THE UNIVERSITY OF TENNESSEE KNOXVILLE

CENTER FOR NATIONAL SECURITY & FOREIGN AFFAIRS

The Impact and Consequences of Chinese Scientific and Technological Acquisition from the United States and South Korea

Sojeong Lee

Jackson Craig Scott

Krista E. Wiegand

July 2025

The Impact and Consequences of Chinese Science and Technology Acquisition from the United States and South Korea

July 2025

Center for National Security and Foreign Affairs
Howard H. Baker Jr. School for Public Policy and Public Affairs
University of Tennessee, Knoxville

Sojeong Lee
Jackson Craig Scott
Krista E. Wiegand

Funded by the Korea Foundation

The Center for National Security and Foreign Affairs

The Center for National Security and Foreign Affairs (NSFA) is a research center housed in the Baker School of Public Policy and Public Affairs (Baker School) at the University of Tennessee, Knoxville. NSFA provides critical insights into national and international security challenges and foreign policy solutions through policy-relevant research, education, and engagement with a global perspective. NSFA faculty, fellows, and affiliates conduct research and publish policy briefs, reports, articles, and books that inform security and foreign affairs policy on topics of expertise:

- Indo-Pacific security & US alliances
- Territorial/maritime disputes & maritime security
- Nuclear deterrence, security, & nonproliferation
- US economic & energy security

The Baker School prepares students for careers in public service through a combination of coursework and real-world experiences. Baker students interested in national security and foreign affairs have opportunities for real-world project assignments with the US Department of State, immersive international travel experiences such as the Japan Ambassadors Program, Baker Scholars, involving a senior thesis on national security or foreign affairs, and student research experience. At the graduate level, students are integrated into a broader academic community through research projects with faculty, and the opportunity to network with visiting scholars and other experts.

About the Authors:

Sojeong Lee (PhD University of Iowa) is a Teaching Assistant Professor of Political Science at the University of Tennessee. She specializes in international conflict, water and natural resources, territorial/maritime/river disputes, climate change, and security in East Asia and Indo-Pacific.

Jackson Craig Scott (BA University of Tennessee, Knoxville) recently earned a Master of Public Policy degree from the Baker School with a concentration in national security. His research focuses on US grand strategy, US national security, and US-China relations.

Krista E. Wiegand (PhD Duke University), is Director of NSFA and Professor of Public Policy and Public Affairs at the Baker School. She specializes in international conflict, territorial and maritime disputes, alliances, dispute resolution, Indo-Pacific security, and US national security.

Table of Contents

Executive Summary

This policy report examines the impact and consequences of the acquisition of science and technology research from the United States and South Korea to China by extra-legal and illegal means. China has strategically prioritized the acquisition of foreign technology through both legal and illegal means as part of its comprehensive strategy of increasing its competitive advantage in power. The Chinese government implements a "whole-of-society" approach to technology acquisition, leveraging multiple entities including the Ministry of State Security, state-owned enterprises, private companies, universities, and military organizations.

The consequences of Chinese technology transfers are far-reaching and significant:

- **For the United States,** economic damages include job losses, market share erosion, and lost profits were estimated in 2017 to be between $225-600 billion annually, with costs higher today.

- **For South Korea,** a technological powerhouse in semiconductors and other advanced industries, the threat is particularly acute. The most notable impact of Chinese technological espionage on the South Korean government is potential damage to South Korea's national security and economic interests in national core technologies produced by South Korea including semi-conductors, ship-building, and electronics.

Chinese science and technology acquisition targets three critical sectors in both countries:

- **In government,** China directly compromises national security by accessing classified information and military technologies, including US space capabilities. Even technology developed for civilian purposes has been applied to enhance China's military capacity, which raises significant concerns if artificial intelligence, quantum computing, biotechnology, and other areas of development are applied to weapons systems.

- **In private industry** in both countries, China has employed both direct and indirect strategies to gain access to South Korean and US intellectual property. South Korea is particularly vulnerable to direct industrial espionage because it has deep economic and industrial linkages to the Chinese semiconductor industry and production. US industries are often most targeted by forced technology transfers through joint ventures and coercive business practices which require US companies to turn over control of their technologies in exchange for market access in China.

- **In academia,** China has successfully recruited researchers from both countries, resulting in unauthorized technology transfers – and in the US, the use of federal funds for research and development whose products ultimately benefit China.

Introduction: Chinese S&T Acquisition and the US-China Competition

Technological innovation is a critical factor in a country's ability to gain power, prestige, and influence and has a broad impact on international politics and security.[1] The People's Republic of China (China)[2] has "long viewed science and technology as an essential part of its 'comprehensive national power.'"[3] Technology acquisition by China has helped the country rise to become a major power.[4] Some describe China as the elephant in the room that cannot be ignored in a new international order.[5] Others assert that as China's power grows so will its appetite for a Sino-centric international system.[6] The legal, extra-legal, and illegal appropriation of science and technology (S&T) research has been directed to help China's military development,[7] a growing concern for the United States (US) and other democracies with strong S&T research programs, including South Korea.

China's strategic focus on S&T acquisition from foreign countries is not new. Indeed, China has utilized nationalistic propaganda to promote foreign IP acquisition. An often-cited Chinese slogan to encourage this process is "pick flowers in foreign lands to make honey in China."[8] As early as the 1980s, the US expressed complaints over intellectual property (IP) theft vis-a-vis China.[9] In 1991, the United States Trade Representative (USTR) conducted a Section 301 investigation into China. The six-month investigation would place sanctions on China if they were not providing the appropriate IP protection.[10] The US and South Korea have implemented several policies to mitigate the threats posed to science and technology from China. However, these efforts continue to fall short of effectively deterring and countering Chinese theft and espionage. In a 2019 Senate hearing, one expert noted that, "China was involved in 90 percent of all economic espionage cases the Department [of Justice] handled from 2011 to 2018."[11]

---

[1] Daniel Drezner, "State Structure, Technological Leadership and the Maintenance of Hegemony," *Review of International Studies* 27 no. 1 (2021): p.3-25.; Robert Gilpin, *War and Change in World Politics*, (Cambridge: Cambridge University Press, 1981).; Andrew B. Kennedy, 2016. "Slouching Tiger, Roaring Dragon: Comparing India and China as Late Innovators," *Review of International Political Economy* 23 no. 1 (2016): p. 65-92.

[2] When the People's Republic of China, the Chinese Communist Party, or China are referred to in this policy brief, the authors are referring to the government and communist party, not the people, culture, or history of China

[3] *China's S&T and Innovation Efforts: Testimony before the Subcommittee on Emerging Threats and Capabilities Committee on Armed Services*, 115th Cong. (2018) (statement from Dean Cheng, Senior Research Fellow, Asian Studies Center, The Heritage Foundation).

[4] William Hannas and Didi K. Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage* (New York: Routledge, 2021).

[5] Gerald Chan, Pak K. Lee, and Lai-Ha Chan, *China Engages Global Governance: A New World Order in the Making?* (Oxford: Routledge, 2011).

[6] Andreas Bøje Forsby, "An End to Harmony? The Rise of a Sino-Centric China." *Political Perspectives* 5 no. 3 (2011): p. 5-26.

[7] *China's Pursuit of Emerging and Exponential Technologies: Testimony before the Subcommittee on Emerging Threats and Capabilities Committee on Armed Services*, 115th Cong. (2018) (statement from Paul Scharre, Senior Fellow and Director, Technology and National Security, Center for a New American Security).

[8] Ibid, 13.

[9] Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order*, (Oxford, UK: Oxford University Press, 2021), 138.

[10] Ibid, 140-141.

[11] *Made in China 2025 and the Future of American Industry: Testimony before the Senate Small Business and Entrepreneurship Committee*, 116th Cong. 1 (2019) (statement of Bonnie S. Glaser, Director, China Power Project, Center for Strategic and International Studies (CSIS)).

