implement the so-called Cybersecurity Basic Law to make clear each agency's role and responsibility and the nationwide cybersecurity framework. The National Intelligence Service, in particular, has pushed for the enactment of the Cybersecurity Basic Law, revised the National Intelligence Service Act, and established the basis for its role regarding cybersecurity. On that basis, the government revised the National Intelligence Service Act in 2020 and enacted the Cybersecurity Business Regulations in 2020 that stipulated the National Intelligence Service's role in cybersecurity.

The revision of the National Intelligence Service Act that established the scope of the NIS's cybersecurity operations, Article 4 of the National Intelligence Service Act, defined three main tasks: collection, analysis, and distribution of cybersecurity-related information; countermeasures related to cybersecurity performance; and preventing and responding to cyber attacks and threats against government agencies and public sector institutions.

In addition, the name of the National Cybersecurity Center was changed from "cyber safety" to "cybersecurity" in Article 3(3) of the Cybersecurity Business Regulations.[83] The National Intelligence Service Act emphasized that the security of cyberspace is an important national security issue. The act therefore defined cybersecurity as one of the key tasks of the National Intelligence Service (NIS). Therefore, the name of the center was changed to the same as the name of the NIS task. In addition, when the National Cybersecurity Center was established (in 2004), the term "national security" was often translated as "safety" in Korea, but more recently it has been generally translated as "security."[84]

The basis for establishing and implementing basic measures for cybersecurity led by the NIS in the consultation of National Security Council and other central government agencies was provided in Article 8 of the Cybersecurity Business Regulations. The National Security Research Institute was designated as a research-and-development (R&D) specialized institution for cybersecurity affairs to expand its work to develop the strategies, policies, and technologies necessary to improve cybersecurity (in Article 17).

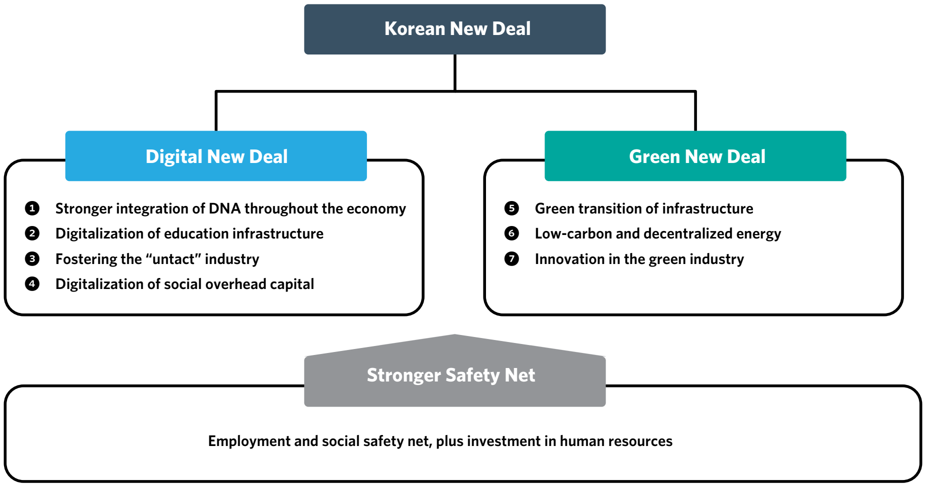
Nevertheless, much like the national cyber strategy, the NIS law and the enforcement ordinance of the law also have room for improvement. First, some terms are not defined under these regulations in a consistent way—not least, the very definition of "cybersecurity." The National Cyber Safety Management Regulations defined this as encompassing three things—cyber attacks, cyber safety, and cyber crisis—but the revised NIS law and the newly enacted enforcement ordinance have no clear definition of "cybersecurity."[85]

It is also necessary to clarify the duties of the different offices and agencies involved in cybersecurity and cyber resilience. For instance, the NIS can collect, create, and distribute "cybersecurity-related information including information on international hacking group and state-sponsored group" according to the law's Article 4.[86] But the scope of "international and national hacking groups" has not been defined in the law.[87]

Korean New Deal

Various fields in Korea, including ICT and cybersecurity, have changed due to the coronavirus pandemic that hit in 2020. With the explosive growth of telecommuting and online services such as telemedicine (which some Koreans refer to as "untact"—a new word combining "un" and "contact"), Korea's dependence on ICT technology is expanding more rapidly than ever before. The government announced the Korean New Deal in July 2020 to overcome the economic recession after the pandemic and to change the paradigm across Korea's economy and society.[88] The Korean New Deal applies to both the public (excluding the military) and the private sectors and consists of three projects: the Digital New Deal, the Green New Deal, and the Strong Safety Net. Cybersecurity is included in the Digital New Deal project.

Figure 12. Focus Areas of the Korean New Deal

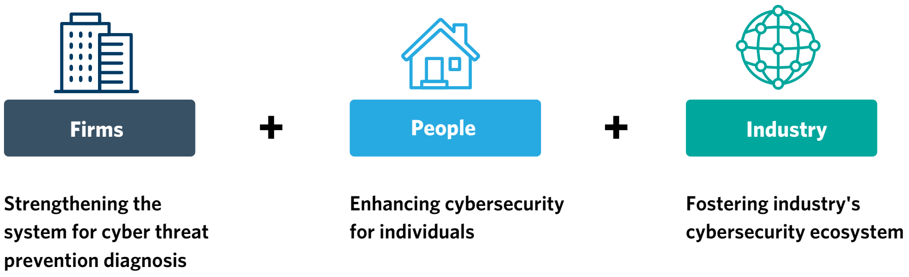

Korean New Deal
Digital New Deal
❶ Stronger integration of DNA throughout the economy
❷ Digitalization of education infrastructure
❸ Fostering the "untact" industry
❹ Digitalization of social overhead capital
Green New Deal
❺ Green transition of infrastructure
❻ Low-carbon and decentralized energy
❼ Innovation in the green industry
Stronger Safety Net
Employment and social safety net, plus investment in human resources

Source: Ministry of Economy and Finance, "Korean New Deal: National Strategy for a Great Transformation," July 2020.

The Digital New Deal is a policy aimed at promoting and spreading digital innovation and dynamism across the economy by expanding the digital divide based on ICT, such as e-government infrastructure services. Cybersecurity is mainly related to the first project on "stronger integration of DNA (data, networks, and artificial intelligence) throughout the economy." That project consists of four subprojects, and two of them deal with cybersecurity.

The first subproject is focused on "making a smart government that utilizes 5G and AI." The government will implement pilot projects based on blockchain technology, establish 5G at all government complexes, and transition to cloud computing for public information system by 2025. Systems that for citizen services, such as homepages for public disclosure, will be transferred to a private cloud center. And systems for public administration are scheduled to be relocated and integrated into a public security cloud center with enhanced security functions.

Figure 13. K-Cyber Prevention System


Firms
+
People
+
Industry
Strengthening the system for cyber threat prevention diagnosis
Enhancing cybersecurity for individuals
Fostering industry's cybersecurity ecosystem

Source: Ministry of Economy and Finance, "Korean New Deal: National Strategy for a Great Transformation," July 2020.

And the second subproject is focused on "advancing cybersecurity." Cybersecurity threats are becoming more sophisticated and causing widespread damage due to digitalization and the spread of untact services. So, the goal of the project is to make the digital environment safer, enable untact services in daily life, and to foster the security industry.

The "advancing cybersecurity" initiative is divided into three domains: firms, people, and industry. First, for firms, the government helps unprepared SMEs make the security investments needed to strengthen cyber defense, diagnose threats, and improve response. In addition, special emphasis is put on addressing vulnerabilities in untact services. For people, the government supports major public facilities for software and website inspections, remote security checks, and safety measures to enhance cybersecurity for people's daily lives. Lastly, for industry, in order to revitalize the cybersecurity industry ecosystem, the government is promoting the application of new technologies such as blockchain and fostering promising AI-based security companies.

The Evolution of Korean Cybersecurity Policy

Notions of cybersecurity—and the challenges it presents—have evolved significantly in Korea over the last twenty years. This is reflected through the development of concepts and terminology used to describe digital technologies and cyber threats.

Research and Development Trend Analysis (by Keyword Comparison)

This chapter's analysis of keywords in cybersecurity-related academic journals demonstrates how research trends in cybersecurity have changed during the last two decades in response to new threats and to the increased attention being paid to this issue.[89] The papers analyzed are limited to highly respected Korean-language journals registered in the Korean Citation Index (KCI).[90] The National Research Foundation of Korea, which manages research journals (including papers published by domestic academic societies), does an annual ranking of journals to determine which will be recognized as KCI-registered journals.

To analyze research trends, the authors divided the catalogue of published papers into four time periods based on when major cyber attacks hit Korea after 2001. The major cyber attacks during this period were the 2003 internet disruption, the 2009 DDoS attack, and the KHNP hacking in 2014.

Table 9. Top Ten Cyber Keywords in Korean Academic Journals

Period	2001–2003 (n = 13)	2004–2009 (n = 62)	2010–2014 (n = 162)	2015–September 2019 (n = 173)
1	Information protection	Information protection	Information protection	Information protection
2	Informatized society	Information security	Information security	Information security
3	Information Disclosure Act	Personal information protection	Personal information protection	Cybersecurity
4	Mass media social ethics	Privacy	Security policy	Cybersecurity (as related to information protection)
5	Mass media freedom of speech	Self-regulation	Information protection governance	Internet of Things (IoT) security
6	Encryption	RFID	Information protection management system	Basic law
7	Information disclosure	Governmental regulation	Personal Information Protection Law	Personal information protection
8	Criminal law	Risk analysis	Cybersecurity	Cyber terror
9	Secret sharing scheme	Bio authentication	Authentication	Privacy
10	-	Encryption	Policy compliance	Cyber crime

Note: From 2001 to 2003, there were not many related studies, thus only nine keywords were derived during this period.

From 2001 to 2003, keywords related to the information society, laws, ethics, and passwords frequently appeared. Information security terms began to be used in the 2004–2009 period. For example, keywords and phrases such as “personal information protection,” “privacy,” “self-regulation,” “government regulation,” “RFID,” “risk analysis,” and “biometrics” began to creep into Korean academic and policy discussions. It was during this period that the Korean government began to regulate the internet. Measures such as an online identification system were implemented, but this led to controversy about freedom of expression on the internet. As a result, the need for self-regulation emerged and the Korea Internet Self-Governance Organization was established in 2008.

For 2010–2014, as in previous time periods, “information protection,” “information security,” and “personal information protection” appear at the top of the rankings. But keywords such as “security policy,” “information protection governance/management system,” and “cybersecurity” appear at the top for the first time, suggesting a further evolution in Korean thinking. Finally, from 2015 to September 2019, the top keywords were “information protection,” “information security,” “and “cybersecurity.” Related keywords such as “security,” “basic law,” “cyber terrorism,” and “cyber crime” were also widely used.

This study shows that terms with similar meanings to cybersecurity, such as “information protection” and “information security,” were incorporated into the research over time. Such terms often lacked clear definitions. Part of the reason for this is that due to interministerial competition, a cyber glossary was not (and still has not been) clearly defined by the government. The development of a cyber glossary, drawing on U.S. and other international research, is essential for the future development of Korea’s cybersecurity policy.

Strategic Training and Competition

In South Korea, the Cyber Conflict Exercise (CCE) is a competition sponsored by NIS and NSR and includes a so-called strategy game.[91] During the CCE, situation report procedure and media response training are part of the strategy game to highlight the importance of comprehensive crisis response capabilities during a cyber crisis, and to improve not only technical response capabilities but also policy response capabilities.

Situation reporting is an activity that promptly “reports a summary of the current situation and related response activities accurately.”[92] It is essential in the event of a cyber crisis. Quick, accurate analysis is needed to identify the cause of the accident and establish countermeasures, support rapid recovery, prevent further spread of damage, and promote coordination and cooperation in response with related domestic organizations.

Media response refers to the activities of participants in the competition to analyze trends in media such as newspapers and social networking services, and to respond to direct inquiries from media parties. In order to limit the cascading effects caused by attacks and minimize social confusion in a crisis, participants need to create content and prepare efficient and consistent communication measures that build and maintain the trust of the public and the media in peacetime as well as in crisis situations.

The policy training scenario consisted of a cyber attack on government agencies and infrastructure in a virtual city called Hope City, Korea, and simulated the response of government officials and other key players. A status report provided a cyber warning at each stage of the exercise. Participants briefed the "media" in the middle of the competition process, and via inquiries and answers on social media.

Most of the participants had no history of work related to situation reporting or media response, but they received positive evaluations, having gained experience in crisis communication and policy decisionmaking through strategic games. These games and simulations helped participants realize the need to improve policymakers' ability to respond to a cyber crisis.

In 2021, the ROK joined the North Atlantic Treaty Organization's Locked Shields exercise.[93] Korea's participation in the exercise was led by the NIS,[94] which combines technical exercise and strategic exercise, and the government placed great significance in participating in strategic exercise.[95]

Strengths and Weaknesses of Korean Cybersecurity Capabilities

Korea is among the most connected economies in the world. This is expected only to intensify with the arrival of the Fourth Industrial Revolution (4IR) and its expansion of machine learning and artificial intelligence. Many Koreans view the 4IR as a new driving force for innovative growth in one of the world's most innovative economies. Better cybersecurity will be a prerequisite to the success of the 4IR. That is why Korea is investing, including in international cyber partnerships, to promote better cybersecurity policies and practices at home while offering its distinctively Korean contributions to other countries.

K-Global Cybersecurity Capability Assessment and Applicability

Korea has developed a tool to make basic data available for cyber-related decisionmaking: the Korea Global Cybersecurity Capability Assessment (GCCA) tool.[96] It assesses the national competency level through comparison and analysis with other countries according to selected criteria.[97]

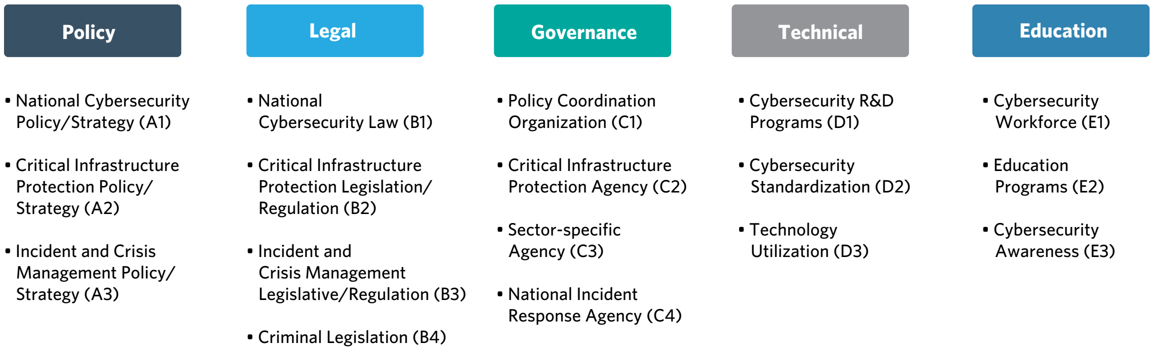
As interest in the GCCA has increased and research has continued, the scope of the project has expanded. Initially, the main purpose of the GCCA was to focus on understanding the current state of cybersecurity and suggest new directions for policy development and capability-building measures. Recent additions to the GCCA can help foster global cooperation, information sharing, and awareness raising. These additions facilitate sharing of policies, technical standards, and best practices between countries. Due to the global nature of cyberspace, the boundaries between countries are blurring and attacks using cyber infrastructures in other countries are easy to carry out and harder to attribute. For that reason, Korean government officials and corporate leaders tend to emphasize how international security is affected by cyber attacks to critical national infrastructure. Through capability assessment, Korea aims not only to strengthen cybersecurity, but also to lay the foundation for strengthening cybersecurity through cross-border cyber defense programs with international partners, enabling cooperative responses to global cyber threats. This trend is well reflected in the International Telecommunication Union's Global Cybersecurity Index 2018.[98]

The GCCA was developed by the NSR using a national cybersecurity assessment methodology that reflects Korea's own unique and distinctive characteristics. The assessment is conducted through expert surveys, with seventeen assessment criteria in five categories: policy, legislation, organization, technology, and education/training.

