SOUTH KOREA'S CYBER SECURITY CHALLENGES AND LEARNING OPPORTUNITIES FROM ESTONIA

by
Melita Phachulia and
Josephine Ørgaard Rasmussen

Introduction

With 2,383 documented cyber-attacks in 2025, the Republic of Korea (ROK, or South Korea) experienced a 26 percent increase from the previous year. A joint report by the ROK Ministry of Science and ICT and Korea Internet & Security Agency (KISA) highlighted increased attacks on essential daily sectors—such as telecommunications, logistics, and finance—alongside supply-chain vulnerabilities that exploit open-source software. The report illustrates a complex cyber threat landscape in which cyberattacks are no longer limited to high-value government or military targets but increasingly seek to disrupt critical civilian infrastructure and digital services.

To mitigate these systemic vulnerabilities, the Lee Jae Myung administration fundamentally restructured South Korea's national cyber defense policy in late 2025, shifting from a traditionally passive posture toward an Active Cyber Defense (ACD) framework. However, the long-term effectiveness of this framework is constrained by South Korea's highly centralized and hyperconnected digital ecosystem. Furthermore, as regional adversaries increasingly weaponize artificial intelligence (AI) for cyber operations, the Lee administration faces a strategic imperative to continuously adapt its cybersecurity architecture to stay ahead of these emerging and AI-enabled threats.

One way to accelerate this process is through closer cooperation with trusted international partners. Among these, Estonia offers a particularly relevant case. Over the past three decades, Estonia has developed one of the world's most resilient digital governance systems by combining technological innovation with strong institutions, distributed digital infrastructure, and a holistic, whole-of-society approach to cybersecurity. Rather than providing a model to replicate, Estonia offers practical policy lessons that can help South Korea strengthen resilience while reducing vulnerabilities associated with its highly centralized digital ecosystem.

This blogpost identifies three areas where the Lee administration could draw lessons from Estonia's cyber resilience framework to strengthen South Korea's cybersecurity. It concludes by proposing three policy recommendations on how to expand bilateral cyber cooperation between South Korea and Estonia.

South Korea's Active Cyber Defense Framework and the Digital Paradox

Beginning in late 2024 and expanding throughout 2025, the government introduced a series of legislative and policy reforms that strengthened cyber threat detection, intelligence sharing, and the ability to disrupt malicious cyber infrastructure before attacks reach domestic networks. This shift marks South Korea's transition from a historically passive, reactive cybersecurity posture to a proactive Active Cyber Defense (ACD) framework, driven by the increasing complexity of modern, state-sponsored cyber threats. Despite these reforms, South Korea continues to face a fundamental structural challenge to its cybersecurity.

South Korea's position as a hyper-connected global tech leader presents a critical double-edged sword. While centralized digital platforms, comprehensive e-governance, and near-universal internet access have generated significant economic and technological advantages, they have also created a broad national cyber-attack surface. As state-sponsored actors and cybercriminal groups increasingly exploit these interconnected systems, Seoul faces a profound "Digital Paradox": the drivers of its remarkable digital transformation have simultaneously introduced distinct security vulnerabilities.

The Digital Paradox is particularly evident in South Korea's dependence on home-grown platforms such as Kakao and Naver. Communications, digital payments, mobility services, financial transactions, and other essential functions are interconnected within

a handful of digital ecosystems. A single ecosystem, such as Kakao, may simultaneously paralyze public warning systems, transportation, and banking across the country through a single cyber-attack, negating the need for an enemy to penetrate thousands of segmented networks. Addressing this challenge requires more than strengthening technical defenses. Overcoming this paradox requires South Korea to transition its cybersecurity strategy away from rigid centralization and toward a distributed digital architecture. This includes revising the relationship between the state, domestic tech monopolies, and citizens.

Why Estonia?

Estonia has emerged as one of the world's leading cyber powers by combining digital transformation with a strong culture of cyber resilience. Following independence from the Soviet Union in 1991, the country viewed digitalization not simply as a modernization project but as a strategic response to limited resources and administrative capacity. Digital governance therefore became a cornerstone of state-building and national resilience.