As China has risen to power, the government led by Xi Jinping has supported China's economy in multiple ways. China has been using unconventional tactics to undermine the US and its allies.[12] The current economic strategy to stay competitive is asymmetric and focuses on its strengths, which includes coercive foreign technology acquisition.[13] China wishes to neutralize the advantages that the US has maintained for decades stemming from an "open, wealth seeking, highly competitive economy."[14] A means to challenge this advantage has been for China to pursue IP theft and conduct espionage against foreign countries to help grow the Chinese economy and strengthen China's national defense. Another way to understand the context of today's challenges from China is by using the term "irregular competition," described as "state and nonstate actors engaging in activities during times of peace, competition, and war to influence populations and affect legitimacy."[15] Intellectual property theft and espionage fall under the category of irregular competition.

The results of these efforts by China have been significant threats to economic and national security interests in the US, South Korea, and several other allies that are liberal democracies with strong scientific and technological sectors. In 2020, Christopher Wray, Director of the US Federal Bureau of Investigation, noted about China's threats to the US, "the great long-term threat to our nation's information and IP, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security – and by extension, to our national security."[16] Additionally, in 2023, the House Foreign Affairs Committee released a report regarding the Department of Commerce's Bureau of Industry and Security, stating that "the unimpeded transfer of US technology to China is one of the single-largest contributors to China's emergence as one of the world's premier scientific and technological powers. For more than 20 years, the Chinese Communist Party has circumvented our export controls and deceived the US officials in charge of administering them."[17]

In this policy report, we examine and assess the impact and severity of Chinese technology transfers that are legal, extra-legal, and illegal, mainly through IP theft and technological espionage, on the US and South Korea. A companion report that we wrote provides an overview and assessment of efforts by the governments and academic institutions in the US and South Korea in countering Chinese S&T technology transfers.[18] A report outlining

[12] Jeremiah C. Lumbaca, "Irregular Competition: Conceptualizing a Whole-of-Government Approach for the United States to Indirectly Confront and Deter State and Nonstate Adversaries," *Military Review* 102, no. 4 (2022): 44.
[13] Dan Blumenthal and Derek Scissors, *China's Technology Strategy: Leverage before Growth* (Washington, DC: American Enterprise Institute, 2023), 1.
[14] Ibid.
[15] Lumbaca, 48-49.
[16] Christopher Wray, "The Threat posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Transcript of speech delivered at Hudson Institute, Washington, DC, July 7, 2020, https://www.fbi.gov/news/speeches-and-testimony/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.
[17] US House of Representatives Foreign Affairs Committee, *Bureau of Industry & Security: 90-Day Review Report*, (Washington, DC: US House of Representatives, 2023), 1.
[18] Krista E. Wiegand, Jackson Craig Scott, and Sojeong Lee, *Policy Efforts and Recommendations to Counter Chinese Science and Technology Acquisition in the United States and South Korea* (Knoxville, TN: Center for National Security and Foreign Affairs, Howard H. Baker Jr. School for Public Policy and Public Affairs, University of Tennessee, Knoxville, 2025).

discussions by US and South Korean experts at a November 2024 conference held at the Center for National Security & Foreign Affairs at the Baker School at the University of Tennessee also provides further assessment about the current challenges and policy approaches.[19]

This report first briefly reviews China's national policy and means of promoting foreign IP and technology acquisition. Next, we examine and assess the impact and consequences of Chinese scientific and technological transfers for the US and South Korea. China's legal, extra-legal and illegal technology acquisitions have been conducted in various areas, including the government, private industry, and academia in both countries. The report walks through each of these main target areas to discuss Chinese transfer, theft, and espionage strategies and activities. We conclude with a summary of the implications of Chinese technological acquisition strategies for American and South Korean national security and the US-China competition in general.

China's Science & Technology Acquisition Strategies

China has ample reason to seek science and technology gains since it has found itself facing the "innovation imperative," which is when a rising state must work to "acquire and create new technologies to meet specific short- and long-run growth objectives...The challenge for the rising power is to develop a strategy and policies to acquire these technologies from the advanced wealthy states that developed them. In the long run, as its economy approaches the technological frontier, the rising power must develop products and processes that are new to the world."[20]

Rising states innovate in three main ways: making, transacting, and taking. The taking strategy includes the acquisition of knowledge through open-source means, which could also include "the acquisition of knowledge that is not in the public domain from non-consenting targets."[21] As China began to develop economically at the end of the 20th century, it became increasingly common practice to acquire IP and research from other countries. China has adopted an official military-civil fusion strategy to assist in its rise in power. The US Department of State defines "Military-Civil Fusion," or MCF, as the Chinese national strategy to develop its military to be the most technologically advanced in the world.[22] This goal can be achieved through research and development efforts, where China has invested significantly in recent years. Although not publicly admitted, another key strategy that the Chinese Communist Party (CCP) has pursued is to acquire other countries' advanced technologies via legal, illegal, and extralegal transfers of technology, ranging from transferring open-source data from universities where research is openly published to IP theft and espionage. Such strategies by China not only threaten international business and industry but also pose grave security threats to the countries whose

[19] Aom Boonphatthanasoonthorn, et. al, *Threats to the Open Scientific and Technological Ecosystem in the United States and the Republic of Korea from the People's Republic of China: Conference Report* (Knoxville, TN: Center for National Security and Foreign Affairs, Howard H. Baker Jr. School for Public Policy and Public Affairs, University of Tennessee, Knoxville, 2025).
[20] Andrew B. Kennedy and Darren J. Lim, "The Innovation Imperative: Technology and US-China Rivalry in the Twenty-first Century," *International Affairs* 94, no. 3 (2018): 556-557.
[21] Ibid.
[22] US Department of State, *Military-Civil Fusion and the People's Republic of China*, (Washington, DC: US Department of State, n.d.).

technologies and industries were targeted by China, as such cutting-edge technologies are critical to economic development and national security. Specifically, the International Intellectual Property Alliance estimated losses from IP theft by China at $415 million in 1992, and as much as $2.8 billion in 1997.[23]

China has instituted multiple policies to assist with technology acquisition and is able to use many elements of society to support its foreign S&T acquisition efforts, including many government agencies, universities, military liaison programs, and private citizens. By using a societal approach to IP theft, China has created the "first digital authoritarian state."[24] The Chinese government utilizes a whole-of-society strategy by giving incentives to its citizens to conduct espionage.[25] In an attempt to surpass the US in economic power, China has enacted several laws to create a whole-of-society approach for Chinese citizens and officials to illegally obtain IP.[26] The whole-of-society nature of China's efforts are shown by the six diverse entities that conduct most of the IP theft and espionage: the Ministry of State Security, the Central Military Commission, state-owned enterprises, private companies and individuals, the United Front Work Department, the People's Liberation Army (PLA) Political Department Liaison Office, and universities administratively under or under contract to the State Administration for Science, Technology, and Industry for National Defense.[27] Importantly, China's foreign S&T collection efforts are closely linked to technologies that have been prioritized by China, emphasizing the state-backed nature of this strategy.[28]

There are several motivating factors for actors in China outside of the government to participate in China's acquisition of foreign S&T knowledge. The government recruits people to commit IP theft and economic espionage in a few different ways: money, ideology, coercion, or ego. 62 percent of those who conducted economic espionage were motivated by business interests and are usually working in private companies.[29] Regarding technology export violations, money was the primary reason why people committed espionage; most of these criminal cases were not isolated events.[30] Other motivators in Chinese recruitment efforts are business opportunities, ethno-nationalism, academic advancement, threats of repression, and emotional bonds.[31]

When assessing the types of Chinese foreign technology acquisition, they can be placed into three categories: legal transfers, illegal transfers, and extralegal transfers. Examples of legal transfers are China-based foreign subsidies, conferences and colloquia, and startup competitions. Types of illegal transfers include breaches of contract, copyright infringement, and reverse engineering. Extralegal transfers – those that happen outside of legal norms which