The policy category provides an assessment of the will and direction to strengthen cyber capabilities at the national level, and consists of five criteria, including cybersecurity policy and infrastructure protection policy. The legislation category provides an assessment of the legal basis for policy promotion, and consists of four criteria, including the level of development of cybersecurity regulations and critical infrastructure protection legislation and regulations.

The categories of organization, technology, and education and training assess the level of implementation of national cybersecurity policies and laws. In the organizational category, there are four criteria, including the level of development of the Korean organizations responsible for cybersecurity and the role of critical infrastructure protection organizations. In the technology category, there are three criteria: the level of development of cybersecurity R&D programs, the establishment of standards, and technology adoption. In the category of education and training, there are three criteria, including education programs for training professional manpower.

Figure 14. Global Cybersecurity Capability Assessment Domains and Criteria



Policy

- National Cybersecurity Policy/Strategy (A1)
- Critical Infrastructure Protection Policy/ Strategy (A2)
- Incident and Crisis Management Policy/ Strategy (A3)

Legal

- National Cybersecurity Law (B1)
- Critical Infrastructure Protection Legislation/ Regulation (B2)
- Incident and Crisis Management Legislative/Regulation (B3)
- Criminal Legislation (B4)

Governance

- Policy Coordination Organization (C1)
- Critical Infrastructure Protection Agency (C2)
- Sector-specific Agency (C3)
- National Incident Response Agency (C4)

Technical

- Cybersecurity R&D Programs (D1)
- Cybersecurity Standardization (D2)
- Technology Utilization (D3)

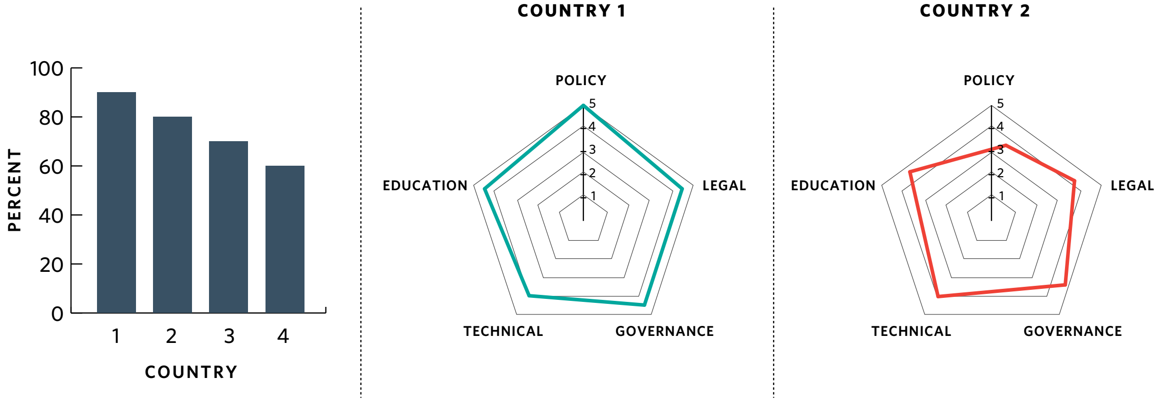
Education

- Cybersecurity Workforce (E1)
- Education Programs (E2)
- Cybersecurity Awareness (E3)

Source: Minkyung Song, "National Cybersecurity Capability Assessment [No. 520-2416-19-020]," National Security Research Institute in Korea, December 2019.

As assessment result indicators, rankings by country were derived for comparative analysis with leading countries. This helps decisionmakers to identify the strengths and weaknesses of each country. In comparison to other countries that have used the assessment tool, Korea was assessed relatively high in terms of the establishment of infrastructure protection standards and implementation of cybersecurity technologies. However, it was assessed to be relatively low with respect to governance and cybersecurity R&D education programs.

Figure 15. Example of a Global Cybersecurity Capability Assessment



Source: Minkyung Song, "National Cybersecurity Capability Assessment [No. 520-2416-19-020]," National Security Research Institute in Korea, December 2019.

Strengths and Weaknesses of Korea's Cybersecurity Capabilities

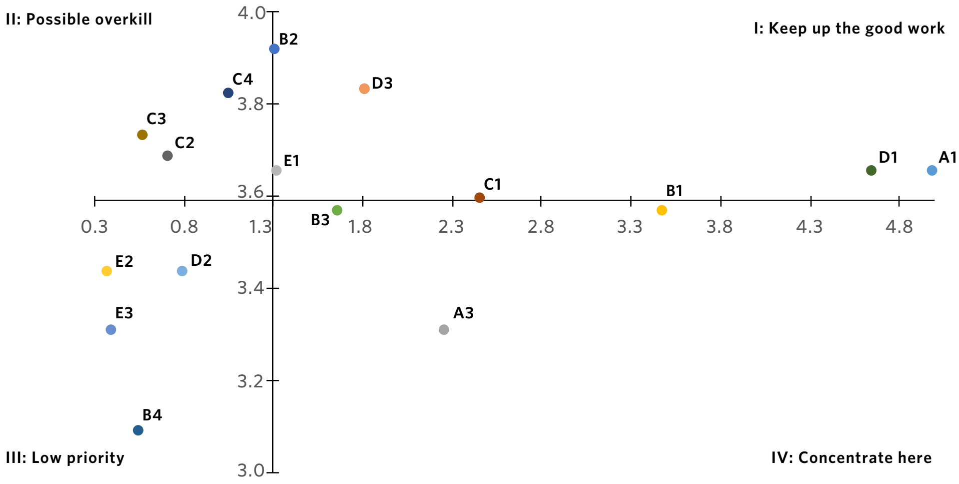
To analyze the strengths and weaknesses of Korea's cybersecurity capabilities, therefore, the authors conducted an importance performance analysis (IPA). The IPA is a method that sets priorities by using the importance and performance of an analysis target.[99] It has been used in various social science fields, such as public administration, policy studies, and business administration.

The IPA displays the results in a quadrant centering on the average value of importance and performance. In the GCCA, the x-axis was defined as the importance of each criterion and the y-axis was defined as the score for each criterion. The IPA matrix was derived by crossing the two axes using the median value for the x-axis and the average value for the y-axis as the origin. Quadrant I ("Keep up the good work") are criteria with high importance and high scores, and it is desirable to maintain the current status. Quadrant II ("Possible overkill") are criteria that scored higher than their importance and require passive management. Quadrant III ("Low priority") reflect both low importance and performance, requiring mid- to long-term improvement. Quadrant IV ("Concentrate here") includes criteria that have a high importance but a low score, so they involve items that need intensive improvement in the future.[100]

The importance of each criterion for the IPA was scored by surveying domestic experts in Korea. The IPA analysis of GCCA results for Korea show that the elements that need to be improved to bolster its cybersecurity capabilities mainly include national crisis management policies and legislation, and cybersecurity regulations. Criteria that need improvement in the mid to long term include cyber crime regulations, standards establishment and implementation, and education programs.

The Korean government announced its National Cybersecurity Strategy in 2019 and soon afterward announced its associated implementation plan, including eighteen key tasks and 100 detailed tasks in the National Cybersecurity Basic Plan. However, the government failed to assign priorities to each task in the strategy and the basic plan. In the future, according to the analysis of Korea's global cybersecurity capability evaluation, it will be important for the efficiency of the implementation of each task to be improved by identifying the assessed criteria that need to be given a priority focus (quadrant IV).

Figure 16. Korea's Result in Global Cybersecurity Capability Assessment, 2019



Note: See figure 14 for corresponding definitions of alphanumeric labels.

Source: Minkyung Song, "National Cybersecurity Capability Assessment [No. 520-2416-19-020]," National Security Research Institute in Korea, December 2019.

Key Features of Cybersecurity Governance and Best Practices in Korea

Cybersecurity Governance

The ROK has continuously encountered cyber attacks. Cyber attacks have occurred at various scales—from simple phishing attacks to infrastructure paralysis. Therefore, the ROK has clarified the responsibilities of organizations addressing cyber threats and established laws and policies to prevent and respond to cyber attacks in both peacetime and crisis periods.

Most components of critical infrastructure in the ROK, including energy, water, and transportation, are designated as public institutions and are operated centrally by the state (almost 70 percent). So, the role of the private sector in strengthening the cybersecurity of critical infrastructure, while essential, is smaller than in many other countries. The state leads the collection and sharing of threat information regarding infrastructure, and the response to cyber attacks on critical infrastructure. Therefore, the establishment and implementation of cybersecurity policies for critical infrastructure could be quickly accomplished with active cooperation without significant opposition or extended negotiations.

Lastly, cybersecurity governance in the ROK involves the public sector, the private sector, and the military, with the National Security Council as the control tower. There is a cooperation framework covering the three sectors. In particular, the NIS, an intelligence agency, has been central since the beginning of the nation's cybersecurity policy establishment in the early 2000s, and the Joint Cyber Threat Response Team (representing the three sectors) is also under the NIS. The NIS viewed cyber attacks as a national security issue and actively collected threat information. On the other hand, the illegal collection of information using software by the NIS has led to its role in cybersecurity being contentious and led to public distrust.

Good Practices

Over the years, the ROK has taken several measures to prevent recurrences of the damage caused by cyber attacks.

After the 2003 internet disruption, Korea established a mandatory system for constant backup.[101] The central government introduced a backup solution near the end of 2003, and it became mandatory for local governments in 2004. After other incidents, countermeasures were focused on the development of defense technologies, such as a proactive response system for DDoS attacks that was established after the 2009 DDoS attack, as well as improving a rapid cyber treatment system for zombie computers following the 2011 DDoS attacks.[102]

In response to these incidents, the government also acted to strengthen information protection in the private sector. In January 2004, the government revised the Information and Communication Network Act to make safety checks of information protection mandatory.[103] The safety check evaluates whether every provider of information and communications services and every business operator of agglomerated information and communication facilities complies with the government's information protection guidelines to prevent intrusion incidents in the private sector.[104] There were complaints from target companies regarding the burden of costs, but the government saw this as an opportunity to raise the security awareness and security level of internet-related companies overall.[105]

Given Korea's extensive history with DDoS attacks, the network environment is well equipped with a DDoS attack response system. DDoS response solutions are installed throughout the network infrastructure, and regular simulation exercises are conducted to prepare for attacks. Also, the government distributes DDoS attack response guides to the public and private sector actors and provides blocking measures tailored to the type of attack.

In addition, the network separation system was introduced in central government ministries in 2006 and the network separation of the public sector was completed in 2010. The necessity of network separation in the private/financial sector emerged after the DDoS attacks in 2011, and the scope of the network separation regulations was expanded. The regulations are defined in relevant legislation by sector. According to this legislation, the public sector should separate internal and external networks, and companies, which have more than 1 million personal information records, should separate the computer network where personal information is stored.[106] It further states that financial companies should block internet access from their business computers, and ensure that computers for system operation, development, and security are on separate networks.[107]

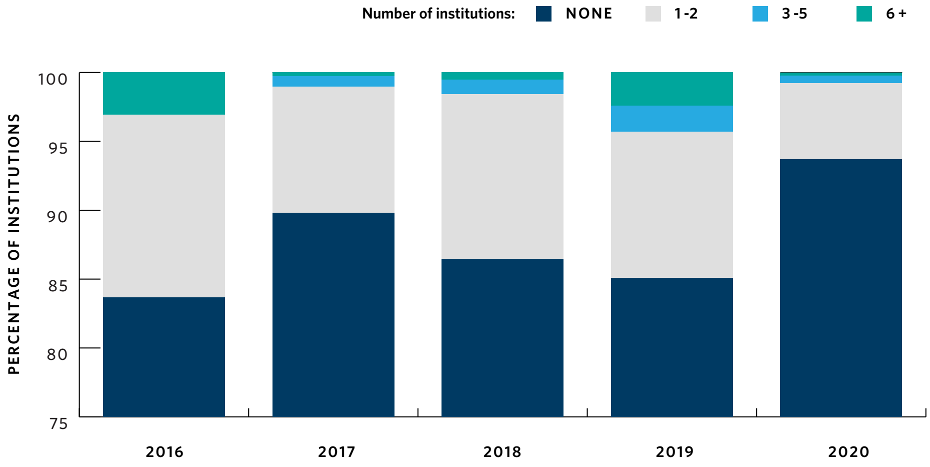
Cyber attacks can occur anytime. So thorough preparations are carried out when hosting large-scale events at the national level, such as the Olympics. Despite that, when Korea hosted the Winter Games at PyeongChang in 2018, information systems related to the Olympics were damaged and most services were stopped due to an attack by an advanced persistent threat (APT) that had been carefully prepared for a long time.

The organizing committee for the Olympics considered the possibility of a cyber attack during preparation and strengthened security when designing the system. In addition, high-intensity hacking exercises, penetration testing, training, information protection pre-diagnosis, and personal information impact assessments were also conducted.[108] In particular, the committee installed a very advanced defense system against DDoS attacks, which are the main type of attack. The committee organized and operated on an information protection system that cooperated with government departments such as the NIS, the Cyber Police Agency, and Cyber Command, as well as an advisory organization composed of private companies and white hat hackers.