In the late 1990s, initiatives such as the Tiger Leap (Tiigrihüpe) program expanded internet access in schools, strengthened digital infrastructure, and promoted digital literacy from an early age. These investments laid the foundation for one of the world's most digitally integrated societies.

The foundation was tested during the 2007 large-scale cyberattacks, widely regarded as a turning point in global cybersecurity. Government institutions, banks, media outlets, and other critical services were targeted in coordinated distributed denial of service (DDoS) attacks, demonstrating how cyber operations could disrupt an entire digital society. Rather than slowing digitalization, the attacks prompted the government to strengthen its cybersecurity institutions, improve public-private coordination, and integrate cyber resilience into national security planning.

Today, cybersecurity policy is coordinated by the Ministry of Justice and Digital Affairs, while the Estonian Information System Authority (RIA), operating under the Ministry, is responsible for securing government networks and coordinating national cyber incident response. Their work is supported by secure digital identity, the X-Road interoperability platform, distributed digital architecture, and close cooperation between government, industry, academia, and civil society.

Although Estonia and South Korea differ significantly in size and strategic environment, both are highly digitalized societies that depend on secure digital infrastructure for economic growth and national security. Estonia's experience therefore offers valuable policy lessons on how to strengthen cyber resilience while reducing systemic vulnerabilities associated with interconnected digital ecosystems.

Learning Prospects from Estonia in Building Cyber Resilience in South Korea

Estonia's experience demonstrates that cyber resilience extends beyond technology. It relies on resilient institutions, distributed digital governance, long-term investment in digital skills, and strong public-private cooperation. These lessons are particularly relevant for South Korea as it seeks to reduce vulnerabilities associated with digital concentration while adapting to an increasingly complex cyber threat environment.

Below are three key lessons from Estonia that the Lee administration can draw on to decentralize South Korea's digital architecture and strengthen its cyber defenses:

1. ***Distributed Digital Governance***

One of the defining features of Estonia's cybersecurity model is its distributed and federated digital governance architecture. Unlike South Korea, where many essential services, including communications, digital payments, and financial services, are concentrated among a small number of dominant platforms, Estonia has developed a digital ecosystem designed to reduce systemic cyber risk by minimizing single points of failure. Two key mechanisms have been used to achieve this:

A. X-Road: Secure and Interoperability Data Exchange

Rather than relying on a centralized database or a single digital platform, Estonia developed X-Road, a secure

interoperability platform that enables government agencies and private institutions to exchange data while retaining control of their own databases. Information is shared through standardized and encrypted interfaces, improving both security and efficiency while preserving institutional control over data.

B. Distributed Digital Architecture

Government ministries, municipalities, healthcare providers, banks, and other institutions maintain separate databases connected through X-Road rather than relying on a single centralized repository. Because critical data are distributed across multiple organizations, a cyber incident affecting one institution is less likely to cascade across the entire system. This approach reduces single points of failure, strengthens the continuity of essential services, and improves overall cyber resilience.

For South Korea, adopting elements of a more distributed digital governance model could help reduce dependence on a small number of dominant domestic digital platforms and strengthen the resilience of critical infrastructure. While fully replicating Estonia's system completely is neither feasible nor necessary, the underlying principles of interoperability, distributed architecture, and secure data exchange could help address vulnerabilities associated with South Korea's highly centralized digital ecosystem.

2. ***Ensuring Government Continuity: The "Data Embassy" Model***

Cyber resilience is not only about preventing attacks but also about ensuring that governments can continue operating during major crises. To strengthen continuity, Estonia established the world's first "Data Embassy" in Luxembourg – a secure, treaty-based facility that stores backup copies of critical government data outside the country's borders.

If domestic infrastructure were disrupted by a large-scale cyberattack or kinetic attack, essential government services could be restored from secure servers abroad. While South Korea's strategic environment differs, the "Data Embassy" model demonstrates the importance of continuity planning, geographically distributed data storage, and resilient digital infrastructure for maintaining government operations during national emergencies.