[23] Ibid, 566.
[24] Eftimiades, Nicholas, *Chinese Espionage: Operations and Tactics, 2nd Ed.* (Columbia, SC: Vitruvian Press, 2025), 5-7.
[25] Ibid, xi.
[26] Ibid, 5-7.
[27] Ibid, 9-10.
[28] Ibid, xi.
[29] Ibid, 37-39.
[30] Ibid, 45.
[31] Ibid, 46-47.

makes the legality unknowable – include document acquisition facilities, recruiting and brokerage websites, and transfer incentive programs.[32] Personnel involved in extralegal efforts include professional facilitators, scientists, overseas scholars, and entrepreneurs, and S&T intelligence workers.[33] Also included in the extralegal strategies are hundreds of talent programs in China, the best-known of which is the Thousand Talents Plan in which the Chinese government recruited experts, mainly Chinese living abroad, to go to China to work in science and technology. This program has been replaced by the Qiming Program, overseen by the Ministry of Industry and Information Technology, and includes multiple recruiting efforts targeting both Chinese and non-Chinese experts to work in China. Many IP transfers happen in this extralegal space, a legal gray zone, where the legal status of S&T acquisition by China is not clear.[34] Such "insider threat[s], and co-optation, platforms exploit access to the free flows of information and trade that characterize open societies."[35]

The main distinction of the Chinese threats in the US and South Korea is that most IP theft and espionage is conducted by South Koreans, not Chinese individuals. This is different from the context in the US, in which Chinese nationals and Chinese-American individuals primarily are the ones pursuing extralegal and illegal S&T acquisition.

Impacts and Consequences of Chinese S&T Acquisition for the US & South Korea

The intensifying technological competition between the US and China challenges the South Korean-US alliance. China increasingly invests in critical technological areas like 5G and 6G networks, AI, advanced computing, and semiconductors, all of which are cutting-edge technology sectors with significant economic importance for both South Korea and the US. China's bold moves in critical technology areas pose challenges and issues to the South Korean-US alliance in developing collective capabilities to maintain their cutting-edge position in S&T and enhance cybersecurity.[36]

A research survey pursued by the Center for Strategic and International Studies (CSIS) provides details of S&T espionage directed at the US government since 2000, noting that "Chinese espionage is undertaken in pursuit of China's strategic objectives," whereas previous efforts consisted mainly of commercial espionage by the Chinese government and companies.[37]

---

[32] Hannas and Huey-Meei Chang, "Chinese Technology Transfer," 7.
[33] Ibid, 8.
[34] *Managing the Dual Challenges of Chinese Technology Appropriation and China's Progress toward General Artificial Intelligence (AGI): Testimony before the House Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet*, 118th Cong. (2023) (statement of William C. Hannas, Research Professor and Lead Analyst, Center for Security and Emerging Technology, Georgetown University).
[35] Matthew Johnson, *China's Grand Strategy for Global Data Dominance*," CGSP Occasional Paper Series No. 2 (Stanford, CA: Hoover Institution), 38-39.
[36] Mark Bryan Manantan and Soyoung Kwon, eds., 2023. *Strengthening ROK-US Critical Technologies Cooperation: Progress and Path Forward* (Honolulu, HI: Pacific Forum International and George Mason University – Korea, 2023).
[37] CSIS, "Survey of Chinese Espionage in the United States Since 2000," *CSIS* (Washington, DC), 2023, https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

Disruptive technologies such as artificial intelligence, cyber weapons, quantum computing and communications, biotechnology, data analytics, can lead to a variety of problems when applied to weapon systems. First, systemic problems such as strategic stability exacerbate existing threats, transform the nature of conventional threats, and affect political, physical and digital security.[38] Second, strategic problems undermine other states' nuclear deterrence, and malware can spread from conventional to nuclear systems.[39] Third, decision-making processes may shorten the ability of policymakers to respond or may take the human out of the loop.[40] Fourth, tactical challenges may include AI and computational fueled disinformation and propaganda that lead to political instability.[41] Lastly, cyberattacks and the shutdown of internet-connected critical infrastructure can be problematic.[42]

Similarly, China has strategically recruited South Korean technology experts from South Korean firms in critical sectors, like semiconductors and batteries, by providing incomparably high salaries since launching its "Made in China 2023" program in 2015.[43] According to the South Korean Ministry of Trade, a total of 165 cases of industrial technology overseas leakages were detected from 2016 to 2023, of which 49 cases were related to national core technology, including semiconductor, electricity/electronics, shipbuilding, and displays.

Three main sectors are threatened in the US and South Korea by extra-legal and illegal S&T acquisition by China: government institutions, private industry, and academia. These threats cause damage to both US and South Korean economic and national security interests.

Figure 1 shows the number of publicly reported Chinese espionage incidents over time in the US.[44] Chinese espionage has been increasing in frequency and scope as the government has focused more on hostile policies of hacking and technological and economic espionage. According to CSIS data and analysis, among the reported and confirmed espionage cases, 49% directly involved Chinese military or government employees and 41% involved private Chinese citizens. Specifically, 29% of incidents were targeted to acquire military technology; 54% sought to acquire commercial technologies, and 17% of the incidents were attempts to gain information on US civilian agencies or politicians.

[38] James Johnson, "Artificial Intelligence & Future Warfare: Implications for International security," *Defense & Security Analysis* 35 no. 2 (2019): p. 147-169.
[39] Lawrence J. Cavaiola, David C. Gompert, and Martin Libicki, "Cyber House Rules: On War, Retaliation and Escalation," *Survival* 57 no. 1 (2015): p. 81-104.
[40] Johnson, p. 147-169.
[41] Katarina Kertysova, "Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and can be Countered," *Security and Human Rights* 29 no. 1-4 (2018): p. 55-81.; Christopher Whyte, "Deepfake News: AI-Enabled Disinformation as a Multi-Level Public Policy Challenge," *Journal of Cyber Policy* 5 no. 2 (2020): p. 199-217.
[42] Junaid Chaudhry, et. al, "Threats to Critical Infrastructure from AI and Human Intelligence," *The Journal of Supercomputing* 74 (2018): 4865-4866.; Simona R. Soare and Joe Burton, "Smart Cities, Cyber Warfare and Social Disorder," in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* eds. A. Ertan, K. Floyd, and T. Stevens (Brussels: NATO Cooperative Cyber Defence Centre of Excellence, 2020), p. 108.; Brandon Valeriano, Benjamin Jensen, and Ryan Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018).
[43] Hannas and Tatlow, 2021.
[44] CSIS, "Survey of Chinese Espionage in the United States Since 2000."