A quantitative evaluation of the effectiveness of various cybersecurity policies of the Korean government has not been conducted. However, the results of an annual survey targeting public organizations and private companies in charge of information protection show that the number of cyber attacks that cause damage is decreasing, and activities for preventing and responding to accidents are being strengthened.[109]

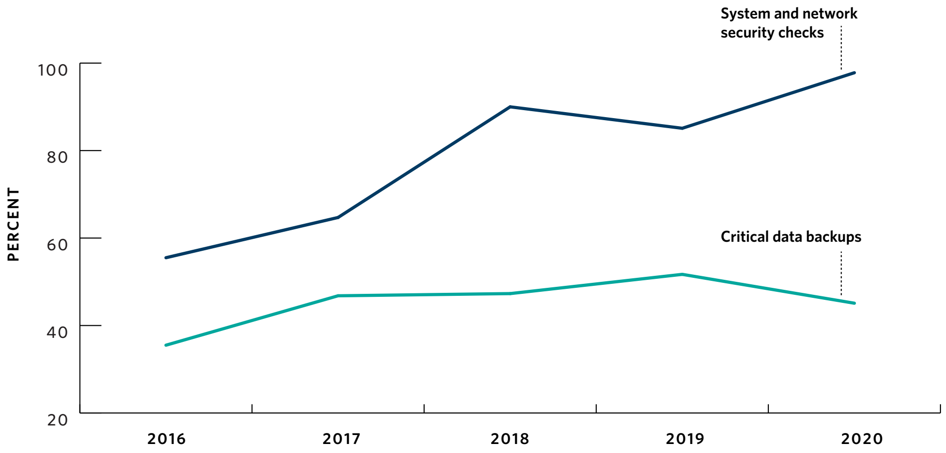
The National Intelligence Service annually surveys the number of cyber attacks in the public sector targeting 130 central administrative agencies.[110] According to the survey, the number of cyber attacks that caused damage is continuously decreasing even though the number of cyber attacks is increasing.

Figure 17. Cyber Attacks That Caused Damage in the Korean Public Sector



Source: Series of white papers on information security by the NIS et al. from 2017 to 2021.

Figure 18. Comparison of Security Checks to Data Backups in the Private Sector



Source: Series of white papers on information security by the NIS et al. from 2017 to 2021.

The Ministry of Science and ICT also annually surveys more than 9,000 businesses to establish and implement information protection policies.[111] According to this survey, the ratio of system and network security check and backup of important data has been increasing (see figure 18).

The ROK's experiences could be useful for other countries to refer to when establishing cyber attack prevention and response systems. Until the last few years, the ROK has been a follower, adopting the cybersecurity policies of other advanced countries, but it is increasingly positioned to become a pioneer.

Further Considerations

Due to Korea's tendency to focus on defense technologies and the fact that different agencies are responsible for different aspects of cybersecurity, the need for a systematic, national cybersecurity strategy was not given high priority. For years, there was no long-term plan or high-level coordinator capable of overseeing an effective national cybersecurity initiative. Instead, after each attack, narrow policy changes were adopted to improve incident response, based on the analysis and experiences with the recent attack.

But preparing to fight the last war does not provide better defenses against new and different threats. And in Korea, it has often seemed that the new policies were aimed primarily at responding to public sentiment and public opinion and showing that policymakers had learned from the postmortems after the incidents.[112] Policies and institutions focused only on recovery and defense from severe attacks, not on fundamental improvements to the legal base or addressing related constitutional issues. The establishment of a basic cybersecurity law or strategy to specify essential elements for cybersecurity functions for national security purposes has not been promoted, leaving uncertainty about the direction of cybersecurity policy at the national level, who coordinates cybersecurity policy, the roles and responsibilities by each department, the authority and resources available for rapid response and prevention against cyber threat, and the scope of information collection and sharing.

After recognizing the problem, the NIS, which has a key role in cybersecurity in public institutions, promoted the Basic Cybersecurity Act in 2016, but it was not enacted due to disagreements with other ministries about their roles and responsibilities, and public distrust of the intelligence agency. It wasn't until 2019 that the government established the first National Cybersecurity Strategy.

The NIS also promoted the preparation of related legislation but encountered opposition and ended up focusing on countermeasures. Time after time, there would be a push for new, far-reaching legislation, but the process would get bogged down, and momentum was lost. This is because there was a culture of "development first, security later," since IT development was judged to be more important, and policymakers had questions about whether cyber attacks were really serious or threatened national security. Worse, because the various strategy documents were not useful, after each new attack, the narrowly focused policy solutions and systems created resulted in a patchwork of overlapping policies and systems.[113]

Finally, there has been no response to instigators of cyber attacks. Through government-led investigations, the reason and background of attacks are evaluated, and if the culprit is North Korea, it is ROK practice to have it be publicly attributed. There are few cases of public attribution in the event of attacks from other countries. Indeed, to date, in cases unrelated to North Korea, no prosecution or separate sanctions have been imposed on the attackers. For example, South Korea has not publicly confirmed that the PyeongChang Olympics incident was due to a cyber attack originating from Russia. Nor have there been cases of public attribution or sanctions to help deter frequent cyber attacks originating from China.

There are various reasons specific to Korea for the absence of public attribution.[114] One is that the reliability of the results from investigations has been low because the technology to conduct these investigations has not been available in Korea and/or the Korean government has been unwilling to hire foreign computer forensics experts. Another is that there is simply no standing procedure in Korea for public attribution, especially when it comes to foreign actors other than North Korea. However, the ROK has shown willingness to take countermeasures in national cybersecurity strategy and is currently making efforts to identify culprits and prepare procedures for disclosure to deter cyber attacks.[115]

How Korea Can Improve Cyber Security Policy and Data Resilience

Korea clearly needs to overcome gaps in its cybersecurity policy in light of these challenges to its current policy approach and governance. Indeed, recent cyber attacks show the strengths and weaknesses of Korea's current cybersecurity capabilities.

The government needs to begin by changing its posture both to deter and to respond to future cyber attacks. Even though Korea has been the target of several large-scale cyber attacks, an analysis of twenty years of major cyber attacks reveals no evidence of active responses against the attackers. In the case of an attack that caused anxiety to the entire nation, such as the attack on KHNP, there was no diplomatic response or action taken to respond to the attackers at all, even though a government joint investigation team analyzed the malicious code and Internet Protocol data used in the attack and found the source.

This should change in the future. The Korean government has announced its willingness to actively respond to attacks that undermine public trust. And the goal of ensuring a proactive deterrent against cyber attacks was included in the National Cybersecurity Strategy in 2019. As part of this, the government announced plans to actively respond to all cyber attacks that infringe upon national security and national interests by concentrating national capabilities and acquiring effective means to analyze causes of cyber attacks and identify the culprits.

Such a proactive response to cyber attacks would be welcome: it can contribute to raising awareness of cybersecurity among decisionmakers—in both the public and private sectors—and to raising the priority of cybersecurity when crafting future policies.

Second, it is necessary to expand the government's effort to address issues of economic and security threats caused by cyber attacks. The Korean government's established policies focus on political and military security in response to cyber attacks. However, cyber attacks on Korean cryptocurrency exchanges to steal financial profits are increasing, as demonstrated by the recent attacks on of Coinrail (2018), Bithumb (2018), and Upbit (2019).[116] In addition, it was revealed that Korean universities were included in the cyber attacks when China took over IT systems used for marine science and technology research at three universities around the world in 2019.[117] Chinese cyber attacks to steal intellectual property from other countries are also increasing.[118]

This shows that although cyber attacks are not equivalent to war or armed attacks, they can still cause billions of dollars of economic harm or lead to the theft of critical intellectual property in peacetime, threatening Korea's economic security. For this reason, policymakers need to focus on economic, political, and military security in tandem. They must recognize that the internet and the cloud have become a space for military operations and that better defenses against cyber attacks are needed. In Korean cybersecurity policy, expanding the priorities for securing economic security and establishing cybersecurity policies that consider economic security seem to be ways to pursue effective benefits in establishing a cybersecurity framework.

Ultimately, Korea needs a national cybersecurity risk management system and many more concerted efforts to strengthen cybersecurity resilience in national public institutions. According to research by Specops Software, Korea ranked fifth in the world in terms of the number of cyber attacks between 2006 and 2020, and these attacks are occurring more and more frequently.[119] Korea is also highly dependent on electronic government, ranking second in the UN's 2020 Global E-government Development Index.[120] Since cyber defenses will never be bulletproof, it is necessary to build tolerance and strengthen resilience against cyber attacks in order to prevent and respond to cybersecurity at the national level.

Backup systems are essential to minimizing damage. A key part of improving cyber resilience of national public institutions is expanding the introduction of cloud solutions through the Cloud Service Assurance Program (CSAP). The CSAP supplies public institutions with private cloud services that have verified safety and reliability, and it has a similar purpose to the United States' Federal Risk and Authorization

Management Program. The scope of certification covers all cloud services for public institution work and services including assets (such as ICT systems, facilities, and so on), organization and management, operations, and support services. There are fourteen categories of control for certification, including cybersecurity policy and organization, supply chain management, and incident management.

If the cloud service is expanded in government agencies, high-quality security solutions (such as antivirus, intrusion detection, and response systems) can be made available at a low cost. In addition, strengthening the security of cloud computing systems can prevent damage and destruction of important data, which will contribute to resilience. This will help the Korean public sector ensure a more rapid response in the event of a future cyber crisis.

CHAPTER 3

A Korean Approach to Data Localization

NOHYOUNG PARK

Introduction

Access to and the sharing of data are increasingly critical to achieve digital transformation and data-driven innovation. In the last few years, countries have focused on "data governance," in particular how, where, and when data, including personal data, should be collected, stored, combined, and analyzed.[121] In June 2020, President Moon Jae-in of the Republic of Korea (hereinafter the ROK or Korea) announced the Digital New Deal to spearhead a forward-looking innovative economy. The Digital New Deal envisioned an accelerated transition to a digital economy by extensively digitalizing the national infrastructure while fostering the DNA—data, network, and artificial intelligence (AI)—ecosystem and non-face-to-face industries.[122] The government's new focus on data governance reflects both technological and social dynamics: the growing importance of global cloud computing services; the emergence of new, powerful big data and machine-learning algorithms; and increasing public concerns about data protection and cybersecurity.

Despite the growing need for access to data and the resulting economic and social benefits, data access and sharing have not realized their full potential due to ever-growing barriers to data access. Many countries have practiced data localization (also known as data localism or data nationalism), such as requiring data, particularly personal data, be stored and accessible inside their borders. This has certainly complicated cross-border data flows with the effect of restricting the development of digital economy. The privacy, data protection, and cybersecurity concerns used to justify data localization are real and important.[123]

Korea is often listed among those countries with significant data localization requirements.[124] Privacy or data protection is certainly a major driver of the controls on cross-border data flows in Korea. However, Korea joined the Cross-Border Privacy Rules (CBPR) system of the Asia-Pacific Economic Cooperation (APEC) in June 2017. Korea has been bolstering privacy protections and diminishing barriers to data flows among the APEC economies that joined the CBPR, including Canada, Japan, and the United States. This chapter focuses on the evolution of Korean policy of data protection and cross-border data flows by analyzing the relevant Korean laws.[125] It explores how Korea has been making efforts to balance between the use of personal data and the data protection internally and to successfully facilitate cross-border data flows.

The Korean Legal Framework for Data Protection and Privacy

Privacy and data protection in Korea are addressed generally by Articles 17, 16, and 18 of the Korean Constitution and specifically by various laws. These articles in the Korean Constitution track Article 12 of the Universal Declaration of Human Rights and Article 17(1) of the International Covenant on Civil and Political Rights: The privacy of citizens must not be infringed, all citizens must be free from intrusion into their place of residence, and the privacy of correspondence of citizens must also not be infringed. Although data protection or the protection of personal information is not explicitly stipulated in the Korean Constitution, in 2005, the country's Constitutional Court recognized the existence of the right to self-determination of personal information as a fundamental right.[126]

Over the last twenty years, several laws on privacy and data protection have been enacted in Korea that flow from these constitutional and legal strictures. Korea enacted the Personal Information Protection Act (PIPA) on March 29, 2011, which became effective on September 30, 2011. This was supposed to be Korea's general law on data protection as it applied to the processing of personal information in both the private and public sectors.[127] However, the Act on Promotion of Information and Communications Network Utilization and Information Protection (known as the Network Act) in 2016 ultimately had a larger impact on the private sector because it applies to the protection of personal information processed by information and communications service providers in the internet environment. Through the so-called three data laws' amendment adopted by the National Assembly on January 9, 2020, the PIPA has become at last a truly general law on data protection by taking those provisions on data protection under the Network Act.[128]

Korea has adopted special laws on data protection covering different sectors or types of personal information (see table 10).

Table 10. Examples of Korea's Data Protection Laws Beyond the PIPA

Credit Information Act (CIA)	The Financial Services Commission (FSC) oversees credit information businesses and their compliance with the CIA and may order any company violating it to take corrective measures. The CIA has certain data protection provisions, which are special rules based on the PIPA. Although it applies only to the processing of personal credit information, the CIA, which covers financial and other related commercial transactions, is very important in practice.
Location Information Act (LIA)	The Korea Communications Commission (KCC) oversees businesses dealing with personal location information and their compliance with the LIA. The KCC may revoke the permission granted to a location information provider or a location-based service provider that violates the LIA through a cease-and-desist order on operations either for a certain duration or permanently.
Framework Act on Consumers (FAC)	The FAC requires a business entity to handle consumers' personal information in such a way that this information is not lost, stolen, leaked, altered, or damaged.
Medical Service Act (MSA)	The MSA stipulates that no person may trace, divulge, alter, or destroy personal information stored in an online prescription without good cause, and that medical personnel may not divulge or disclose personal information that they become aware of in the course of performing medical treatment.
Fair Hiring Procedure Act (FHPA)	The FHPA forbids hiring managers from demanding that a job applicant provide information that is not necessary for the job in the basic examination materials. Such information includes the applicant's physical condition, place of birth, marital status, and academic background, as well as information about their parents, children, and siblings.
Elementary and Secondary Education Act (ESEA)	Under the ESEA, the head of a school is prohibited from providing any third party with school records and health examination records without the consent of the relevant student or the student's guardian or parents.

Implementation of Korean Privacy and Data Protection Laws

The Personal Information Protection Commission

Through the three data laws' amendments of 2020, the Personal Information Protection Commission (PIPC) has become a genuinely independent supervisory authority, similar to those found in European Union (EU) countries under the General Data Protection Regulation (GDPR).[129] The PIPC sits under the Office of the Prime Minister and is charged "to independently conduct work relating to the protection of personal information."[130] The PIPC chairperson is subject to the direction and supervision of the prime minister, according to the president's orders. Nevertheless, the following missions are not subject to the prime minister's direction and supervision: matters concerning investigation into infringement upon the right of data subjects and the ensuing dispositions; the handling of complaints or remedial procedures relating to personal information processing and mediation of disputes over personal information; and matters concerning the assessment of data breach incident factors.[131]

Balancing the Use and Protection of Personal Information

The PIPA purports to protect personal information. Its purpose is "to protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information."[132] Like many data protection laws around the world, the PIPA was enacted by referring to the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which are regarded as model data protection principles in most countries. Unlike the OECD guidelines, the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data (108 Convention) of the Council of Europe and the GDPR, however, the purpose of the PIPA does not explicitly mention the use or cross-border flows of personal information.[133] The PIPA has been dubbed "Asia's toughest data privacy law" by the scholars Graham Greenleaf and Whon-il Park, as it tilts the balance in favor of the protection of personal information.[134]

Still, the approach to and the level of data protection provided in the PIPA have been criticized for obstructing the advancement of the Fourth Industrial Revolution, which relies on big data analytics and artificial intelligence. Thus, the revision of the legislative framework for data protection has been a hotly debated part of regulatory and institutional reforms suggested by the Presidential Committee on the Fourth Industrial Revolution (PCFIR). There were several hackathons and deliberations by the PCFIR to reform data protection laws in early 2018. The results were reflected in the amendment to major laws relating to data protection introduced in the National Assembly on November 15, 2018. The three data laws' amendment enacted in February 2020 expanded the PIPA and gave the PIPC independent and stronger enforcement powers. Yet industry representatives used the slogan of the Fourth Industrial Revolution and blocked the efforts of nongovernmental organizations trying to stick to stronger protection of personal information.[135] It remains to be seen whether the application and implementation of Korean data protection laws (including the PIPA) will really encourage more active and innovative use of personal information.

