The Asan Institute for Policy Studies

ISSUE BRIEF Executive Summary

No. 2025-31(S)

# Recommendations on Cybersecurity Law and Strategy for the Lee Jae-myung Administration

**Shin Sohyun**
Research Fellow
2025-09-18

## Letting go of the Obsession with Enacting a Basic Act on Cybersecurity

Since 2005, successive attempts have been made across nearly 20 years and several National Assemblies to legislate a basic law on cybersecurity, with multiple bills introduced under different names by lawmakers from both major parties, but all have lapsed without passage. For the last nearly two decades, repeated attempts to enact a Basic Act on Cybersecurity have failed largely due to bureaucratic power struggles over governance among the relevant ministries and agencies. There is additionally public distrust that information collection could lead to surveillance, and a lack of recognition of cybersecurity as part of broader national and international security. The recurring debates have been driven less by considerations of national cybersecurity from the citizens' perspective. For citizens, whether reform comes through a basic law or amendments to existing statutes is less important. Indeed, the debate over a "basic law" reflects bureaucratic turf wars more than substantive needs. We should therefore refrain from further wasteful legislative wrangling. Instead, national cybersecurity ought to be strengthened in practical terms by amending the National Intelligence Service Act and enacting new legislation as necessary.

## Legislative Framework Trends on (1) Foreign Information Collection and South Korea's Gaps

### *1. International Legislative Trends*

The United States (the Foreign Intelligence Surveillance Act: FISA), the United Kingdom (The Investigatory Powers Act: IPA), Australia (The Assistance and Access Act), and Canada (The Communications Security Establishment Act: CSE Act) all legally permit overseas information collection but require safeguards against abuse, such as prior authorization and post-action reporting and oversight by parliament. Japan also enacted the Active Cyber Defense Law in 2025, which legalized neutralization measures by the police and Self-Defense Forces.

### *2. South Korea's Challenges and Gaps*

Regulation on Cybersecurity Services which was amended in March 2024, newly enacted Article 6-2(3): "the Director of the National Intelligence Service may take necessary measures, such as tracking, neutralizing, etc., overseas and overseas bases located in North Korea, in order to preemptively identify, control, check, and block activities, such as international and national hacking organizations, which are contrary to national security and national interests." It is unconstitutional on two grounds.

**First**, the current provisions on preemptive tracking and neutralization measures lack adequate safeguards against abuse (misuse) in NIS operations —protections that are already in place in other like-minded countries, including the U.S., the U.K., Australia, the Netherlands, and Japan.

**Second**, the current presidential decree—the Regulation on Cybersecurity Services must acquire a mandate from a certain Act superior to the decree. By the Constitution of South Korea, Article 37(2) states that "the freedoms and rights of citizens may be restricted by Act only when necessary for national security, the maintenance of law and order or for public welfare. Even when such restriction is imposed, no essential aspect of the freedom or right shall be violated." Hence, without a law-level enactment, the Presidential Decree alone cannot authorize preemptive tracking and neutralization measures against overseas bases (Article 6-2(3)) or South Korean nationals suspected of connecting to malicious foreign actors (Article 3(1)(b)).

Japan, in May 2025, passed the enactment of the so-called "Active Cyber Defense Act," accompanied by safeguards to prevent misuse or overreach of these preemptive tracking and neutralization measures. Therefore, it is necessary to reinforce provisions such as Article 6-2 of the current Regulations on Cybersecurity Services and incorporate them into the higher-level National Intelligence Service Act as the legal basis to establish provisions for

preemptive tracking and neutralization measures and their control mechanisms against misuse or abuse. Only then will the legislation be brought to a level comparable to that of other advanced countries in similar circumstances.

## Legislative Framework Trends on (2) Foreign Interference and South Korea's Gaps

### *1. International Legislative Trends*

The EU introduced the concept of Foreign Information Manipulation and Interference (FIMI), and the United States adopted Foreign Malign Influence (FMI), each creating dedicated institutions and legislation. The United Kingdom established the National Security Online Information Team (NSOIT), France created VIGINUM under the Prime Minister's Office, and Australia enacted laws covering both online and offline interference.

### *2. South Korea's Challenges and Gaps*

**First,** South Korea currently lacks any clear legal framework to counter foreign interference conducted through online information manipulation. Therefore, legislation regulating such activities should be enacted, which is consistent with the approach of similarly situated countries, and related statutes, including the espionage offense, should likewise be revised.

**Second**, distinguishing domestic misconduct from organized foreign campaigns (Collaborated Inauthentic Behaviors) can be mistaken for censorship, while effective responses often depend on offline evidence such as HUMINT, financial tracing, and proxy investigations. Recent cases in the Philippines and Germany show how foreign powers use troll farms and financial support to influence domestic politics. The South Korean government should revise espionage-related provisions in criminal law and enact new legislation to regulate emerging forms of foreign information manipulation and interference.

## Recommendations for the National Cybersecurity Strategy of the Lee Administration

South Korea's 2024 National Cybersecurity Strategy needs an adequate review of the previous strategy and a process for gathering stakeholder input during its revision. The Harvard Belfer Center's assessment also ranked Korea the lowest among seven countries—the United States, the United Kingdom, Germany, Australia, Japan, Singapore, and the Republic of Korea—pointing out insufficient specificity and a lack of concrete policy proposals. In particular, the exclusion of key actors such as industry, civil society, and local governments, as well as weak accountability and performance evaluation, were highlighted

as shortcomings. Moreover, it would be advisable to elevate the contents of the National Cybersecurity Basic Plan into the Strategy to produce a more comprehensive and detailed framework, while disclosing the National Cybersecurity Implementation Plan except in cases involving classified matters. Under the Lee Jae-myung administration, the new National Cybersecurity Strategy should be more comprehensive and concrete by incorporating the contents developed by the Cybersecurity Basic Plan.

Just as technological progress is critical, so too is the establishment of efficient governance through legal and institutional reforms, achievable by amending the National Intelligence Service Act and enacting new legislation. Since the National Cybersecurity Strategy falls under the authority of the National Security Office under the President, a comprehensive and detailed strategy addressing both national and international security dimensions is required. The Lee administration should focus not only on AI and cybersecurity but also on strengthening the legal and strategic foundations of national cyber defense, based on pragmatism and continuity.

## About the Author

**Dr. Shin Sohyun** is a research fellow in the Centre for Foreign Policy and National Security at the Asan Institute for Policy Studies. Her research mainly focuses on the international norm change and progress in the new spaces: cyberspace and outer space following the development of emerging technologies such as ICT, AI, space technology and quantum computing, etc. Dr. Shin has interests in interdisciplinary and socio-legal research combining new technologies and law and policy relating to armed conflict, military operations, weapons, cyber espionage and intelligence as well as disaster, environment and human rights. She was the founding member of Sejong Institute Cybersecurity Centre(2020-2022) and organised 'Cybersecurity Forum'. She worked as a research fellow of Korea University Institute of Cyber Security & Privacy. Dr. Shin published "The Regulation of State's Hostile Disinformation Operations in Cyberspace", "Space Security and International Law", and "Cyber Deterrence and US Defence Forward Strategy in International Law", etc.

This article is an English Summary of Asan Issue Brief (2025-27).
('이재명 정부의 사이버 안보 법·전략에 대한 제언')