Figure 1. Total Chinese Espionage Cases in the United States

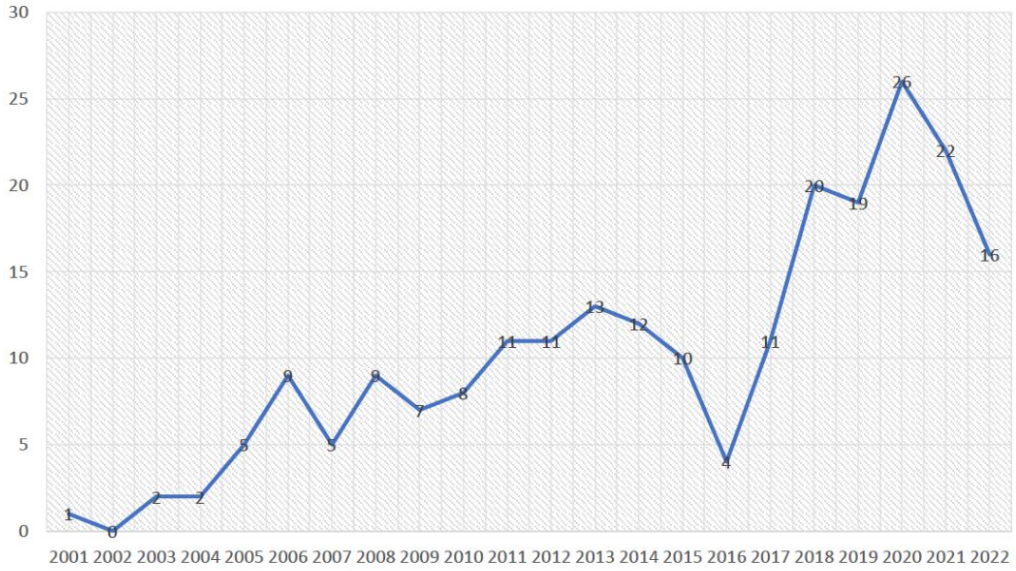
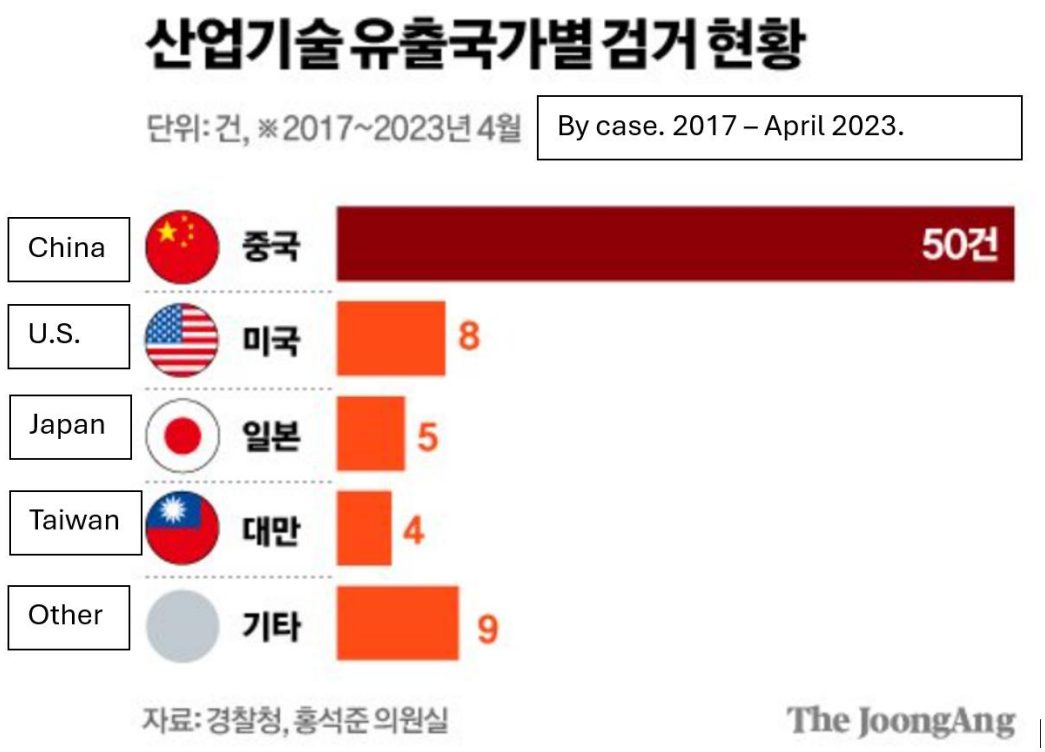


Image: CSIS

Compared to the state of Chinese S&T acquisition from the US, there has been limited systemic analysis and assessment of the scope and intensity of Chinese espionage in South Korea's various sectors. Several individual cases have been reported via news stories, and the National Intelligence Service has provided general case overviews in recent years. The National Police Agency provides the number of arrests involving industrial technology leaks by country, as presented in Figure 2.[45] With those provided data, it is apparent that China is the number one actor in technological espionage and IP theft. Still, the statistics and reports are in many cases a simple count of cases, rather than an analysis and assessment of exactly which areas and expertise have been targeted by China's acquisition strategies. Therefore, in this report, instead of looking at specific numbers or technology, we look at three major sectors that have been targeted by China's espionage and gray zone tactics toward the US and South Korea: government, private industry, and academia.

[45] Heekwon Lee, "They Kicked Out Koreans Without Severance Pay … China is Now OLED Talent Hunting," *The JoongAng* (Seoul), July 13, 2023, https://www.joongang.co.kr/article/25177289.

Figure 2. Number of arrests involving industrial technology leaks, by country



US Government Impacts

China's S&T acquisition hurts the US government in multiple ways: by removing jobs from the US, loss of profit due to counterfeit and pirated tangible goods and software piracy, technological competition, faster speeds of production by China, negatively affecting US market share. 76% of counterfeit goods seized in the US are from China; that number rises to 87% if you include Hong Kong.[46] According to a US Senate report, IP theft and production of counterfeit goods creates 8% of China's GDP (though not all of this may be from S&T industries).[47] China has also accelerated its military development in part because of stolen technology from the US and its allies. China targets US space capabilities like advanced space optics, sensors, cryogenic coolers, composites, engine design, fabrication techniques, software, and others.[48] The US Department of Justice states that 80% of economic espionage cases involve China.[49]

One strategy China pursues is somehow collecting information from people connected to the US government. In 2013, China attempted to obtain the personal information of US federal employees from the Office of Personnel Management.[50] In 2022, the FBI stated that China had

[46] Eftimiades, 174.
[47] Ibid.
[48] Ibid, 175.
[49] Derek Scissors, "The Rising Risk of China's Intellectual-property Theft," *National Review* (New York City), July 16, 2021.
[50] Scissors, "The Rising Risk of China's Intellectual-property Theft."

targeted US citizens with ties to the intelligence community, with a goal of collecting important US government and military secrets and the country's "most sensitive information."[51]

Theft of military technology is also a known problem. When China released its Fifth Generation fighter jet, which had similarities to the US F-35, some linked this to a 2008 CCP-sponsored hack of the Pentagon Joint Strike Fighter Project.[52] In 2014, a Chinese citizen pled guilty to stealing military technical data, some of which related to the C-17 aircraft and other fighter jets that were produced by private firms for the US government. The person also admitted to conspiring with two people in China from 2008 to 2014.[53] While this problem stems from security failures in private industry, it impacts the US government as well. The long-term threat to the US government is not simply the loss of IP. China has shown that from its perspective, "new technology is not primarily a means to improve people's lives; it's primarily a means to enhance party supremacy."[54]

A surprising transfer of technology to China is from DOD funded grants to universities and national labs. At least $48 million of DOD-funded research has benefited Chinese military-linked firms, either directly or indirectly through joint research conducted by US researchers and Chinese researchers who are affiliated with malign Chinese entities.[55] These entities are key pieces of China's military industrial complex. Participants of China's Thousand Talents participants have been hired by US national labs operated by the US Department of Energy. Here, participants are utilizing funding from the US federal government to make innovations in fields such as technology and medicine. Then, they transfer the research back to China.[56] Additionally, US researchers are working either knowing or unknowingly with Chinese universities that are on US government lists of Chinese military affiliated institutions with which US institutions should not work. Examples of DOD entities involved in these types of funding include the Army Research Office, Office of Naval Research, and Air Force Office of Scientific Research.[57] Thus, the DOD is utilizing US tax dollars to fund Chinese capabilities either unknowingly or unwittingly in fields such as semiconductors, quantum computing, artificial intelligence, cyber warfare, telecommunications, and biotechnology. Each of these sectors are strategically important for China's military modernization.[58] The examples are staggering. In one instance in November of 2024, the Massachusetts Institute of Technology received $24 million from the Army Research Office for a research project conducted with i Technologies in

[51] Matthew Olsen, "Assistant Attorney General Matthew Olsen Delivers Remarks on Countering Nation-State Threats," transcript of speech delivered in Washington, DC, February 23, 2022, https://www.justice.gov/archives/opa/speech/assistant-attorney-general-matthew-olsen-delivers-remarks-countering-nation-state-threats.
[52] Alec Goodrich, "International Intellectual Property Theft: Background Framework for Private Enforcement," *International Law and Policy Brief* (2022).
[53] *How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy: Testimony before the House Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet*, 118th Cong. (2023) (statement from Benjamin Jensen, Senior Fellow, International Security Program, CSIS).
[54] Ibid.
[55] LJ Eads, *Undermining Deterrence: The Case for a Total Ban of DoD Research Involving Chinese Military Companies*, (Beavercreek, OH: Parallax Advanced Research, 2025, 3-5.
[56] Blake Wiseman, "Stolen Riches: Stopping China's Continued Theft of American Intellectual Property," *Ave Maria Law Review* 22 (2024): 200.
[57] Ibid.
[58] Ibid, 3.