Korea has not been an island in developing its data protection regime. Indeed, Korean laws on data protection have developed by referring to the international documents as well as foreign laws like the European Union's GDPR. Through the three data laws' amendment, for example, new concepts like pseudonymization were adopted by the PIPA and the Credit Information Act, and data portability by the latter law.[136] These concepts had already been introduced by the GDPR. Moreover, the PIPC is designed to be precisely the type of supervisory authority provided for in the GDPR, as Korea has been trying to meet the GDPR's adequacy criteria.[137] On March 30, 2021, the PIPC and the European Commission jointly announced the successful conclusion of the adequacy talks between Korea and the EU. The adequacy decision is expected to be made by the European Commission sometime in 2021.[138] The adequacy dialogue confirmed the high degree of convergence in data protection between Korea and the European Union. Achieving an adequacy decision from the European Commission may imply that

Korean laws on data protection will correspond to the developments of the GDPR if Korea intends to keep an adequacy status.

Cross-Border Transfer of Personal Information and Data Localization Under Korean Laws

Korea's data protection laws, including the PIPA, constrain any company or government agency wishing to transfer personal information outside Korea. The data, other than personal information, is protected under the laws governing intellectual property in Korea.[139] The U.S. government and industry have argued that the restrictions the PIPA imposes on the transfer of personal information outside of Korea are too strict, and this has become a subject of contention between the two countries.[140]

Cross-border transfer of personal information may be classified into two types for regulatory purposes: providing personal information to third parties abroad and outsourcing personal information processing abroad. In most cases, providing personal information to third parties is conducted for the benefit of the transferee, while outsourcing of personal information processing is conducted for the benefit of the transferor.[141] The differences between the two types of cross-border transfer are substantial, especially for the personal information of information and communications service users (hereinafter IT service users). The prior consent of and some form of notice to IT service users are required for providing personal information to third parties abroad, whereas outsourcing does not necessarily require prior consent of IT service users.[142] For outsourcing the processing of personal information, the notice and consent may be replaced, inter alia, by the posting of the required notice in the controllers' privacy policies.[143]

Providing Personal Information to Third Parties Abroad

Under the PIPA, when providing data subjects' personal information to third parties abroad, the controller must obtain the prior consent of those data subjects.[144] To do this, a controller must follow the same procedure used to notify data subjects about how their personal information might be transferred to domestic third parties. In both cases, data subjects must be notified: the entity to which the personal information is provided; the purpose of using the personal information by the entity to which such information is provided; the particulars of the personal information to be provided; the period of time when the personal information will be used and retained; and the fact that the data subject is entitled to refuse consent, and the disadvantages, if any, resulting from the refusal to give consent.[145] These requirements are regarded to be "stringent" on service providers seeking to transfer customer data outside Korea.[146]

Transferring IT Service Users' Personal Information Abroad

The PIPA has special provisions applying to the transfer of personal information abroad by information and communications service providers (hereafter IT service providers).[147] Thus, the general provisions applicable to providing personal information to third parties abroad, as provided in Article 17(3), do not apply to transferring personal information of the IT service users abroad. IT service providers must obtain IT service users' consent if they intend to provide, outsource the processing of, or store IT service users' personal information abroad. IT service providers must notify IT service users of the following information in advance before obtaining such users' consent: the particulars of the personal information to be transferred; the country to which the personal information is transferred, the date of transfer, and transfer methods; the name of the entity to which the personal information is transferred; and the purpose of using the personal information and the period of retaining and using such personal information by the entity to which such information is transferred.[148]

IT service providers must implement safeguards as prescribed by the Enforcement Decree of the Personal Information Protection Act (hereinafter Presidential Decree 30892) if they intend to transfer the personal information of IT service users abroad with the prior consent of the latter.[149] The safeguards to be implemented are measures to ensure the safety for protecting personal information in accordance with internal management plans, measures to handle the complaints relating to data breach and dispute resolution, and other measures necessary to protect IT service users' personal information.[150] IT service providers intending to transfer personal information abroad must in advance consult the safeguards mentioned above with the entity to which such information is transferred and reflect them in the terms of any contract.[151]

IT service providers need not obtain IT service users' consent to outsource the processing of or storage of such personal information. However, if all the items, which must be notified to IT service users, are made public in the privacy policy of the IT service providers or if the IT service users are notified using a method such as email, or by another method prescribed by Presidential Decree 30892, including written notices.[152] IT service providers must obtain IT service users' consent, however, when providing, including accessing, IT service user's personal information to third parties abroad.

Onward Transfer of IT Service Users' Personal Information to a Third Country

The entity to which the personal information of IT service users is transferred, when transferring such information to a third country, must comply with the provisions of the PIPA applicable to transferring such information abroad.[153] Thus, for the onward transfer of IT service users' personal information, Articles 39-12 (1 through 4) for the cross-border transfer of personal information discussed above must be observed by such IT service providers transferring to another third country. The data protection during onward transfer is an element for the adequacy decision by the European Commission.[154]

Designation of Domestic Agents

IT service providers with no address or business office in Korea that meet the criteria prescribed by Presidential Decree 30892 must designate a domestic agent in writing.[155] A foreign IT service provider is required to designate a domestic agent if it has sales for the preceding year that reached or exceeded 1 trillion Korean won, roughly equal to $890 million; its sales from IT services for the preceding year reached or exceeded 10 billion Korean won, roughly equal to $8.9 million; it stored or maintained at least 1 million domestic users' personal information on an average daily basis over the three months immediately before the end of the preceding year; or it caused or is likely to cause a data breach incident in violation of the PIPA and was required by the PIPC to submit relevant articles, documents, and so on as part of an investigation.[156]

On behalf of the IT service provider, the domestic agent does the following: fulfilling the role of a data protection officer; notifying and reporting data breaches, including the loss, theft, or divulgence of personal information; and submitting related articles, documents, and so on when required by the PIPC.[157] If the domestic agent violates the PIPA, its IT service provider is deemed to have committed such a violation.[158] A domestic agent must have an address or business office in Korea.[159] When a domestic agent is designated, contact information for the agent must be included in the privacy policy.[160] Through the designation of a domestic agent, the PIPA may have de facto extraterritorial effect by indirectly controlling those foreign IT service providers abroad.[161]

Reciprocity and the Transfer of Personal Information Abroad

When implementing data protection laws, countries must deal with a tension between the desire to encourage the inbound cross-border data flows and the need to ensure their citizens' personal data is protected at home and abroad. Countries with equivalent levels of data protection will allow and encourage cross-border data flows between each other.[162]

Recently, countries like China, Russia, and Vietnam have restricted cross-border flows of personal information. In reaction to these actions, Korea has embraced the reciprocity principle to encourage and enable the cross-border transfer of personal information. Thus, personal information may not be allowed to be transferred to foreign IT service providers located in a country that restricts the transfer of personal information abroad.[163] This provision was designed to respond to the different levels of data protection in different countries. However, the requirement of reciprocity is not applicable when the transfer of personal information abroad is necessary to implement a treaty or other international agreement.[164] The proper application of the reciprocity principle would require detailed internal guidelines so as not to impair bilateral relations with those countries to be subject to the restrictions applied by Korea. Although there needs to be a flexible and reasonable response to other countries' restrictions on cross-border flows of personal information, there must be clear guidelines for the reciprocity principle to apply consistently and proportionately. The implementation of the reciprocity principle is also to be added to the missions of the PIPC.

Export of Location-Based Data Disputed by the United States

The Act on the Establishment, Management, etc. of Spatial Data (Spatial Data Act) prescribes matters concerning the standards and procedures for the surveying of land and waterways as well as the preparation, management, and so on of cadastral records and comprehensive real estate records.[165] The Spatial Data Act has a provision that may affect the cross-border transfer of information, particularly location-based data. No person can take abroad the results of a fundamental land survey: when it is likely to harm national security (or other important national interests) or when the land survey data are confidential as defined by other statutes.[166] In addition, no person can take abroad the results of a publicly available survey in cases where it is likely to harm national security (or other important national interests) or where the data are confidential.[167] Nevertheless, a consultative body may make a decision to allow the results of a fundamental survey to be taken abroad after the national security implications of doing so are considered.[168]

There is no general legal prohibition on exporting location-based data in Korea. Nevertheless, Korea has not approved the exportation of location-based data, although there have been numerous applications by foreign suppliers.[169] U.S. companies, including Google, seeking approval to export location-based data in order to offer competitive mapping and navigation services, have argued that Korea is linking such approval to individual companies' willingness to blur satellite imagery of Korea on their global mapping service sites for national security concerns.[170] As a matter of fact, Article XXI of the General Agreement on Tariffs and Trade (GATT) provides for the security exceptions, which are supposed to be judged by the claiming World Trade Organization (WTO) member itself.[171] Nevertheless, the United States argues that Korea is the only significant market in the world that maintains such restrictions on the export of location-based data.[172]

Cross-Border Transfer of Personal Information and Data Localization Under Korean Foreign Trade Agreements

Korea has been an assertive player in negotiating bilateral, plurilateral, and multilateral trade agreements. As such, it has negotiated some data-specific provisions that have influenced, or been influenced by, its domestic paradigm. Since the conclusion of its first free trade agreement (FTA) with Chile in 2003, Korea has concluded twenty-one FTAs.[173] The Korea-Chile FTA does not have provisions on cross-border data flows and data localization as such, but its subsequent FTAs generally do. Those data localization provisions, except for the Regional Comprehensive Economic Partnership (RCEP), address the location of computing facilities in the context of financial services.

Under the Korea-EU FTA and the Korea-U.S. FTA, Korea expressed its intent to undertake modification to its regulatory regime that will result in its adoption of approaches that will permit the transfer of financial information across borders while addressing such areas as the protection of sensitive information of consumers, prohibitions on unauthorized reuse of the sensitive information, the ability of financial regulators to have access to records of financial service suppliers relating to the handling of such information, and requirements for the location of technology facilities.[174]

Under the Korea-U.S. FTA, the parties recognize the importance of the free flow of information in facilitating trade, and thus they must endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.[175] This "endeavor" obligation for free flows of electronic information across borders, although not being directly binding, must be a commitment by the parties, in principle, to not impose data localization requirements. Notably, there are no provisions on data localization in the Korea-China FTA. The rigid requirements of data localization provided in China's various laws and regulations may explain why no provision was agreed on data localization in the Korea-China FTA.[176]

The RCEP includes provisions on the location of computing facilities in Chapter 12 on electronic commerce.[177] First, the parties recognize that each party may have its own measures regarding the use or location of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.[178] Second, any party must not require a covered person to use or locate computing facilities in that party's territory as a condition for conducting business in that party's territory.[179] Third, a party is not prevented from adopting or maintaining any measure inconsistent with the obligation not to require the use or location of computing facilities that it considers necessary to achieve a legitimate public policy objective.[180] The measure taken above must not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.[181] In addition, a party is not prevented from adopting or maintaining any measure that it considers necessary for the protection of its essential security interests.[182] Such measures must not be disputed by other parties.[183] Thus, the essential security interests may work as a definite and decisive excuse for adopting or maintaining the measures regarding the use or location of computing facilities.

Lessons From Korea's Experience

Korea has become a major manufacturing powerhouse and, like other countries, seeks to anchor its next economic surge in the deployment of data and the development of a digital economy. To make breakthroughs in the Fourth Industrial Revolution and cultivate new industries and growth paths, Korea has adopted several national strategies and policies to fully use data including personal information. Thus, the Personal Information Protection Act was recently amended to cover pseudonymization of personal information to facilitate more use of personal information, following the example of the EU's GDPR. Korea has also supported free cross-border flows of personal information in the development of digital trade rules in the WTO and the G20 as well as its FTAs.

Korea needs more good quality data, including personal information, ready and fit for uses in the global digital economy. This means Korea needs both stronger data protection within its borders and free cross-border data flows with limited data localization requirements outside its borders.

The challenge, then, is that Korea needs to keep its data protection laws effective to protect data subjects while enabling more use of personal information and developing the digital economy. The digital economy can develop stably only with the trust of customers or clients who willingly provide their personal information. The good news is that after four years of negotiation, the European Commission is expected to make an adequacy decision in Korea's favor later in 2021, as it already issued a draft decision on the adequate protection of personal data by Korea on June 14, 2021. After the PIPA is formally recognized to have an equivalent level of data protection to the GDPR, Korea will be able to import more good quality personal information from the EU. And, in a sense, the EU, for its part, will be able to export its data protection rules to Korea. Korea's data protection laws, including the PIPA, are very likely to be affected by the developments in the EU.

Data protection laws protect data subjects in processing their personal information. Data protection is considered a fundamental right both in the EU and in Korea. Thus, the collection and use of personal information must be based on the consent of data subjects in principle from the perspective of the right to self-determination of personal information. However, the consent of data subjects is not given priority in comparison to other legal bases for the collection and use of personal information both in the EU and in Korea. Critics of Korean privacy laws argue that Korea allows the cross-border transfer of personal information only upon the consent of the data subjects concerned. This rule in the PIPA would indeed restrict the cross-border transfer of personal information, but the PIPA is expected to be amended later in 2021 to cover other legal bases for cross-border transfer of personal data, like those in the GDPR. As the PIPA has the reciprocity principle to discourage the restriction of the cross-border flows of personal information, Korea will have to facilitate the outbound flow of personal information.

Privacy and data protection and cybersecurity in the digital economy need to be understood in a different way from the current WTO rules, which were negotiated and agreed without knowing the digital economy or trade in data properly. These concepts have been an important exception to free trade in the GATT and the General Agreement on Trade in Services (GATS), but in the digital economy and digital trade, privacy and data protection are important to obtain and sustain the trust of individuals. Cybersecurity is also important to protect the flows of data. Thus, privacy and data protection and cybersecurity are to be recognized as essential elements positively supporting the stable operation of digital trade where data, including personal information, flows cross country borders. In this respect, privacy and data protection and cybersecurity measures should not be viewed as unjustifiable or unreasonable causes of data localization, although they must not be unjustifiably misused or abused intentionally.