3. ***Whole-of-Society Cyber Defense***

Estonia's cybersecurity strategy extends beyond government institutions through a whole-of-society approach to cyber resilience. Alongside close public-private cooperation, the "Cyber Defence Unit of the Estonian Defence League" (EDL) brings together volunteer cybersecurity experts from government, academia, and the private sector who can be mobilized during major cyber incidents. This strengthens national preparedness, facilitates information sharing, and improves coordination between civilian and military actors.

For South Korea, the Estonian experience highlights the importance of institutionalizing cooperation among government agencies, technology companies, telecommunications providers, financial institutions, universities, and cybersecurity professionals. Given that many of South Korea's essential digital services are concentrated among a small number of private platforms, a structured public-private coordination mechanism would enable faster information sharing, coordinated incident response, and more effective protection of critical infrastructure during major cyber crisis. As AI-enabled cyber threats become increasingly complex, strengthening societal resilience will be as important as enhancing technical capabilities.

Recommendations: Expanding South Korea-Estonia Cyber Cooperation

Beyond sharing best practices, South Korea and Estonia have significant opportunities to deepen bilateral cooperation in cybersecurity in the coming years. Existing multilateral and bilateral cooperation provides a strong foundation for expanding joint cyber exercises, policy dialogue, and research and development (R&D) initiatives. To mitigate systemic digital vulnerabilities, Estonia and South Korea can forge a more resilient cyber partnership by institutionalizing cooperation in three key areas:

Recommendation 1: Joint Cyber Exercises

South Korea can further integrate its military and intelligence cyber capabilities into Estonia's world-class

training environments by building on its participation in NATO's "Cooperative Cyber Defence Centre of Excellence" (CCDCOE) and the 2017 Estonia-South Korea Cyber Security Cooperation Agreement. An Estonia-ROK joint cyber exercise platform could provide the two countries' governments, militaries, and private-sector organizations with high-fidelity simulations to stress-test defenses and train response teams. South Korea has previously participated in such exercises, both multilaterally (NATO's CCDCOE "Locked Shields" Exercise) and bilaterally (Netherlands-led CyberNet exercise), making such coordination with Estonia conceivable.

Recommendation 2: Cybersecurity Education Cooperation and Workforce Development

Estonia's cyber resilience is rooted not only in technology but also in long-term investment in digital literacy and cybersecurity education. Beginning with the Tiger Leap program and extending to universities, professional training, and public awareness initiatives, Estonia has cultivated a digitally skilled workforce and a cyber-aware society. South Korea and Estonia should expand cooperation through joint university programs, researcher exchanges, cybersecurity fellowships, and professional training involving government agencies, research institutes, and industry. Such initiatives would strengthen long-term cyber capacity and prepare specialists to address evolving cyber threats.

Recommendation 3: R&D Cooperation to Tackle Artificial Intelligence Cyber Threats

The convergence of threat perceptions—with South Korean intelligence agencies flagging "AI-powered hacking" as a top risk, and Estonia defining AI in cyberattacks as an accelerator that compresses traditional cyber defense timelines—highlights the potential for immediate cooperation on joint R&D to address the current and future use of AI in cyberattacks. As AI enables both cyber defense and cyberattacks, joint research on AI governance, threat detection, critical infrastructure protection, and secure digital innovation would strengthen the resilience of both countries while contributing to broader international cybersecurity efforts.

Melita Phachulia is an Executive Assistant at the Institute for Security and Development Policy (ISDP), working closely with the Stockholm Center for Research and Innovation Security (SCRIS) and the Asia Program. Her work focuses on hybrid warfare, security, research and innovation, and resilience with regional expertise in the Nordic-Baltic and Black Sea regions, as well as NATO-related security environments.

Josephine Ørgaard Rasmussen is the Project Manager at the Stockholm Korea Center of the Institute for Security and Development Policy. Her research focuses on domestic politics and the security situation on the Korean Peninsula.