China, a telecommunications and artificial intelligence company that has extensive ties to the People's Liberation Army.[59] Just in the past two years, there have been 17 documented cases of DOD-funded collaborative research projects involving top US universities and Chinese military companies.[60]

US Private Industry Impacts

While China's legal and extra-legal means of S&T acquisition from the US government is increasingly common, illegal Chinese industrial espionage has been ongoing for several decades. The Chinese target a wide range of industrial sectors and technologies in private industry, many of which are central to industrial development and technological advancement of the US. China has created a network of data clusters while at the same time creating new policies to reinforce the obligations of industry and corporations to help the Chinese government with its science, technology, and national security goals. An expert explains, "Through this emerging system of data accumulation and transfer platforms, commercial data in strategically important – and nationally sensitive industries is drawn into an entire ecosystem designed to facilitate long-term sustained espionage, IP theft, and interference."[61]

The major IP theft from global companies by China has been the foundation of its rapid economic rise. Its innovation and technology strategy is built on "forced technology transfer, cybertheft, massive state-led capital investment, and global strategic acquisitions done by state-run corporations." This strategy has made American firms the research and development arm of China and its firms.[62] Chinese industrial espionage has targeted a wide range of industrial sectors and technologies, many of which are central to industrial development and technological advancement not only in the US but in allies such as South Korea, Japan and Taiwan.[63] China has a well-developed network of strategies to target advanced science and technology firms. The Chinese government engages in legal but coercive business practices such as requiring IP transfer from foreign companies to China in exchange for market access or more favorable market access.[64] China prefers a joint venture model of corporate structure to require the transfer of IP and expertise, involving corporate contracts that ensure the Chinese firm, often a state-owned enterprise, keeps the control over the joint venture. Chinese regulation forces foreign firms to help with advanced technology, providing Chinese partners control over the technology that was transferred from the foreign firm.[65] China gives its companies large state subsidies and uses a zero-sum strategy to erode foreign firms that are competitive. Chinese theft of IP and forced technology transfers hurts joint innovation and

[59] Ibid, 4-5.
[60] Ibid.
[61] Matthew Johnson, *China's Grand Strategy for Global Data Dominance*," CGSP Occasional Paper Series No. 2 (Stanford, CA: Hoover Institution), 38-39.
[62] Johnathon DT Ward, *China's Vision of Victory* (Atlas Publishing and Media Company, LLC: Rancho Sante Fe, 2019), 113.
[63] Yong, "Industrial Espionage."
[64] Dan Blumenthal and Derek Scissors, *China's Technology Strategy: Leverage before Growth* (Washington, DC: American Enterprise Institute, 2023), 3.
[65] Karen M. Sutter, "Foreign Technology Transfer through Commerce," in *China's Quest for Foreign Technology: Beyond Espionage*, eds. William C. Hannas and Didi Kirsten Tatlow (Milton Park, Abingdon, Oxon: Routledge, 2021), 57-58, 62-64.

investments by US and private Chinese companies.[66] In 2018, 75% of members of the American Chamber of Commerce in China reported they increasingly did not feel welcome, which reflects the sentiment amongst foreign-invested companies in China that they were not treated like domestic companies.[67]

The sectors China targets in its attempts to gain foreign technology are listed in their *Made in China 2025* plan: aerospace, advanced manufacturing, artificial intelligence, biotechnology, data analytics, new materials, and semiconductors, among others.[68] All of these are key areas of research that affect US national security and interests of the US government. The main mechanisms for China to obtain foreign IP and trade secrets are through the funding of key industries, foreign investment approvals, taxes, corporate structures (as mentioned previously), corporate theft and espionage, procurement, standards, IP, antitrust, trade barriers, market pressures, and overseas investments.[69]

China's espionage activities in the US that have led to criminal charges have involved mainly illegal export of military and dual-use technology. These include infractions against the International Energy Economic Powers Act, Export Administration Regulations, Arms Export Control Act, and International Traffic in Arms Regulations. China's espionage usually centers around Massachusetts, Michigan, New York, Pennsylvania, Florida, New Jersey, and Texas. This is because of the presence of major educational, research, and manufacturing facilities in these states. The place with the highest frequency of Chinese illegal technology transfers in the US is northern California, home to many Silicon Valley companies innovating and performing cutting edge research in technology. In California, the priority industries for the Chinese are information technology, aerospace, and aeronautical equipment, followed by automated machine tools and robotics, then biotechnology.[70]

Examples from private industry can shed light on the types of IP theft and economic espionage used by China. A US citizen, Zheng Xiaoqing, who worked for General Electric Power (GE), used a technique called steganography where he "hid confidential files [he] stole from his employers in the binary code of a digital photograph of a sunset, which Mr[.] Zheng then mailed to himself."[71] The information was related to the design and creation of gas and steam turbines. He sent this information to an accomplice in China where it would then benefit the Chinese government, companies, and universities. The information was estimated to be worth millions of dollars.[72] In November of 2022, a Chinese national plotted to illegally obtain trade secrets from multiple US aviation and aerospace companies; one of these was also GE.[73] Other charges by the Department of Justice for theft and espionage include stealing technology from oil and

[66] Johnathon DT Ward, *China's Vision of Victory*, 112.
[67] Ibid, 111.
[68] Karen M. Sutter, "Foreign Technology Transfer through Commerce," in *China's Quest for Foreign Technology: Beyond Espionage*, eds. William C. Hannas and Didi Kirsten Tatlow (Milton Park, Abingdon, Oxon: Routledge, 2021), 57-58, 62-63.
[69] Ibid, 60-69.
[70] Eftimiades, 20-22.
[71] Nicholas Yong, "Industrial Espionage."
[72] Ibid.
[73] Ibid.

gas manufacturers, malicious web shells placed on computers in the US, allowing the Chinese government access to US computer networks, stealing trade secrets about silicon carbide MOSFET technology from GE, illegal exporting of maritime raiding craft and engines to China, and unlawful exports of dual-use electronics components.[74]

China's coercive practices have led to harm for US industries that make solar panels, wind turbine control software, steel manufacturing, autonomous vehicles, and semi-conductor chips.[75] In 2019, CNBC surveyed CFOs of leading companies in the US. The results showed that 20% of companies had IP stolen from China in the past year. A 2017 report estimated that the total theft of US IP – not only from China, but all countries - amounted to losses of $225 billion annually, and stolen trade secrets cost up to $600 billion per year.[76] Since China threatens economic retaliation against firms that do not comply, most firms do not take their case to the World Trade Organization.[77] Firms that are impacted by Chinese IP theft and economic espionage include a large range of subfields of S&T. For example, China has attempted to steal secrets about genetically modified corn in Iowa and from Apple, Coca-Cola, DuPont Chemicals, and US aviation companies.[78] China has also attempted to steal cutting-edge semi-conductor technology and seeds for pharmaceutical purposes that took millions of dollars of investment and years of research to develop.[79]

US Academia Impacts

The Chinese government engages in "picking flowers in foreign lands to make honey at home,"[80] by having Chinese and foreign scholars transfer S&T research to China through legal, extra-legal, and illegal means. China not only relies on PLA military scientists and engineers, but also Chinese students and scholars studying abroad and on its university collaborations with foreign institutions,[81] as well as US scholars in some cases.