The problem is that there are not yet international agreements governing privacy and data protection, on the one hand, and cybersecurity, on the other. Indeed, there is a conspicuous gap in data protection levels even between democratic allies such as the United States and EU countries. Even after almost twenty years of negotiation on cybersecurity in the United Nations, there is no hope of reaching an international agreement in the near future.

One of the main tacit purposes of the GATT and the GATS was a need for governments not to interrupt international free trade by prescribing what they are allowed to do or not. Likewise, there is a good and urgent need for an international agreement for digital trade where governments are not allowed to unjustifiably interrupt cross-border flows of data. Privacy and data protection and cybersecurity are most common and plausible justifications that governments may raise for the sake of human rights and national security, respectively. Thus, a plurilateral agreement on trade-related aspects of electronic commerce, or on digital trade, being negotiated in the WTO can only be successful if it covers privacy and data protection and cybersecurity sufficiently to support digital trade or trade in data. Then, it seems that the digital trade provisions in the RCEP would affect the negotiations of digital trade rules in the WTO, as China is a major supporter of those provisions on its own. It remains to be seen whether the digital trade provisions to be agreed in the WTO would advance further in favor of free cross-border data flows than those of the RCEP. Newly negotiated digital trade rules of the WTO must be better than the United States-Mexico-Canada Agreement (USMCA), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and the RCEP in dealing with privacy and data protection and cybersecurity at least in the context of digital trade.

Considering that many contracting parties to both the RCEP and the CPTPP are in the same boat, the difference in forging a way forward may come from countries that become first-movers. In a sense, China was the driving force behind the rather restrictive digital trade rules in the RCEP, while the United States was the driving force of the rather free digital trade rules in the Trans-Pacific Partnership agreement, the forerunner to the CPTPP. Korea has to push this debate and rule-making process forward. After all, the RCEP and its digital trade rules, in particular, may not satisfy Korea's desire to develop digital trade. Thus, Korea needs to go further. For one, it must join the CPTPP in order to benefit from its much freer digital trade rules. If the United States also joins, the CPTPP may become a more influential instrument for digital trade than the RCEP. And that is not all. Korea and its democratic trading partners must also be more ambitious in negotiating and agreeing to freer digital trade rules in the WTO. Those digital trade rules must have more meaningful and effective rules on privacy and data protection and cybersecurity to support the stable operation of digital trade even for a limited number of WTO members in the beginning.

Korea has an important role to play in this effort because it has successfully developed data protection laws over the past ten years. And the impending PIPA amendment will further facilitate the use of personal information by adopting new elements like data portability and the right to respond to automated decisions. The PIPA amendment will also cover other legal bases for cross-border transfer of personal information in addition to the consent of data subjects. In this way, Korea, both by its own example and as a prospective leader in plurilateral and multilateral trade negotiations, could drive forward a new architecture of digital trade including data localization rules.

Acknowledgments

I would like to express my deepest appreciation to the Carnegie Endowment for International Peace, in particular Tim Maurer for inviting me to write the chapter, Evan Feigenbaum for encouraging the conduct of research, Michael R. Nelson for giving me good suggestions after a thorough review, and Alexander Taylor for taking care of administrative matters.

AFTERWORD

Korea's Challenge to the Standard Internet Interconnection Model

KYUNG SIN "KS" PARK AND MICHAEL R. NELSON

The development of the data economy in Korea could not have succeeded without high penetration of affordable, high-speed broadband networks.[184] This spurred innovation by the largest computer, telecom, and consumer electronics companies and by startups and universities. Unfortunately, over the last five years, new telecommunications regulations threaten to decrease competition among network providers and increase the cost of connectivity—particularly for access to non-Korean content and services. These include cloud computing and storage, which as mentioned in earlier chapters, are key parts of any strategy to improve cybersecurity and cyber resilience.

The network infrastructure that enables the internet has expanded so rapidly over the last two decades for two simple reasons: competition and interconnection. Companies running networks have had huge incentives to connect each other's customers, which has meant that often network providers simply agree to connect their networks for free. In other cases, where a small network provider wants to reach the customers and services on a much larger network, they negotiate a price for interconnection and transit. That is the way the internet has worked almost everywhere—enabling fair and vigorous competition. The result is a global network of networks that connects more than 4 billion customers to each other and to a phenomenal variety of different services and websites.

However, there *have* been some attempts to "mess with success," and Korea's experience is among them. In particular, starting in early 2016, the Korean telecommunications regulator has mandated "network use fees." These new fees would flip the entire business model of the internet—and were designed to favor the three large telecommunications companies that most Koreans depend upon. Understandably, these companies have lobbied hard for this new scheme, which rather than having individual users and businesses pay to connect to the internet and access the full range of content and services available there, would require providers of services to "pay by the bit" for the traffic generated when their customers download content. The established practice—where users, companies, and individuals alike are not charged for the bits they send or receive but only for maintaining physical access to the network ("Bill and Keep")—would be replaced with a "Sending Party Network Pays" (SPNP) model.

Although this change is being applied selectively (for example, only among internet service providers, ISPs, for now), it is already having a notable impact on the future of data and internet usage in Korea—increasing the cost of broadband and causing some companies, such as Facebook and Netflix, to suspend or degrade the services they provide to Korean customers rather than pay the new, artificially high charges for interconnection demanded by Korea's big three ISPs.

Even before the SPNP rule kicked in, the market for mobile broadband in Korea was dominated by three big ISPs, resulting in the second-lowest level of competition in the mobile market (as measured by HHI,[185] a standard measure of market concentration) among the large, developed countries (those with a population of more than 20 million).[186] These Korean SPNP rules will reduce competition further.

According to TeleGeography, the cost of transit in Seoul is typically eight to ten times that of major European network hubs like London and Frankfurt.[187] Elsewhere in Asia, technological improvements in optical fiber network technology and vigorous competition are leading the cost of transit to fall about 20 percent per year.[188] That is simply not happening in Korea, in part due to the added costs imposed by these interconnection fees.

Therefore, many Korean content providers cannot handle the higher cost for hosting their content in Korea and have either moved overseas or were outcompeted by foreign content providers because Korean firms cannot provide speed-intensive content, such as 4K video. As a result, Korean consumers are shifting to foreign content providers.

Unfortunately, the Korean government has not learned lessons from other attempts to switch to a SPNP model, particularly in Europe. In 2012, the European Telecommunications Network Operators (ETNO) group suggested that the United Nations' International Telecommunication Union recommend that national governments adopt the SPNP model. The reaction to this proposition was rapid and unequivocal. The Body of European Regulators for Electronic Communications (BEREC) rejected the whole idea of trying to regulate interconnection costs because "ETNO's proposed end-to-end SPNP approach to data transmission is totally antagonistic to the decentralized efficient routing approach to data transmission of the Internet. The connection-oriented nature of end-to-end SPNP, with its focus on charging based on the actual volumes or value of the traffic, would represent a dramatic change from the existing charging framework operating on the Internet."[189] Additionally, BEREC stated that "If 'bill & keep' were to be replaced by SPNP then the ISP providing access could exploit the physical bottleneck for traffic exchange and derive monopoly profits, requiring regulatory intervention." Basically, these regulators concluded that the ETNO proposal would threaten the market's ability to sort out how much each network pays other networks to accept its customers' traffic. As a result, the ETNO proposal went nowhere.

In Korea, several content companies and smaller network providers are fighting the three big Korean telecoms champions in court—and usually losing.[190] Unless this policy is revised, over time it will decrease investment in network infrastructure and slow the digital transformation in Korea.

But unfortunately, the situation is getting worse (and messier) not better. Rather than reversing course, in May 2020, Korea's National Assembly approved the Content Providers' Traffic Stabilization Law, which goes beyond the SPNP rules adopted by the country's telecommunications regulator. This new law not only set interconnection charges for network providers (and further favored the three large Korean telecommunications companies) but also required large content providers to shoulder the responsibility of ensuring reliable access to their content, which had been the responsibility of ISPs everywhere else.[191] In addition, in December 2020, assembly member Jun Hye-sook of the Minjoo Party proposed an amendment to the Telecommunication Business Act (bill no. 2106370) to prohibit "acts to unduly impose unreasonable or discriminatory conditions or restrictions in agreements for the use or provision of telecommunication networks." The bill's provisions, if adopted, could extend and entrench the SPNP model even further.

Korea has been considered a model country with a high internet penetration rate and dense fiber network penetration, but these new laws could make it more difficult for Koreans to fully enjoy the global services they access today, including not just video services but also content distribution networks, cloud services, and cybersecurity tools that make the internet faster, more reliable, and more secure. The new laws will also hold back new Korean telecoms startups trying to compete with the established network providers. Worse, the laws are creating a dangerous precedent that other countries might seek to emulate, slowing internet development and harming consumers there, too. (An attempt in Indonesia was recently nipped in the bud.[192]) This is why more than a dozen civil society organizations have called on the government of Korea to repeal the new Content Providers' Traffic Stabilization Law and the SPNP rule. They include Open Net Korea (in South Korea), Access Now, European Digital Rights (EDRi), Article 19, and other groups from Brazil to Norway to Mexico.[193]

About the Authors

EVAN A. FEIGENBAUM is a vice president for studies at the Carnegie Endowment for International Peace, where he oversees research in Washington, Beijing, and New Delhi on a dynamic region encompassing both East Asia and South Asia. He was also the 2019–2020 James R. Schlesinger Distinguished Professor at the Miller Center of Public Affairs at the University of Virginia, where he is now a practitioner senior fellow.

Initially an academic with a PhD in Chinese politics from Stanford University, Feigenbaum's career has spanned government service, think tanks, the private sector, and three major regions of Asia. From 2001 to 2009, he served at the U.S. State Department as deputy assistant secretary of state for South Asia (2007–2009), deputy assistant secretary of state for Central Asia (2006–2007), member of the policy planning staff with principal responsibility for East Asia and the Pacific (2001–2006), and an adviser on China to deputy secretary of state Robert B. Zoellick, with whom he worked closely in the development of the U.S.-China senior dialogue. Following government service, Feigenbaum worked in the private and nonprofit sectors. He was vice chairman of the Paulson Institute at the University of Chicago and the co-founder of MacroPolo, its digital venture on the Chinese economy; head of the Asia practice at the markets consultancy Eurasia Group; and senior fellow for Asia at the Council on Foreign Relations.

Before government service, he worked at Harvard University as lecturer on government in the faculty of arts and sciences and as executive director of the Asia-Pacific Security Initiative and program chair of the Chinese Security Studies Program in the John F. Kennedy School of Government, and was lecturer of national security affairs at the U.S. Naval Postgraduate School. He is the author of three books and monographs, including *The United States in the New Asia* and *China's Techno-Warriors: National Security and Strategic Competition From the Nuclear to the Information Age*.

MICHAEL R. NELSON is a senior fellow in the Carnegie Endowment's Technology and International Affairs Program, which helps decisionmakers understand and address the impacts of emerging technologies, including digital technologies, biotechnology, and artificial intelligence. Prior to joining Carnegie, he started the global public policy office for Cloudflare, a startup that has improved the performance and security of more than 10 million websites around the world. Nelson has also served as a principal technology policy strategist in Microsoft's Technology Policy Group and before that was a senior technology and telecommunications analyst with Bloomberg Government. In addition, Nelson has been teaching courses and doing research on the future of the internet, cyber policy, technology policy, innovation policy, and e-government in the Communication, Culture, and Technology Program at Georgetown University.

Before joining the Georgetown faculty, Nelson was director of internet technology and strategy at IBM, where he managed a team helping define and implement IBM's next generation internet strategy. He has served as chairman of the Information, Communication, and Computing Section of the American Association for the Advancement of Science, serves as a trustee of the Institute for International Communications, and was selected to be a "Global Leader of Tomorrow" by the World Economic Forum. From 1988 to 1993, he served as a professional staff member for the Senate's Subcommittee on Science, Technology, and Space and was the lead Senate staffer for the High-Performance Computing Act. In 1993, he joined then vice president Al Gore at the White House and worked with president Bill Clinton's science adviser on issues relating to the Global Information Infrastructure, including telecommunications policy, information technology, encryption, electronic commerce, and information policy.

JANG GYEHYUN is a research professor at the School of Cybersecurity at Korea University. He earned his PhD in information security and a BE in industrial engineering from Korea University. Jang has contributed to numerous cybersecurity-related research projects in Korea. He has advised on Korea's national cybersecurity policy as a participant in research projects for the Presidential Advisory Council on Science and Technology, the Office of National Security in the Office of the President of the Republic of Korea (Cheongwadae), the Ministry of National Defense, the Joint Chiefs of Staff, and other ministries and agencies. He also has been involved in other research projects from institutions such as the National Security Research Institution and the Korea Internet and Security Agency. Jang lectures at Korea University and works as a mentor in the "Best of the Best" program, a training program for Korean cybersecurity talent. He has also published various articles in Korean journals on cybersecurity in the context of national security, security policies, and other issues, including online authentication.

LIM JONG-IN is a professor at the Graduate School of Information Protection and the Department of Cyber Defense at Korea University. In 2015, he served as the special adviser on cybersecurity to the Korean president. He currently chairs the Digital Investigation Advisory Committee of the Supreme

Prosecutors' Office and is also the chairman of the Financial Security Advisory Committee at the Financial Security Institute. He has been president of the Korea Association of Chief Information Security Officers and chairman of the Board of Academia for Information Security at Korea University's School of Information Security, where he has been a professor for thirty-three years. He holds three degrees from Korea University, including a doctorate in algebra.

SO JEONG KIM is a principal researcher for the National Security Research Institute. Since joining in 2004, she now leads the cybersecurity policy team and provides recommendations on cybersecurity policy and regulatory issues. She was involved in drafting South Korea's National Cyber Security Strategy, published in April 2019. She was also involved in the 4th and 5th UN Group of Governmental Experts as an adviser, and the MERIDIAN process as an adviser and organizer. Her main research area is national cybersecurity policy, specifically, international norm-setting processes, confidence-building measures, critical information infrastructure protection, law and regulations, and cybersecurity evaluation development.

SUNHA BAE received an MS degree in electrical engineering from the Korea Advanced Institute of Science and Technology in 2009. From 2009 to 2012, Bae worked for LIGNex1 in Korea's defense industry as a software engineer on a missile system, and from 2013 to 2014 for Doosan Heavy Industry as a software engineer on a power plant control system. In 2015, Bae joined the National Security Research Institute of Korea to conduct research on national cybersecurity policy. Bae's current areas of research interest are critical infrastructure cybersecurity strategy, and the assessment of national cybersecurity capability and cyber attack severity.

