202.464.1982 1800 K Street NW

THE PENINSULA

Changing South Korea's Espionage Law is Good for Business

Published September 24, 2024

Author: Ben Forney

Category: South Korea

Lawmakers from South Korea's two major political parties have a notoriously difficult time agreeing on much of anything. However, one issue that enjoys bipartisan support is reforming the country's espionage law, a proposal now under consideration in the National Assembly. The focus is on updating Article 98 of the Criminal Act as the legislation, in its current form, has long hindered the government's ability to prosecute offenders. While the reform measures have clear national security implications, much of the debate centers on economic security—specifically, South Korea's capacity to safeguard its commercial trade secrets from industrial espionage.

Between 2003 and 2023, South Korea experienced 552 cases of industrial secrets being leaked to foreign countries, and since 2018, these incidents have resulted in financial losses exceeding 25 trillion won, according to the National Intelligence Service (NIS). Yet, despite the large number of cases and their punishing economic impact, South Korea's legal framework has been slow to address the full scope of the problem, especially when it comes to state-sponsored intellectual property theft.

Limited Scope of South Korean Legislation

In the United States, such activities are covered under the Economic Espionage Act of 1996, which sets punishments of up to 15 years in prison and $5 million in fines for individuals who steal trade secrets to benefit entities linked to foreign governments. However, in South Korea, no legal framework directly addresses economic espionage, and the existing definition of espionage itself—codified in Article 98 of the Criminal Act—is narrowly focused on traditional threats from "enemy" states. The definition is problematic because it does not account for the evolving nature of espionage as a tool of economic statecraft, where foreign competitors and state-backed entities target critical technologies and intellectual property (IP). Since North Korea is South Korea's only legally defined enemy, espionage cases involving other nations, particularly China, which has been implicated in the majority of these cases, do not fall under this law, limiting the scope of prosecution.

It is important to recognize that overseas technology leakage represents only a small part of the industrial espionage problem in South Korea, as most incidents occur between domestic companies rather than involving foreign actors. According to the National Police Agency, of the 589 cases of industrial technology and trade secret theft reported over the past five years, 517 involved domestic parties. While these cases may pose fewer national security risks compared to leaks involving foreign competitors, they still inflict significant harm on the affected companies.

Fortunately, things are beginning to change. In recent years, there has been increasing awareness within the South Korean government of the importance of countering both domestic and foreign industrial espionage. Policymakers from both major political parties are now calling for revisions to Article 98, which would broaden the definition of espionage to include actions that benefit any foreign country, not just enemy states.

The broader implications of this change would be significant. South Korea's cutting-edge industries—including semiconductors, smartphones, and shipbuilding—are critical not only to the domestic economy but also to global supply chains. And the need to find a solution is becoming ever more urgent as these IP theft cases become increasingly brazen. One of the most shocking cases emerged in 2023 regarding the attempted theft of Samsung semiconductor fabrication plant designs by a former executive who was accused of planning to build a competing facility in China.

But while headlines often focus on high-profile cases involving South Korean *chaebols*, small and medium enterprises (SMEs) are more frequently the victims of industrial espionage. According to the National Police Agency, SMEs have constituted 89 percent of domestic and foreign technology leakage over the past five years. These SMEs, which often lack the resources to implement robust cybersecurity measures or insider threat programs, are vital players in the supply chains of major companies, producing specialized equipment and components that make them prime targets for technology theft.

South Korean Efforts to Combat Espionage

In recognition of this growing threat, the South Korean government has taken steps to address the problem. Since 2020, various new departments have been established to tackle industrial espionage, and the government has launched public awareness campaigns to educate workers on best practices for protecting sensitive technologies. The National Police Agency conducted a special crackdown on technology leakage in 2022, resulting in an increase in arrests and convictions. And in November 2023, the Yoon Suk-yeol administration launched the Pan-Government Technology Leak Joint Response Team, highlighting the whole-of-government approach needed to tackle the issue.

In addition to government action, companies are also stepping up their efforts to prevent insider threats. Many larger companies have implemented strict security protocols, such as prohibiting the use of USB devices and cameras in sensitive areas. Samsung Display, for example, has introduced a "camera filming prevention solution" to prevent technology leaks through remote work systems, though this has sparked controversy with labor unions that argue such measures infringe on workers' privacy. In more than half of industrial espionage cases, the culprits are former employees with decades of specialized knowledge who have been lured by lucrative offers from foreign firms. Several companies have responded by offering ceremonial positions to retirees to deter these kinds of defections.

Recommendations for Reducing South Korea's Vulnerability

Despite these efforts, there is still work to be done. South Korea's espionage laws must be updated to reflect the reality of economic espionage, and more stringent penalties for technology theft need to be imposed. The Industrial Technology Protection Act, introduced in 2007, has recently been strengthened to include sentencing standards comparable to US laws, but enforcement has been sporadic. And given the complex nature of many cases, trials often take years to conclude, by which time the stolen technologies are no longer cutting-edge.

But more importantly, South Korea must acknowledge the role of foreign governments—especially China—in orchestrating these espionage campaigns. The current approach, which focuses on punishing individuals who steal technology, is akin to targeting low-level criminals while ignoring the masterminds behind the operation. Economic espionage needs to be prioritized as a geopolitical issue rather than just a criminal issue. This means mitigating the risk factors associated with Chinese economic espionage efforts, including overseas networks like the United Front Work Department, talent recruitment programs that incentivize the sharing of sensitive information, and joint ventures that facilitate technology transfers.

A broader cultural shift is also needed. The rigid hierarchical structure of many Korean companies, combined with long working hours and poor work-life balance, often leaves employees disgruntled and more susceptible to sharing company secrets. Educating both workers and businesses about the national security implications of protecting IP is essential to creating a more secure environment.

Finally, South Korean companies, universities, and research institutions must be more cautious about forming partnerships with high-risk entities, including Chinese organizations linked to the People's Liberation Army (PLA) or other government departments. For example, in early September, LG Electronics announced a partnership with the Harbin Institute of Technology—one of the "Seven Sons of National Defense," which are PLA-linked universities that spearhead Chinese military research and development. The research involving LG relates to core technologies for next-generation heat pumps that have dual-use capabilities. Partnerships like this pose significant risks to South Korean national security and economic competitiveness.

Conclusion

Amending Article 98 and strengthening existing laws are necessary steps to protect South Korea's industries from economic espionage. However, a broader approach is needed—one that involves not just the government and law enforcement but also businesses, educational institutions, and society at large. Only through coordinated efforts can South Korea safeguard its position as a global leader in innovation and ensure the long-term competitiveness of its strategic industries.

Ben Forney is the author of The Spy Hunter newsletter and a PhD candidate at Seoul National University. The views expressed here are the author's alone.

Photo from Shutterstock.

KEI is registered under the FARA as an agent of the Korea Institute for International Economic Policy, a public corporation established by the government of the Republic of Korea. Additional information is available at the Department of Justice, Washington, D.C.

Return to the Peninsula

Tweet Share Share Email