Chinese academics, professors, and researchers in universities and laboratories have provided immense value to the US and the world. However, some Chinese citizens have cooperated with the Chinese government to steal IP and research. Foreign adversary countries, particularly China, have influenced higher education institutions in the US to further their strategic, military, and economic goals. These adversaries understand that academia is the foundation of US innovation, science and technology leadership, and economic competitiveness. These countries use open science and technology research in the US to exploit IP so that they do not have to

[74] "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," US Department of Justice, November 19, 2021, https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.
[75] Eftimiades, 174.
[76] Commission on the Theft of American Intellectual Property, National Bureau on Asian Research, "The Theft of American Intellectual Property: Reassessments of the Challenge to the United States," 2017.
[77] McMaster, 145.
[78] Goodrich, "International Intellectual Property Theft: Background Framework for Private Enforcement."
[79] Olsen, "Assistant Attorney General Matthew Olsen Delivers Remarks on Countering Nation-State Threats."
[80] Alex Joske, *Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities*, Report No. 10/2018 (Canberra: Australian Strategic Policy Institute, 2018).
[81] Alex Joske, *The China Defence Universities Tracker: Exploring the Military and Security Links of China's Universities*, Report No. 23/2019 (Canberra: Australian Strategic Policy Institute, 2019).

bear the large costs and risks of doing their own research.[82] Nor does China attempt to hide what it is doing. Xi Jinping in 2013 emphasized the importance of utilizing US universities to help serve China.[83]

China's talent plans, the most notable being the Thousand Talents Program, place people willing to support the Chinese government in businesses, laboratories, and universities. People abroad loyal to China receive incentives to obtain research from universities and laboratories. The programs themselves are not illegal but the operations, undisclosed and illegal transfers of information, hurt US universities and laboratories.[84] Some Chinese professors and researchers are stealing data from universities or national laboratories and then going back to their other place of employment in China and training Chinese citizens with the stolen IP.[85] Others are US citizens, mainly Chinese-American, but not exclusively, who have close ties to Chinese universities. Those charged by the Department of Justice during the China Initiative investigations included professors and researchers at University of Florida, MIT, University of Arkansas, Emory University, West Virginia University, University of Kansas, and Southern Illinois University.[86]

Some Chinese civilian universities are a part of their military-civil fusion program, collaborating with American counterparts to obtain access to field-leading research in the US. This research is then transferred to China's military, assisting in its rising capacity to challenge the US military. China weaponizes what might appear as benign programs – student exchange programs, non-immigrant visa processes, and research collaborations – to obtain sensitive information and next-generation technology. Many of these talent programs are overseen by the Chinese military. Thus, Chinese talent programs directly assist China's military development. China obtains access to next-generation research which is not classified, but can have dual purpose, both civilian and military.[87] The DOD released a list of Chinese research institutions that support China's military and intelligence goals. As of 2023, four of those universities have over 70 known partnerships with America's leading universities. Many of these, such as MIT, Harvard, and Yale, receive US government funding for research and development.[88] There have even been cases of IP theft at the National Institutes of Health (NIH), NASA, and national laboratories including Los Alamos National Laboratory.[89] In 2018, the NIH sent a letter to thousands of research institutions warning that some NIH funding recipients had sent IP to other countries,

[82] *Exposing the Dangers of the Influence of Foreign Adversaries on College Campuses, Testimony before the House Committee on Education and the Workforce, Subcommittee on Higher Education and Workforce Development*, 118th Cong. (2023) (statement from Craig Singleton, China Program Deputy Director and Senior Fellow, Foundation for Defense of Democracies).
[83] Ibid.
[84] Blake Wiseman, "Stolen Riches: Stopping China's Continued Theft of American Intellectual Property," *Ave Maria Law Review* 22 (2024): 198-199.
[85] Ibid, 200.
[86] "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," November 19, 2021.
[87] *Exposing the Dangers of the Influence of Foreign Adversaries on College Campuses, Testimony before the House Committee on Education and the Workforce, Subcommittee on Higher Education and Workforce Development*, (Singleton).
[88] Ibid.
[89] "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," November 19, 2021.

given private application data to foreign entities, attempted to impact funding decisions, and did not disclose resources they were receiving from foreign governments which distorted the decisions on the use of funds from NIH.[90] Yet the problem of IP transfers from academia continue.

South Korean Government Impacts

US allies such as South Korea, Japan and Taiwan have also been targeted by Chinese industrial espionage.[91] Possibly the most notable impacts of Chinese technological espionage on the South Korean government are the potential damage to South Korea's national security and economic interests based on national core technologies produced by the country. The government defines national core technologies as those "likely to have a significant adverse impact on national security and the development of the national economy if leaked overseas due to high technological and economic value or high growth potential of related industries and special management."[92]

According to the South Korean Ministry of Trade, almost a third of the total cases of industrial technology overseas leakages from 2016 to 2023 were related to national core technologies, including semiconductor, electricity/electronics, shipbuilding, and displays.[93] As Chinese technological and industrial espionage activities have focused on South Korea's national core technology, it poses grave threats to South Korea's national security and government capacity to sustain South Korea's economic and technological leadership. As the Ministry of Trade, Industry and Energy indicated in its press release in December 2023, "foreign investments with high chances of strategic technology leaks (also) come under the scope of national security deliberation."[94] South Korean National Intelligence Service (NIS) Director Kim Kyou-Hun made a remark in this sense, saying "for the past two decades, the National Industrial Security Center (NISC) has worked together with private industry to strengthen the national core technologies and industrial competitiveness," also noting "the NIS commitment to safeguarding the technologies pivotal to Korea's future."[95]

Chinese espionage strategies in some cases more directly target South Korean government officials and agencies. In 2024, a civilian employee at the Korea Defense Intelligence Command

[90] Jeffrey Stoff, "Sino-Foreign Research Collaboration," *China's Quest for Foreign Technology: Beyond Espionage*, eds. William C. Hannas and Didi Kirsten Tatlow (Milton Park, Abingdon, Oxon: Routledge, 2021), 170.
[91] Nicholas Yong, "Industrial Espionage: How China Sneaks out America's Technology Secrets," BBC News (London), January 16, 2023, https://www.bbc.com/news/world-asia-china-64206950.
[92] Sang-yong Park, "Last year, there were 23 cases of industrial technology being leaked overseas, the highest ever … 'Semiconductors' more than half." *Kyunghyang* (Seoul). February 6, 2024, https://www.khan.co.kr/article/202402061521001.
[93] Ministry of Trade, Industry and Energy, "MOTIE and NIS hold joint Industrial Security Conference 2023 for Industrial Technology Protection Day," Press Release, Seoul, Ministry of Trade, Industry and Energy, November 23, 2023. https://english.motie.go.kr/eng/article/EATCLdfa319ada/1562/view.)
[94] Ministry of Trade, Industry and Energy, "MOTIE to receive options on proposed amendments to Foreign Investment Promotion Act", Press Release, Seoul, Ministry of Trade, Industry and Energy, December 22, 2023. https://english.motie.go.kr/eng/article/EATCLdfa319ada/1624/view.
[95] Ministry of Trade, Industry and Energy, "MOTIE and NIS hold joint Industrial Security Conference 2023 for Industrial Technology Protection Day," Press Release, Seoul, Ministry of Trade, Industry and Energy, November 23, 2023. https://english.motie.go.kr/eng/article/EATCLdfa319ada/1562/view.)

was arrested and formally indicted on charges, including nearly 30 counts of bribery and handing over sensitive data either in document or voice message format to a suspected Chinese intelligence agent since 2019.[96] The leaked information contained a list of undercover agents from the command who were operating in China, Russia, and other countries, according to the military prosecutors. It was an eye-opening moment to many South Korean government agencies and officials, as it proved that Chinese espionage and infiltration tactics have penetrated into the South Korean government sector, severely risking South Korea's national security.