NOHYOUNG PARK has been a professor of law at Korea University Law School since 1990, where he has also been dean of the Law School and vice president. His background is in international economic law focusing on the WTO, but he also studies cybersecurity and data privacy, and negotiation and mediation. He is currently director of the Cyber Law Centre at Korea University, president of International Cyber Law Studies in Korea, and president of the Korean Society of Mediation Studies. He has advised governments and businesses on various international legal matters, including participating in the negotiation of Korea's first free trade agreement (Korea-Chile) and by attending the meetings of the fourth and fifth UN Groups of Government Experts between 2014 and 2017. He has pursued international research cooperation with various academic institutions in China, the EU, Japan, Russia, and the United States over cybersecurity, data privacy, digital trade, mediation, the Belt and Road Initiative, and the Nagoya Protocol.

KYUNG SIN "KS" PARK is a professor of law at Korea University. He served as a commissioner at the Korea Communication Standards Commission, a presidentially appointed internet content regulation body (2011–2014), and as a member of the National Media Commission, an advisory body to the National Assembly set up to examine the bills allowing media cross-ownership and other media and internet regulations. He is executive director for both Open Net Korea and PSPD Law—part of People's Solidarity for Participatory Democracy, a Seoul-based nongovernmental organization that promotes popular participation in government decisionmaking—which have pursued and won several high-profile legal cases and pushed for legislative action in the areas of freedom of speech, privacy, net neutrality, web accessibility, digital innovation, and intellectual property.

Introduction

[1] Debby Wu, Henry Hoenig, and Hannah Dormido, "Who's Winning the Tech Cold War? A China vs. U.S. Scoreboard," Bloomberg, June 19, 2019, https://www.bloomberg.com/graphics/2019-us-china-who-is-winning-the-tech-war/; DealBook, "Inside the New Tech Cold War," *New York Times*, October 1, 2020, https://www.nytimes.com/2020/10/01/business/dealbook/tech-cold-war-us-china.html; Adam Segal, "The Coming Tech Cold War With China," *Foreign Affairs*, September 9, 2021, https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china; Stu Woo, "The U.S. vs. China: The High Cost of the Technology Cold War," *Wall Street Journal*, October 22, 2020, https://www.wsj.com/articles/the-u-s-vs-china-the-high-cost-of-the-technology-cold-war-11603397438; and Robert D. Kaplan, "A New Cold War Has Begun," *Foreign Policy*, January 7, 2019, https://foreignpolicy.com/2019/01/07/a-new-cold-war-has-begun/.

[2] Jacob Poushter, Caldwell Bishop, and Hanyu Chwe, "Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones," Pew Research Center, June 19, 2018, https://www.pewresearch.org/global/2018/06/19/across-39-countries-three-quarters-say-they-use-the-internet/.

[3] Ryan Daws, "Research: These Countries Are the 'Most Connected' in the World," Telecoms Tech News, July 6, 2021, https://telecomstechnews.com/news/2021/jul/06/research-these-countries-are-the-most-connected-in-the-world/.

[4] White House, "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy," April 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[5] National Institute of Standards and Technology, "Identity & Access Management," U.S. Department of Commerce, accessed July 2021, https://www.nist.gov/identity-access-management.

[6] Bae Hyunjung, "South Korea's Trade Dependency Slips in 2019 Amid Sluggish Reports," *Korea Herald*, October 18, 2020, http://www.koreaherald.com/view.php?ud=20201018000119.

[7] World Integrated Trade Solution, "Country Snapshot: Republic of Korea," World Bank, accessed July 2021, https://wits.worldbank.org/countrysnapshot/en/KOR.

[8] Santander, "South Korea: Foreign Investment," accessed July 2021, https://santandertrade.com/en/portal/establish-overseas/south-korea/foreign-investment.

[9] Human Rights Watch, "Mobile Location Data and Covid-19: Q&A," May 13, 2020, https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.

[10] Alex Pentland, Alexander Lipton, and Thomas Hardjono, eds., “Building the New Economy,” MITP Works in Progress, accessed July 2021, https://wip.mitpress.mit.edu/new-economy.

[11] Born2Global Centre, “Ministry of Science and ICT Rolls out Digital New Deal to Leap Forward Into a New Economy Beyond COVID-19,” PR Newswire, June 15, 2021, https://www.prnewswire.com/news-releases/ministry-of-science-and-ict-rolls-out-digital-new-deal-to-leap-forward-into-a-new-economy-beyond-covid-19-301312248.html.

[12] Ovum Consulting, “Broadband Policy Development in the Republic of Korea: A Report for the Global Information and Communications Technologies Department of the World Bank,” October 2009, https://www.infodev.org/infodev-files/resource/InfodevDocuments_934.pdf.

[13] Ernesto Falcon, “Why Is South Korea a Global Broadband Leader?,” Electronic Frontier Foundation, March 16, 2020, https://www.eff.org/deeplinks/2020/02/why-south-korea-global-broadband-leader.

[14] “South Korea’s Network Infrastructure May Be State of the Art, but the Country’s ‘Pay to Play’ Regime for Delivering Traffic Is an Unprecedented Threat to the Free and Open Internet,” Open Net Korea, September 17, 2020, http://opennetkorea.org/en/wp/3122?ckattempt=3.

[15] Michael Kende and David Abecassis, “IP Interconnection on the Internet: a White Paper,” Analysys Mason, May 21, 2020, https://www.analysysmason.com/consulting-redirect/reports/ip-interconnection-korea-white-paper/.

[16] Kyung Sin Park, “The World’s Only Attempt to Legislate ‘Network Use Fees’ Will Further Damage Consumers – the Illusion of Charging ‘Delivery Fees’ on the Internet Will Disincentivize Investment in Network Expansion,” Open Net Korea, May 11, 2021, http://opennetkorea.org/en/wp/3265.

[17] Song Su-hyun, “[News Focus] Netflix’s Net Neutrality Logic Loses Ground in Korea,” *Korea Herald*, June 28, 2021, http://www.koreaherald.com/view.php?ud=20210628000798.

[18] Casey Corcoran, Bo Julie Crowley, and Raina Davis, “Disinformation Threat Watch the Disinformation Landscape in East Asia and Implications for US Policy,” Belfer Center for Science and International Affairs, 2019, https://www.belfercenter.org/sites/default/files/2019-06/PAE/DisinfoWatch%20-%202.pdf.

[19] Choe Sang-hun, “South Korea Declares War on ‘Fake News,’ Worrying Government Critics,” *New York Times*, October 2, 2018, https://www.nytimes.com/2018/10/02/world/asia/south-korea-fake-news.html.

[20] Charlotte Stanton, “How Should Countries Tackle Deepfakes?,” Carnegie Endowment for International Peace, January 28, 2019, https://carnegieendowment.org/2019/01/28/how-should-countries-tackle-deepfakes-pub-78221.

[21] Eric Horvitz, “A Promising Step Forward on Disinformation,” Microsoft on the Issues, February 22, 2021, https://blogs.microsoft.com/on-the-issues/2021/02/22/deepfakes-disinformation-c2pa-origin-cai/.

[22] Encryption Working Group, “Cyber Policy Initiative: Encryption Working Group,” Carnegie Endowment for International Peace, accessed July 2021, https://carnegieendowment.org/programs/technology/cyber/encryption.

[23] Digital Watch, “The G20 Osaka Track Raises Controversy,” July 1, 2019, https://dig.watch/updates/g20-osaka-track-raises-controversy.

[24] World Economic Forum, “Data Free Flow With Trust (DFFT): Paths Towards Free and Trusted Data Flows,” June 2020, https://www.weforum.org/whitepapers/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows.

[25] Scroll Staff, “G20 Summit: India Does Not Sign Osaka Declaration on Cross-Border Data Flow,” Scroll India, June 29, 2019, https://scroll.in/latest/928811/g20-summit-india-does-not-sign-osaka-declaration-on-cross-border-data-flow.

[26] OECD, “Broadband Portal,” last updated July 29,2021, https://www.oecd.org/sti/broadband/broadband-statistics/.

[27] Speedtest, “South Korea’s Mobile and Fixed Broadband Internet Speeds,” https://www.speedtest.net/global-index/south-korea#fixed.

[28] Economist Intelligence Unit, “The Asian Digital Transformation Index 2018,” http://connectedfuture.economist.com/wp-content/uploads/2018/12/ADTI-whitepaper.pdf.

[29] ITU, “ICT Development Index 2017,” https://www.itu.int/net4/ITU-D/idi/2017/index.html.

[30] Statista, “Penetration Rate of Smartphones in Selected Countries 2020,” https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/.

[31] UN Department of Economic and Social Affairs, “E-Government Survey 2020,” https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020.

[32] Statistics Korea, “Monthly Online Shopping Survey,” http://kostat.go.kr/portal/eng/surveyOutline/2/5/index.static.

[33] Kim Jee-Hee, “To Borrow Money, Koreans Go Online,” Korea JoongAng Daily, April 5, 2021, https://koreajoongangdaily.joins.com/2021/04/05/business/finance/bank-of-korea-internet-banking-mobile-banking/20210405163900371.html.

34 Korean Ministry of Land, Infrastructure, and Transport, "Ratio of Population in Urban Areas" (in Korean), Korean National Indicator System, last updated 2020, https://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1200.

35 Microsoft News Center, "Microsoft Korea Announces 'Cyber Security Threat Report'" (in Korean), June 18, 2018, https://news.microsoft.com/ko-kr/2018/06/18/cybersecurity-report/.

36 Yonhap News Agency, "Damage from N.K. Cyber Attacks Estimated at 860 Bln Won: Lawmaker," October 15, 2013, https://en.yna.co.kr/view/AEN20131015003200315.

37 Korea Times, "It's Urgent to Wage War on Cyber Terror," July 8, 2009, http://www.koreatimes.co.kr/www/news/opinon/2009/07/137_48133.html.

38 Sang-hee Han, Eun-Woo Lee, Byeong-il Oh, and Hyun-sik Yoon, "Status of the Usage of Resident Registration Numbers: Research Findings" (in Korean), National Human Rights Commission of Korea, 2005, https://www.humanrights.go.kr/site/inc/file/fileDownload?fileid=1055872&filename=05_78.pdf.

39 Min-ok Han, "12 Percent of Netizens 'Experienced Resident Registration Number Theft'" (in Koream), Digital Times, December 1, 2003, https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=105&oid=029&aid=0000049852.

40 Lee Kyung-min, "I-PIN Identification System Hacked," Korea Times, March 5, 2015, https://www.koreatimes.co.kr/www/news/nation/2015/03/116_174690.html.

41 Tae-jin Kim, "I-PIN Usage, 4 Percent Compared to Mobile Phone Authentication" (in Korean) October 9, 2017, ZD Net Korea, https://zdnet.co.kr/view/?no=20171009111654.

42 Public I-PIN, "Notice of Suspension of New Issuance or Renewal Due to Phase Out" (in Korean), October 31, 2018, http://www.gpin.go.kr/center/customer/noticeView.gpin?currentPage=2&no=27420.

43 Korea Communications Commission, "Three Companies Designated as Identity Verification Agencies by the Korea Communications Commission" (in Korean), December 28, 2012, https://kcc.go.kr/download.do?fileSeq=36847.

44 Kyung-ha Kwon, "Credit Card Identity Verification Service Method Policy Direction" (in Korean), Korea Communications Commission, October 20, 2016, https://kcc.go.kr/user.do?boardId=1008&page=A02020600&dc=&boardSeq=44056&mode=view.

45 Ministry of Information and Communication, "Portals With More Than 300 Users Daily…Limited Identity Verification" (in Korean), Korea Policy Briefing, February 23, 2007, https://www.korea.kr/news/pressReleaseView.do?newsId=155178693.

46 Yeong-ju Kim, "Businesses Subject to Limited Identity Verification System in 2009" (in Korean), Korea Communications Commission, January 30, 2009, https://kcc.go.kr/user.do?mode=view&page=A05030000&dc=&boardId=1113&cp=376&boardSeq=15512.

47 Jeong-hoon Lee, "Impact of the Decision on the Unconstitutionality of the Identity Verification System on Internet Regulation" (in Korean), Korea Internet and Security Agency, 2013, https://www.kisa.or.kr/uploadfile/201306/201306101706190871.pdf.

48 Kyeong-shin Park, "Constitutional Review of Anonymity Regulation and Review of 2015 Constitutionality Decision on Election Internet Real Name Law" (in Korean), Republic of Korea National Election Commission Election Studies 7, no. 1 (2016), https://www.nec.go.kr/common/board/Download.do?bcIdx=15433&cbIdx=1133&streFileNm=BBS_201701160247379835.pdf.

49 Ji-sook Woo, Hyeon-soo Na, Jeong-min Choi, "Empirical Study of the Effect of Using Real Names on Internet Bulletin Boards" (in Korean), Korean Journal of Public administration 48, no. 1 (2010), https://s-space.snu.ac.kr/bitstream/10371/69064/1/48-1_04%EC%9A%B0%EC%A7%80%EC%88%99_%EB%82%98%ED%98%84%EC%88%98_%EC%B5%9C%EC%A0%95%EB%AF%BC.pdf.

50 Hankyoreh, "Google Refuses South Korean Government's Real-Name System," April 10, 2009, http://english.hani.co.kr/arti/english_edition/e_international/349076.html.

51 Hankyoreh, "YouTube Korea Now Exempt From Real Name System," April 7, 2010, http://english.hani.co.kr/arti/english_edition/e_national/414784.html.

52 Constitutional Court of Korea, Decision on case number 2010 Heon Ma 47, 252 (consolidated). Hosted by Open Net Korea. See: http://opennetkorea.org/en/wp/wp-content/uploads/2014/03/Korean-real-name-law-decision-english.pdf.

53 Kyung Sin Park, "Establishing Game Users' Constitutional Right in Light of the Constitutional Court's Recent Decisions on Game Shutdown Case and Game Real Name Case," Korea Citation Index, 2020, https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002561011.

54 IT Find, "Market Trends by E-Commerce Business Type" (in Korean), https://www.itfind.or.kr/WZIN/jugidong/933/93303.html.

55 Korea Internet Security Agency, "Authorization Practices" (in Korean), https://www.rootca.or.kr/kor/accredited/accredited01.jsp.

[56] Yeong-Kwan Song, “2016 Modularization of Korea’s Development Experience: Korea’s E-Commerce Policy Experiences,” Knowledge Sharing Program, 2016, https://www.ksp.go.kr/api/file/download/11457?downloadFilename=Korea%E2%80%99s%20E-commerce%20Policy%20Experiences%20(English).pdf.

[57] Joon-kyung Geum, “Moon Jae-in Highlights the Core of His Promise to Abolish Authorized Certificates” (in Korean), Media Today, http://www.mediatoday.co.kr/news/articleView.html?idxno=135414.

[58] Financial Services Commission of Korea, “(Q&A) After Abolishing the Authorized Certification System on December 10, How Will Financial Transactions Be Different?” (in Korean), Korea Policy Briefing, December 11, 2020, https://www.korea.kr/news/visualNewsView.do?newsId=148880842.