South Korean Private Industry Impacts

South Korea serves as one of the key players, along with Japan and Taiwan, in high-tech supply chains and technological innovations capabilities.[97] As the US-China technological competition intensifies, South Korea's leading position in high-tech industries and semiconductors supply chains, especially with strategic competition with Japan and Taiwan and led by the US, make it a frequent and attractive target for technological espionage and IP theft.[98]

South Korea is particularly vulnerable to Chinese espionage strategies and illegal IP theft as South Korea has deep economic and industrial linkages to the Chinese semiconductor industry and production. Samsung and SK Hynix, South Korea's two largest memory producers and two of the world's leading companies in semiconductor and high-technology industry, have a significant share of their global memory production located in China. Given the intensifying tensions between the US and China and their technological competition, both Samsung and SK Hynix have considered and planned to move their production facilities out of China and relocate back on Korean soil to avoid any unnecessary exposure to economic disadvantages like export controls and tariffs.[99] This relocation strategy also serves to protect Samsung and SK Hynix from Chinese espionage and illegal theft and poaching of human capital, IP, and core technology. As pointed out by industry officials at CSIS, "Chinese talent poaching from Samsung and SK Hynix's Chinese production facilities played a major role in the rapid technological ascent of both YMTC and CXMT. If operating leading-edge facilities in China requires training the workforce of your Chinese competitors, Samsung and SK Hynix will certainly view that as a less attractive option."[100]

[96] "South Korea Says an Official Leaked a Classified Spy Roster to China," *New York Times* (New York City), August 30, 2024.
[97] Seungjoo Lee, "US-China Technology Competition and the Emergence of Techno-Economic Statecraft in East Asia: High Technology and Economic-Security Nexus," *Journal of Chinese Political Science* 29 (2023): 397-416, (https://doi.org/10.1007/s11366-023-09878-8)
[98] Mark Button, "Editorial: Economic and Industrial Espionage," *Security Journal* 33 (2020): 1-5.
[99] Allen, "China's New Strategy for Waging the Microchip Tech War," 16.
[100] Ibid. 16-17

Table 1: Number of detected overseas leaks of national core technologies in South Korea, by year and industry type

division	2016	2017	2018	2019	2020	2021	2022	2023	Sum
semiconductor	-	-	-	2	2	One	3	One	9
electrical/electronic	2	One	-	One	One	2	-	-	7
Shipbuilding	6	2	2	-	2	One	-	-	13
display	-	-	3	-	One	2	-	One	7
information and communication	-	-	-	-	One	2	-	-	3
automobile	-	-	-	2	One	One	-	One	5
biotechnology	-	-	-	-	-	-	-	-	0
chemistry	-	-	-	-	-	-	-	-	0
machine	-	-	-	-	One	One	One	-	3
etc	-	-	-	-	-	-	-	-	0
Sum	8	3	5	5	9	10	4	3	47

Source: "Over the past 8 years, 47 cases of national core technology have been leaked overseas… Ministry of Trade, Industry and Energy "Sentencing standards must be raised." Yonhapnews. May 26, 2023.

From 2016 to 2022, the number of cases of overseas leakage of industrial technologies such as semiconductors, electronics, shipbuilding and displays reached a total of 142 cases. Among 143 cases, 47 cases of overseas leakage of 'national core technologies' designated in Article 2 of the Industrial Technology Protection Act, such as 30-nano DRAM, 30-nano NAN, and 30-nano foundry, were detected from 2016 to 2023, as presented in Table 1. According to the South Korean Ministry of Trade, Industry, and Energy report, a total of 96 cases of overseas industrial technology leakage were detected from 2019 to 2023. Semiconductors have been most victimized in technology leaks, having 38 cases total (39.6%), followed by 16 cases of displays (16.7%) and 9 cases of automobiles (9.4%). It should be noted that among the leaked technologies in recent years, 33 cases (34%) were related to 'national core technologies" designated in Article 2 of the Industrial Technology Protection Act.[101]

Notably, those national core technologies have been major targets of Chinese espionage. Since China launched its "Made in China 2023" program in 2015, it has strategically recruited South Korean technology experts from South Korean firms in critical sectors like semiconductor and

[101] Eung-Hyeong Cho, "Over the past 5 years, 96 cases of industrial technology have been leaked overseas, with 38 cases of semiconductors being the most." *Donga Ilbo* (Seoul). February 7, 2024. https://www.donga.com/news/Economy/article/all/20240207/123421696/1.

batteries by providing incomparably high salaries.[102] According to South Korea's National Intelligence Service (NIS), more than 60% of the leaked industrial technology overseas from 2017 to 2022 was destined for China.[103] South Korea's National Police Agency data confirmed 78 cases of industrial technology leakage crimes detected by the police over the five years and six months from 2018 to June of 2023 and 225 cases of arrest; by country of leakage, according to the National Police Agency, China took the most with 51 cases, which accounted for 65.5%.[104]

One of the most shocking and alerting cases of Chinese espionage targeting South Korean tech industry and national core technologies was that of a former Samsung Electronics executive, surnamed Choi, who was charged with illicitly acquiring basic engineering data and the plant layout used in Samsung's chip factory. Such information was classified as national core technology under South Korean law. He allegedly leaked the information, which cost at least ₩300 billion ($232.7 million) in trade secrets, to build a copycat chip factory in China.[105] According to a news source, Choi, who headed a chip company called CHJS, was "funded by the Chengdu city government, [and] attempted to build a chip factory in China just 1.5 kilometers (0.9 miles) from Samsung Electronics' manufacturing plant in Xi'an. Choi had hired 200 engineers at the Chengdu-based company, mainly from Samsung and SK Hynix."[106] Fortunately, the project fell through due to the company's failure to secure promised funding from a Taiwanese chipmaker.

China's targeted IP theft cases are more notable and graver for South Korea's industrial sectors. In 2023, South Korea's Suwon District Prosecutor's Office accused five suspects of sending confidential information related to semiconductor cleaning equipment to China.[107] The Korean Intellectual Property Office and Deajon District Prosecutor's Office also caught six people from three South Korean companies for allegedly leaking core chip manufacturing technology to China.[108] Son Seung-woo, President of the Korea Institute of Intellectual Property, noted that, "China is working on advancing its industries, and is attempting to acquire technologies from other countries with more advanced levels, … Washington's chip control measures on China caused a shortage of [advanced] semiconductors, which pushed Beijing to seek South Korean chip technology."[109]

---

[102] William C. Hannas and Didi Kirsten Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage*, (Oxford: Routledge, 2020).
[103] Heekwon Lee, "They Kicked Out Koreans Without Severance Pay … China is Now OLED Talent Hunting," *The JoongAng* (Seoul), July 13, 2023, https://www.joongang.co.kr/article/25177289.
[104] Seung-Hyun Gye, "65% of industrial technology leaked overseas to China… 225 people arrested over 5 years." *Yonhap News* (Seoul). October 9, 2023. https://www.yna.co.kr/view/AKR20231008038100004.
[105] Eun-Jee Park, "Korea to Get Tough on Industrial Espionage from China," *Korea Joongang Daily* (Seoul), June 16, 2023. https://koreajoongangdaily.joins.com/2023/06/16/business/tech/Korea-China-technology-theft/20230616182016080.html.
[106] Ibid.
[107] Seong Hyeon Choi, "Tech War: South Korea on Alert for Technology Leaks to China as US Restrictions Intensify," *South China Morning Post* (Hong Kong) February 12, 2023, https://www.scmp.com/tech/tech-war/article/3209635/tech-war-south-korea-alert-technology-leaks-china-us-restrictions-intensify.
[108] Ibid.
[109] Ibid.