[59] Information Disclosure Center, “When Will the Continuous Omission of Target Organizations in the Information Disclosure Annual Report Be Improved?” (in Korean), February 5, 2018, https://www.opengirok.or.kr/4555.

[60] Bong-su Kim, “In the Government 3.0 Era, the Trap of ‘Information Disclosure Rate of 95%’” (in Korean), Asian Economy, July 8, 2013, https://cm.asiae.co.kr/article/2013070810494738241.

[61] Information Disclosure Center, “When Will the Continuous Omission of Target Organizations in the Information Disclosure Annual Report Be Improved?”

[62] Ministry of Interior and Safety, “Government 3.0 Basic Plan” (in Korean), June 19, 2013, https://mois.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000027748&fileSn=0.

[63] Ministry of Government Administration and Home Affairs, “2020 E-Government Basic Plan” (in Korean), 2016, https://www.mois.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000791371GzYtix&fileSn=0.

[64] Korea Data 119 Project, “Presidential Committee on the Fourth Industrial Revolution of Korea,” 2021, https://www.4th-ir.go.kr/article/download/757.

[65] IMD, “IMD World Digital Competitiveness Ranking 2017,” https://www1.imd.org/globalassets/wcc/docs/release-2017/world_digital_competitiveness_yearbook_2017.pdf?MRK_CMPG_SOURCE=sm_lk_pp_wall_sv_exp.

[66] Korea Data Industry, “2017 Data Industry White Paper” (in Korean), July 12, 2017, https://www.kdata.or.kr/info/info_02_download.html?dbnum=224.

[67] Kyung-hwan Kim, “Issues of Cross-Border Data Transfer and the Countermeasures” (in Korean), PIS Fair, 2013, https://www.slideshare.net/ssuserbd0159/l-49862245.

Chapter 2

[68] Korea has been making continuous efforts to realize an information society, first introduced the internet in 1982, and commercialized it in 1994. NIS, “National Cybersecurity White Paper 2004” (in Korean), 2004, p. 3.

[69] Awareness of information protection has increased across the country, including government agencies and telecommunication companies after the 2003 internet disruption. NIS, “National Cybersecurity White Paper 2004” (in Korean), 2004, pp. 6–7.

[70] OECD, “Declaration for the Future of the Internet Economy (The Seoul Declaration),” OECD/LEGAL/0366, adopted on June 17, 2008.

[71] “Seoul Framework for and Commitment to Open and Secure Cyberspace,” United Nations, 2013, https://www.un.org/disarmament/wp-content/uploads/2019/10/ENCLOSED-Seoul-Framework-for-and-Commitment-to-an-Open-and-Secure-Cyberspace.pdf.

[72] JinKyu Kang, “NIS, National Cyber Security Strategy to Be Implanted in the Second Half of Year,” Digital Times, June 11, 2009, https://www.dt.co.kr/contents.html?article_no=2009061202010560739004.

[73] The National Security Research Institute has hosted the GCPR since 2014 five times with NCSC and Ministry of Foreign Affairs (three times).

[74] Sea Min, “Significantly Strengthen National Cybersecurity” (in Korean), BoanNews, March 18, 2015, https://www.boannews.com/media/view.asp?idx=45697&kind=2.

[75] NIS et al., “White Paper on Information Security 2004” (in Korean), 2004, p. 7.

[76] From 2015 to 2018, the NSC designated the cybersecurity adviser to lead the cybersecurity efforts nation-wide, however, this position was merged with the cyber information convergence adviser under the same NSC.

[77] NIS et al., “White Paper on Information Security 2021” (in English), 2021, p. 64.

[78] The NCSC investigates the causes and attack vector of cyber incidents that occur in the national computer network and shares information to prevent and respond to cyber attacks in the public sector.

[79] Most critical infrastructure in the ROK is owned by public institutions and is operated by the government. In fact, the Korean government continued to promote the privatization of public enterprises to enhance the competitiveness of public institutions, and as a result, some infrastructure such as finance, power generation, telecommunications, airports, and transportation were privatized. However, due to various problems such as resistance from stakeholders and lack of information on the privatization of public enterprises, partial privatization happened rather than absolute privatization, and in many cases, the ownership could not be transferred. As a result, the company manages and operates

the infrastructure, but the government budget is injected and the government can intervene in the management. As a result, the government is leading efforts for infrastructure cybersecurity, but management and operating companies are also actively participating in the development and implementation of government policies.

[80] Supra note 12, p.6.

[81] National Security Office of Cheong Wa Dae, "National Cybersecurity Strategy" (in Korean), April 2019.

[82] National Security Office of Cheong Wa Dae, "National Cybersecurity Basic Plan" (in Korean), September 2019.

[83] In English, the NCSC has been represented as the National Cyber Security Center, however, it was originally named the National Cyber Safety Center. This has resulted in some confusion about the NCSC among Koreans.

[84] Kum Hyun, "How Did Security Become 'Security' (An-bo in Korean)? Focusing on the Process of Transition to 'Safety' (An-jeon in Korean), 'Ensure Security' (An-Jeon Bo-Jang in Korean), and 'Security' (An-bo in Korean)," *Korea Journal of International Relation* 60, no. 4 (2020): 41–77.

[85] The National Cyber Security Management Decree defines as follows: The term "cyber attack" means any attack that illegally invades, disrupts, paralyzes, destroys, or intercepts information on the national information and communications network by electronic means, such as hacking, computer viruses, logic bombs, mail bombs, service interruptions, etc. The term "cyber safety (security)" means the state of maintaining stability, such as the confidentiality, integrity, availability, etc. of national information and communications networks by protecting the national information and communications network from cyber attacks. The term "cyber crisis" means a situation in which information distributed and stored through information and communication networks from cyber attacks is leaked, changed, or destroyed, affecting national security, creating social and economic chaos, or undermining or suspending key functions of the national information and communication system.

[86] Korean National Law Information Center, "National Intelligence Service Act" (in Korean), https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EA%B0%80%EC%A0%95%EB%B3%B4%EC%9B%90%EB%B2%95.

[87] Supra note 23, p.10.

[88] Ministry of Economy and Finance, "Korean New Deal: National Strategy for a Great Transformation," April 2020. See https://english.moef.go.kr/pc/selectTbPressCenterDtl.do?boardCd=N0001&seq=4948.

[89] Minkyung Song, "Trend Analysis of Information Protection Research in Korea," Korea Institute of Information and Security and Cryptology, Chungcheong Chapter (KIISC CC), 2019.

[90] The KCI is a system to analyze citation relationship among articles in a database of domestic journals, articles (including original papers), and other references.

[91] It was conducted at the CCE 2019 by the authors.

[92] "Situation Report (SITREP) Template," Persimmon Group, April 3, 2016, https://www.thepersimmongroup.com/situation-report-sitrep-template/.

[93] Locked Shields is NATO's cyber defense exercise. See more at https://www.ccdcoe.org/exercises/locked-shields.

[94] The NIS formed a joint team with the Korea Electric Power Corporation and the National Security Research Institute. Technical training to defend against attacks on systems and strategic training to introduce Korea's cybersecurity policy were conducted by dividing manpower by sectors such as energy, defense, and network.

[95] ByungChul Won, "NIS Participates in Locked Shield, Which Is World's Largest Cyber Defense Exercise, for the First Time," BoanNews, April 14, 2021, https://www.boannews.com/media/view.asp?idx=96502.

[96] Sunha Bae and Minkyung Song, "K-Global Cybersecurity Capacity Assessment and Application," GCPR 2019, September 30, 2019.

[97]
Assessment Criteria," *Journal of The Korea Institute of Information Security and Cryptology* 25, no. 5 (2015): 1293–1314.

[98] The Global Cybersecurity Index (GCI) is a multi-stakeholder initiative to raise cybersecurity awareness and to measure the commitment of countries to cybersecurity and its wide field of application cutting across industries and sectors. Find the 2018 edition at https://www.itu.int/pub/D-STR-GCI.01-2018.

[99] John A. Martilla and John C. James, "Importance-Performance Analysis," *Journal of Marketing* 41, no. 1 (1977): 77–79.

[100] Supra note, 37, p.18.

[101] Gayong Moon, "2003: 1.25 Internet Disruption, Changing the Frame of Information Protection," BoanNews, May 12, 2019, https://www.boannews.com/media/view.asp?idx=79427.

[102] Gilju Lee, "Established a DDoS Response System for Public Institutions," Korea Information Telecommunication News, October 2009, http://www.koit.co.kr/news/articleView.html?idxno=32885; Chulsun Park, "3.4 DDoS Cyber-Attack Response and Future Countermeasures," Korea policy briefing, March 2011, https://www.korea.kr/news/policyNewsView.do?newsId=18709693.

103 Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. (January 29, 2004) Article 46(30), see https://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=58583&chrClsCd=010203&urlMode=engLsInfoR&viewCls=engLsInfoR#0000.

104 The Safety Check of Information Protection System was changed to the ISMS (Information System Management System) in 2012.

105 Sujeong Sin, "Issues and Implications for the Safety Check of Information Protection System," BoanNews, March 13, 2006, https://www.boannews.com/media/view.asp?idx=1688&direct=mobile.

106 Enforcement decree of the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. (August 18, 2012); National Information Security Basic Guideline (Confidential).

107 Dain On, "Network Separation Regulations Need to Be Reorganized in Accordance With Data Importance," ETNews, June 28, 2020, https://etnews.com/20200626000119.

108 Kyungae Kim, "PyeongChang Olympic Target Attack! Defense With Real-Time Detection and Sharing System," BoanNews, January 9, 2018, https://www.boannews.com/media/view.asp?idx=65988&kind=2.

109 The results of survey are published annually through the "White Paper on Information Security." The English version of the "White Paper on Information Security" will be published this year, and more detailed information can be found in this.

110 NIS et al., "White Paper on Information Security 2021" (in Korean), 2021, p. 218.

111 NIS et al., "White Paper on Information Security 2021" (in Korean), 2021, p. 243.

112 Final research report for commissioned project in KISA, "A Study on the Comparative Method of Information Protection Legislation to Strengthen the Cyber Security Framework (KISA-WP-2015-0042)," 2015.

113 In order to address the lack of a single point person to lead responses to cyber attacks, the NCSC was designated as a "control tower" by the National Cyber Crisis Comprehensive Countermeasures (2009) and the National Cyber Security Master Plan. Nevertheless, criticisms of the lack of coordination continued until the National Cyber Security Comprehensive Measures (2013) designated the Blue House National Security Office as the "control tower."

114 Public attribution in its most elementary form is the blaming of a particular actor as responsible for a cyber incident. It can be done by a variety of actors, including governments, companies, and NGOs. But public attribution by the government is mainly considered in this chapter because government action to assign blame is an inherently political act. Florian J. Egloff, "Contested Public Attributions of Cyber Incidents and the Role of Academia," Contemporary Security Policy 41, no. 1 (2020): 55–81.

115 National Security Office of Cheong Wa Dae, "National Cybersecurity Strategy," April 2019, p. 16.

116 HyungJoong Yoon, "Coinrail Hacking, 10 Types of Coins Such as Ethereum Leaked Worth 45 Billion Won," Coindesk Korea, June 11, 2018, http://www.coindeskkorea.com/news/articleView.html?idxno=22904; BBC News Korea, "Exchange Hacking Continues to Steal 35 Billion Won Worth of Virtual Currency," June 20, 2018, www.bbc.com/korean/news-44543609; GeunMo Park, "Upbit Hack Ethereum About 20,000 Out of 342,000 Can Be Washed," Coindesk Korea, January 16, 2020, http://www.coindeskkorea.com/news/articleView.html?idxno=65024.

117 Emily Price, "Chinese Hackers Targeted 27 Universities to Steal Maritime Research, Report Finds," *Fortune*, March 5, 2019, https://fortune.com/2019/03/05/chinese-hackers-targeted-27-universities-to-steal-maritime-research-report-finds/.

118 According to the Council on Foreign Affairs' Cyber Operations Tracker, in 2017, the Bronze Butter Group spied on companies in the fields of biotechnology, electronics manufacturing, and chemistry. In 2018 and 2020, China's Winnti Group conducted cyber attacks targeting Korean game and software companies. In 2020, malicious hackers used Bisonal malware to attack Korean companies and also appeared to use spear phishing to attack government research institutes in Korea.

119 Lanna Deamer, "Which Countries Have Been Most Targeted by Cyber Attacks?," Electronic Specifier, July 21, 2020, https://www.electronicspecifier.com/products/cyber-security/which-countries-have-been-most-targeted-by-cyber-attacks.

120 See https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020.

Chapter 3

121 For example, on November 25, 2020, the European Commission published the Data Governance Act (DGA) in response to a public consultation on the European Strategy for Data. The DGA aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. See also Australian Government, "Data Governance Framework 2020," approved on August 24, 2020, https://www.aihw.gov.au/getmedia/a10b8148-ef65-4c37-945a-bb3effaa96e3/AIHW-data-governance-framework.pdf.aspx. This chapter uses the terms "personal data" and "personal information" in the same way. The latter is more often used in the context of Korean laws.

122 Cheong Wa Dae (President's Office of Korea), "Opening Remarks by President Moon Jae-in at 6th Emergency Economic Council Meeting," June 1, 2020, https://english1.president.go.kr/Briefingspeeches/Speeches/833. The Korean government has been pursuing digital economic policies based on the "Fourth Industrial Revolution Action Plan" made in November 2017.

123 For discussing the causes or reasons for data localization, see Joshua P. Meltzer, "Data and the Transformation of International Trade," Brookings Institution, March 6, 2020, https://www.brookings.edu/blog/up-front/2020/03/06/data-and-the-transformation-of-international-trade/.

124 United States Trade Representative, "2021 National Trade Estimate Report on Foreign Trade Barriers," March 2021, pp. 323–35; International Regulatory Strategy Group, "How the Trend Towards Data Localisation Is Impacting the Financial Services Sector," December 2020, https://www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf; and Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," Information Technology and Innovation Foundation, May 2017, http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.45773412.1159173050.1620277743-1412413491.1620277743.

125 The following analysis of Korean laws is effective as of June 2021.

126 On May 26, 2005. See decision 99Hun-Ma513.

127 The PIPA was in fact developed from the Act on the Protection of Personal Information Maintained by Public Institutions where the Interior Ministry was responsible for its implementation. Thus, although the PIPA covers the processing of personal information by private sectors, the Interior Ministry, not the Personal Information Protection Commission, was responsible for the PIPA until the so-called three data laws' amendment in 2020.

128 The three data laws' amendment refers to the amendment to the PIPA, the Network Act, and the Credit Information Act. The PIPA was amended on February 4, 2020, and effective on August 5, 2020. This amendment records as the tenth since its enaction in March 2011. The Network Act is currently similar to the e-Privacy Regulation to be adopted by the European Union.