The economic losses from economic espionage in South Korea from foreign countries (not only China), in the period from 2018 to 2023 is estimated at about ₩25 trillion, or about $1.8 billion, according to the National Intelligence Service (NIS) of South Korea.[110] South Korea's competitiveness and reputation as a top producer of advanced technology is directly challenged by China's acquisition efforts. For example, a Korean researcher was indicted in 2024 for sharing materials with China for advanced display automation technology, one of South Korea's national core technologies, shortening China's ability to produce such materials by a decade.[111] On a broader level, the national security implications are even harder to measure, but nevertheless a critical issue of concern for the South Korean government.

South Korean Academia Impacts

China has been actively 'taking away' talented scholars and experts from South Korea. Its Thousand Talents Plan works not only in the US, but also in South Korea, where at least 13 Korean experts have been confirmed as Chinese recruits. All were very talented and key experts in their research areas, especially related to national strategic technologies such as biotechnology, artificial intelligence, and new materials.[112] China has spared no effort in approaching South Korean scholars and experts considered to have skills and expertise that are potentially useful and necessary for China. China has recruited South Korean experts and scholars either through Chinese professors with whom they had connected via research projects, or through Chinese students whom they taught in South Korea. Most alarmingly, those recruited to China were not motivated or moved by monetary benefits, but by a more 'supportive research environment,' being promised that they would be able to conduct research without funding concerns.[113] A case that alerted South Korea to the dangers of the Thousand Talents Plan in South Korean universities involved a professor at the Korea Advanced Institute of Science and Technology (KAIST), one of the top universities in South Korea, hosting a number of scholars and experts in national core technology and science. Despite holding such a prominent position in a prestigious South Korean university, this KAIST professor was recruited to the Thousand Talents Plan in 2017 and was accused of leaking 72 files to Chinese professors from 2017 to 2020, including research data on light detection and ranging (LIDAR) technologies, in exchange for ₩3.3 billion ($2.4 million) for research projects and other expenses.[114]

In 2004, South Korea had the world's first Chinese Confucius Institute, which was nationally sponsored and governed by the Chinese government, and since then, China has established government-funded Confucius Institutes in 23 South Korean universities. Confucius Institutes

[110] Ben Forney, " Changing South Korea's Espionage Law is Good for Business," Korea Economic Institute, September 24, 2024. https://keia.org/the-peninsula/changing-south-koreas-espionage-law-is-good-for-business/.
[111] "Espionage Threats Continue to Undermine South Korea's Edge in Hi-Tech Sectors," KOREAPRO, November 22, 2024, https://koreapro.org/2024/11/espionage-threats-continue-to-undermine-south-koreas-edge-in-hi-tech-sectors/.
[112] "China Takes Away Key Talent from Korea," *Dong-A Ilbo* (Seoul), September 30, 2024, https://www.donga.com/en/article/all/20240930/5198560/1.
[113] Ibid.
[114] Jung Min-ho, "Two-Year Prison Term Upheld for KAIST Professor who Leaked Autonomous Tech to China," *Korea Times* (Seoul), May 30, 2024, https://www.koreatimes.co.kr/southkorea/law-crime/20240530/two-year-prison-term-upheld-for-kaist-professor-who-leaked-autonomous-tech-to-china.

are also operating in four high schools and one private academy in South Korea. In all, South Korea is home to the largest number of Chinese Confucius Institutes in any Asian country.[115] The Confucius Institute is run by the State Hanban, a branch of the Central United Front Work Department of the Chinese Communist Party. China asserts that the Confucius Institute is "an institution established for the purpose of teaching Chinese and disseminating traditional Chinese culture," but in reality, the Confucius Institutes serve as a "propaganda agency of the Chinese Communist Party."[116] Because of the Confucius Institute's cunning approach to provide information favorable to China to students and scholars, many have warned about its danger. People's Strength Rep. Jeong Kyung-hee has warned that "because of the name of Confucius, Confucius Institutes are positively accepted in Korea, where Confucianism is strong, and there is no objection. They are brainwashing students, but they are not aware of the dangers. We need to find a path to legal expulsion, not just a civic movement."[117]

The negative impacts and consequences of Chinese S&T acquisition in South Korean education and research areas have been significant. It is noted that "with the Chinese focused on R&D and talent acquisition at the national level, Korea's technological competitiveness in eleven key national science and technology areas has been overtaken by China for the first time in 2022. Talent that should be brought into science and engineering [of South Korea] are being taken away by medical schools, with developed talent leaving the country. Universities are finding it difficult to acquire proper research equipment and recruit professors to teach students."[118]

Conclusion

China's extra-legal and illegal acquisition of science and technology from foreign countries has increased significantly as the balance of power has shifted between the US and China. In recent years, it has become clear that the US no longer maintains its position as sole international superpower and top technology powerhouse. China has become the second largest economy in the world and is considered to be, and behaves as, a near-peer competitor entering a meaningful power competition with the US.[119]

Given the continually increasing tensions and the intensifying technological competition between the US and China, both the US and South Korea should invest more effort to properly address Chinese acquisition of S&T research in their two countries. To avoid losing its significant upper hand in technological competitions, the US should continue its strong measures and approach to evaluate and counter Chinese S&T acquisition from the government, academia,

[115] Bruce Klingner, *South Korea Must Counter Chinese Influence Operation – and the US Should Provide Support*, No. 3815 (Washington, DC: Heritage Foundation, 2024).
[116] Yoon-Jeong Lee, ""In the Name of Confucius" - Korea Premiere revealing the reality of the Confucius Institute," *The Epoch Times* (South Korea). May 22, 2021. https://inthenameofconfuciusmovie.com/in-the-name-of-confucius-korea-premiere-revealing-the-reality-of-the-confucius-institute-the-epoch-times-south-korea/.
[117] Ibid.
[118] "China Takes Away Key Talent from Korea," *Dong-A Ilbo* (Seoul), September 30, 2024, https://www.donga.com/en/article/all/20240930/5198560/1.
[119] Wooseon Choi, "New Horizons in Korea-US-Japan Trilateral Cooperation," *CSIS* (Washington, DC), June 27, 2024, https://www.csis.org/analysis/new-horizons-korea-us-japan-trilateral-cooperation.

and private industry sectors. Compared to the US, South Korea has been relatively less assertive in addressing China's IP theft and espionage due in part to concern about potential Chinese retaliation as it experienced during the THAAD crisis in 2016 when the US placed THAAD missiles in South Korea and China retaliated with sanctions on South Korea. However, as various South Korean national agencies have noted, there are increasing numbers of incidences where China's S&T acquisition infiltrates South Korea's government agencies, universities and private industry, all of which pose grave dangers to South Korea's national security and national economy. As the first step to properly counter China's S&T acquisition from South Korea, it is crucial for South Korea to accurately assess and evaluate to what extent China's espionage, theft, and other extra-legal and illegal tactics have affected South Korea, in which areas, and what policy actions should be adopted and implemented to properly address the impacts, severity, and consequences.

Technological security is one of the main areas on which the US and South Korea have recently focused regarding their strategic cooperation. Along with like-minded countries, South Korea and the US have been closely working together via the Chip 4 agreement with Japan and Taiwan to minimize China's influence over industries that are critical to economic and technological security, like the semiconductor supply chain. The Spirit of Camp David Joint Statement of the Republic of Korea, the United States, and Japan also underlines the importance of technological security, in which the three countries will "enhance cooperation on technology protection measures to prevent the cutting-edge technologies we develop from being illegally exported or stolen abroad" and "strengthen trilateral cooperation on export controls to prevent our technologies from being diverted from military or dual-use capabilities that could potentially threaten international peace and security."[120] The Camp David joint statement did not directly accuse China, but it is logical to assume that one of the major concerns regarding technological security is China and its hostile exploitation of open scientific and technological research. In other words, it is critical for South Korea not only to accurately assess how risky China's technological exploitation is for its own economy and national security, but also to come up with effective measures to collaborate with the US and other democracies in securing S&T research from Chinese acquisition.

[120] "The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States," (joint statement, Camp David, MD: Ministry of Foreign Affairs of Japan, 2023), https://www.mofa.go.jp/files/100541826.pdf.