129 Before the amendment in February 2020, the enforcement powers under the PIPA were entrusted not to the PIPC but to the Interior Ministry. The PIPC had only deliberation powers on data protection policymaking until that amendment.

130 PIPA, Art. 7(1). The Korea Internet and Security Agency (KISA) performs the functions, including receiving reports of data breaches and collecting relevant materials from a controller in case of an alleged violation of the PIPA, delegated by the PIPC.

131 PIPA, Art. 7(2). First, the investigation power, given to the PIPC by the three data laws' amendment in 2020, used to be conducted by the Interior Ministry. Those foreign-related companies were imposed administrative fines for violating the provisions of the PIPA. For example, Audi-Volkswagen Korea was imposed a fine of 12 million Korean won, roughly equivalent to $11,000, for violating the obligation of destruction after the expiry of the retention period in February 2018. In February 2019, along with other foreign-related companies, DHL Korea was fined 32 million Korean won, roughly equivalent to $28,000, for violating the obligation of notifying the required items to data subjects for obtaining their consent. Second, the Personal Information Dispute Mediation Committee has dealt with mediation over personal information disputes. The disputes subject to mediation have mainly involved the out-of-purpose use and provision to third parties of personal information, the collection of personal information without the consent of data subjects, and the denial of access to personal information or failure of taking measures necessary to correct or erase personal information, etc. Third, the PIPC may advise the head of central administrative agencies over matters necessary to improve the relevant statutes in terms of data protection by analyzing and reviewing the data breach incident factors of such statutes. It has been reviewing most of the statutes subject to enactment or amendment since September 2016. For example, the National Intelligence Service (NIS) submitted a proposal on the Framework Act on Cyber Security to the PIPC for assessment on October 25, 2016. The PIPC recommended the NIS, inter alia, to prevent the misuse and abuse of personal information by accurately defining the scope of data to be collected and used in cybersecurity activities. The proposal was automatically discarded, however, as the session of the National Assembly was closed in May 2020.

132 PIPA, Art. 1.

133 The 108 Convention is the first legally binding international instrument for data protection. On May 18, 2018, the Committee of Ministers of the Council of Europe adopted the protocol amending the 108 Convention. Korea, like Japan, the Philippines, and Indonesia in Asia, is accredited as an observer to the Consultative Committee established by the 108 Convention. Joining the Consultative Committee as an observer may imply that Korea would ultimately accede to the 108 Convention.

134 Graham Greenleaf and Whon-il Park, "Korea's New Act: Asia's Toughest Data Privacy Law," *Privacy Laws & Business International Report*, no. 117 (June 2012): 1–6, (UNSW Law Research Paper No. 2012-28).

135 Mediaus, "Three Data Laws Criticized as the Law Stealing Human Rights in Information" (in Korean), July 17, 2020, http://www.mediaus.co.kr/news/articleView.html?idxno=188321.

[136] The provisions on data portability and the right to respond to automated decisions are also included in a proposed amendment to the PIPA that was circulated in January 2021.

[137] In January 2017, the European Commission adopted a communication on the international aspects of privacy, which set out the EU strategy in the field of international data flows and protection. In this communication it was announced that the European Commission would actively engage with key trading partners in East and Southeast Asia, starting with Japan and Korea. After the conclusion of the EU-Japan talks on adequacy decision in July 2018, the mutual EU-Japan adequacy decision was adopted on January 23, 2019.

[138] The European Commission issued a draft decision on the adequate protection of personal data by Korea on June 14, 2021.

[139] For example, trade secrets are protected under the Unfair Competition Prevention and Trade Secret Protection Act, where trade secret is defined as "information, including a production method, sale method, useful technical or business information for business activities, which is not known publicly, is managed as a secret, and has independent economic value."

[140] U.S. Department of State, "2020 Investment Climate Statements: South Korea," https://www.state.gov/reports/2020-investment-climate-statements/south-korea/. A proposed amendment to the PIPA, covering the provisions on cross-border transfer of personal information, was circulated by the PIPC in January 2021. It remains to be seen whether this amendment would be successful throughout the legislative process in 2021.

[141] Providing personal information to third parties includes sharing personal information with third parties. PIPA, Art. 17(1).

[142] PIPA, Art. 39-12(2).

[143] PIPA, Art. 39-12(2). Administrative fines not exceeding 20 million Korean won, roughly equivalent to $18,000, may be imposed for outsourcing the processing of, or storing, users' personal information overseas in violation of this provision.

[144] PIPA, Art. 17(3). Providing personal information to third parties abroad is more restricted than providing to domestic third parties in that there are other legal bases in addition to the consent of data subjects for the latter. See PIPA, Art. 17(1).

[145] PIPA, Art. 17(2). For the prevention and combating of crime, including terrorism, the US and Korea may, in compliance with their respective national laws, in individual cases, supply with the personal data of the data subject(s), inter alia, that will commit or has committed a criminal offense, or participates in an organized criminal group or association, or will commit or has committed terrorist or terrorism-related offenses in the other country, or offenses related to a terrorist group or an association in the other country. The Agreement between the Government of the Republic of Korea and the Government of the United States of America on Enhancing Cooperation to Prevent and Combat Crime, signed on November 7, 2008, Art. 8(1). Public institutions may provide personal information to third parties abroad for other purposes than collected where it is necessary to perform a treaty or other international agreement; or where it is necessary for the investigation of a crime, indictment, and prosecution. PIPA, Art. 18(2)(vi) and (vii) respectively.

[146] U.S. Trade Representative, "2017 National Trade Estimate Report," p. 284.

[147] For the protection of IT service users' personal information transferred abroad, providing, outsourcing the processing of, or storing IT service users' personal information abroad are collectively referred to as transferring. Providing IT service users' personal information abroad includes accessing to such information. PIPA, Art. 39-12(2).

[148] PIPA, Art. 39-12(3).

[149] PIPA, Art. 39-12(4).

[150] Presidential Decree 30892, Art. 48-10(1).

[151] Presidential Decree 30892, Art. 48-10(2).

[152] Presidential Decree 30892, Art. 48-10(3).

[153] PIPA, Art. 39-12(5).

[154] When assessing the adequacy of the level of data protection, the European Commission must take account of the elements including "rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization." GDPR, Art. 45(2)(a).

[155] PIPA, Art. 39-11(1). For example, Netflix, a global OTT service provider, has not been required to designate a domestic agent, because it has its own business office in Korea.

[156] Presidential Decree 30892, Art. 48-9(1).

[157] PIPA, Art. 39-11(1).

[158] PIPA, Art. 39-11(4).

[159] PIPA, Art. 39-11(2).

[160] PIPA, Art. 39-11(3).

161 On September 9, 2020, the PIPC decided to recommend seven foreign IT service providers to improve the management of a domestic agent. Those IT service providers included Facebook, Microsoft, and TikTok. For reference, the GDPR provides for the designation of a domestic agent to exert its extraterritorial effect explicitly. The controller or the processor, which are not established in the EU, are required to designate a representative in the EU in the following two cases: (1) where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or (2) the monitoring of their behavior as far as their behavior takes place within the EU. GDPR, Art. 27.

162 For example, the 108 Convention of the Council of Europe seeks to reduce restrictions on transborder data flows between the contracting parties on the basis of reciprocity. Though, "an equivalent protection" provided in Art. 12(3)(a) of the convention needs to be carefully determined.

163 PIPA, Art. 39-13.

164 PIPA, Art. 39-13.

165 Spatial Data Act, Art. 1.

166 Spatial Data Act, Art. 16(2). See also Art. 14(3).

167 Spatial Data Act, Art. 21(2). *See* also Art. 14(3).

168 Spatial Data Act, Arts. 16(2) and 21(2). A consultative committee is organized by the minister of land, infrastructure and transport with the heads of the relevant agencies, including the minister of science and ICT, the minister of foreign affairs, the minister of unification, the minister of national defense, the minister of the interior, the minister of trade, industry and energy, the director of the national intelligence service, and so on.

169 U.S. Trade Representative, "2020 National Trade Estimate Report," p. 320.

170 U.S. Trade Representative, "2019 National Trade Estimate Report," pp. 324–25. The precise satellite imagery of certain facilities is argued to pose a threat to the national security of Korea, which is still technically in an armed conflict with North Korea.

171 According to Art. XXI(a), a contracting party (WTO Member) must not be required to furnish any information the disclosure of which it considers contrary to its essential security interests. In addition, according to Art. XXI(b)(iii), a contracting party must not be prevented from taking any action that it considers necessary for the protection of its essential security interests taken in time of war or other emergency in international relations. The "self-judging" principle seems to apply in this case. In the dispute raised with respect to Section 232 of the Trade Expansion Act of 1962, the United States argued that "the tariffs imposed pursuant to Section 232 are issues of national security not susceptible to review or capable of resolution by WTO dispute settlement." Panel Report, United States-Certain Measures on Steel and Aluminum Products, Communication from the United States, WT/DS544/2, April 17, 2018. Although a ceasefire and armistice agreement brought the fighting to an end in 1953, the Korean War is technically still ongoing.

172 U.S. Trade Representative, "2020 National Trade Estimate Report," p. 320.

173 Korea has concluded FTAs with Chile, Singapore, the EFTA, the Association of Southeast Asian Nations (ASEAN), India, the EU, Peru, the United States, Turkey, Australia, Canada, China, New Zealand, Vietnam, Colombia, the Republics of Central America, the UK, Indonesia, Israel, and Cambodia in chronological order. Korea is also a signatory to the Regional Comprehensive Economic Partnership (RCEP). The FTAs with Indonesia, Israel, Cambodia, and the RCEP have not yet entered into force.

174 The Korea-EU FTA, Annex 7-D on the additional commitment on financial services, para. 1, and the letter from Hyun Chong Kim and Sung Jin Kim on June 30, 2007, attached to Chapter 13 on financial services of the Korea-U.S. FTA. This kind of deference in regard to the requirements for the location of technology facilities is also provided in the Korea-Turkey FTA (Annex D on Schedule of Specific Commitments [Korea], Footnote 32), the Korea-Australia FTA (Annex 8-B on Specific Commitments, Section A[2] on Transfer of Information), the Korea-Canada FTA (Annex 10-B on Specific Commitments, Section C on Transfer of Information, para. 10, second sentence), and the Korea-Republics of Central America FTA (Annex 11-A on Cross-Border Trade [Korea], Footnote 9).

175 Korea-U.S. FTA, Art. 15.8.

176 For a brief analysis of China's data localization requirements, see Dehao Zhang, "China: Data Localization Requirements," September 1, 2020, https://www.fieldfisher.com/en/insights/china-data-localisation-requirements.

177 The RCEP was signed among the ten member states of ASEAN as well as Australia, China, Japan, Korea, and New Zealand on November 15, 2020. The RCEP was initiated by ASEAN, but China must have influenced its economic and political strength during the negotiations as the other signatories are largely dependent on China's market.

178 RCEP, Art. 12.14(1). A similar provision is found in the CPTPP.

179 RCEP, Art. 12.14(2). The identical provision is found in the CPTPP and the USMCA.

180 RCEP, Art. 12.14(3)(a). The identical provision is found in the CPTPP.

181 RCEP, Art. 12.14(3)(a). The identical provision is found in the CPTPP.

182 RCEP, Art. 12.14(3)(b). This provision is not found in the CPTPP and the USMCA. This exception for essential security interests is also found for the cross-border transfer of information by electronic means. See RCEP, Art. 12.15(3)(b).

183 RCEP, Art. 12.14(3)(b). This provision is not found in the CPTPP and the USMCA.

Afterword

184 This summary includes excerpts from blog posts on Open Net Korea by KS Park, including "The World's Only Attempt to Legislate 'Network Use Fees' Will Further Damage Consumers – the Illusion of Charging 'Delivery Fees' on the Internet Will Disincentivize Investment in Network Expansion," May 17, 2021, http://opennetkorea.org/en/wp/3265; and "South Korea's Network Infrastructure May Be State of the Art, but the Country's 'Pay to Play' Regime for Delivering Traffic Is an Unprecedented Threat to the Free and Open Internet," September 17, 2020, http://opennetkorea.org/en/wp/3122.

185 The Herfindahl–Hirschman Index, which measures market concentration, is calculated by squaring the market share of each firm competing in the market and then summing the resulting numbers.

186 Ofcom, "The International Communications Market 2017: Telecoms and Networks," December 2017, https://www.ofcom.org.uk/__data/assets/pdf_file/0026/108908/icmr-2017-telecoms-networks.pdf.

187 See the TeleGeography's annual bandwidth pricing review from 2021, especially slide 17, available here: https://blog.telegeography.com/2021-global-pricing-trends-in-20-minutes.

188 Ibid.

189 Body of European Regulators and Electronics Communications, "BEREC's Comments on the ETNO Proposal for ITU/WCIT or Similar Initiatives Along These Lines," November 14, 2012, https://berec.europa.eu/eng/document_register/subject_matter/berec/others/1076-berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines.

190 For example, Chambers and Partners, "Korean Court Ruling Over a Network Usage Fee Dispute Between Netflix and SK Broadband," July 4, 2021, https://chambers.com/articles/korean-court-ruling-over-a-network-usage-fee-dispute-between-netflix-and-sk-broadband; Ben Munson, "Netflix Handed Loss in South Korea Network Usage Fee Court Case," FierceVideo, June 29, 2021, https://www.fiercevideo.com/regulatory/netflix-handed-loss-south-korea-network-usage-fee-court-case.

191 Yonhap, "Netflix Pressed to Share Network Costs in S. Korea," *Korea Herald*, May 21, 2020, http://www.koreaherald.com/view.php?ud=20200521000754.

192 Safenet, "[Joint-Statement] Civil Society Demand That Net Neutrality Be Protected in Interconnection Rules," February 15, 2021, https://safenet.or.id/2021/02/joint-statement-civil-society-demand-that-net-neutrality-be-protected-in-interconnection-rules/.

193 Open Net Korea et al, "Open Letter to South Korea's ICT Minister: Ensure Net Neutrality," Access Now, September 16, 2020, https://www.accessnow.org/open-letter-south-korea-net-neutrality/.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Asia Program

In Asia, rapid growth and strong economic fundamentals have lifted hundreds of millions from poverty. But significant cracks have emerged in this hopeful story. The Carnegie Asia Program explores three disruptive risks to Asia's future: (1) disruptive security risks, from competition among the big powers; (2) disruptive governance risks, from uneven state capacity or insufficiently inclusive growth; and (3) disruptive technological risks, arising from new innovations, regulatory diversity, or competing standards. Our program recommends policies to manage the growing threats to Asia's long peace. We also help decisionmakers address social, institutional, and political obstacles to achieving Asia's development potential.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program develops strategies to maximize the positive potential of emerging technologies while reducing risk of large-scale misuse or harm. With Carnegie's global centers and an office in Silicon Valley, the program collaborates with technologists, corporate leaders, government officials, and scholars globally to understand and prepare for the implications of advances in cyberspace, biotechnology, and artificial intelligence.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org