
THE UNIVERSITY OF TENNESSEE KNOXVILLE

CENTER FOR NATIONAL SECURITY & FOREIGN AFFAIRS

# Policy Efforts and Recommendations to Counter Chinese Scientific and Technology Acquisition from the United States and South Korea

**Krista E. Wiegand**

**Jackson Craig Scott**

**Sojeong Lee**

July 2025

# Policy Efforts and Recommendations to Counter 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

Krista E. Wiegand
Jackson Craig Scott
Sojeong Lee

*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:*

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.

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.

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.

# Table of Contents

## Executive Summary

This policy report examines current efforts by the United States and South Korea to counter Chinese scientific and technological acquisition through illegal and extralegal means, particularly intellectual property (IP) theft and espionage. China uses cutting-edge technology from both countries to undercut US and Korean industry and enhance its own military capabilities – thus endangering both countries' economic interests and national security. The open nature of science and technology (S&T) research and development in both the US and South Korea has sparked major innovations in both countries. However, this openness also presents a unique challenge in developing policies that combat China's illegal and extralegal activities without sacrificing the transparency of US and South Korean research and development. Key policies recommended in this report include:

- **Provide research security standards for private industry companies.** Private industry needs to prioritize countering multiple forms of IP theft and espionage, not just cybersecurity. Government defense contractors must meet the highest standard of securing research and development. The governments of South Korea and the U.S. should develop high standards for security in research and development for other S&T companies working in high-value sectors as well.

- **Strengthen the research security efforts of US and South Korean universities** by establishing government-supported, coordinated efforts to raise scholars' awareness of the impacts of Chinese S&T acquisition, how it threatens national security, and how to deter these threats.
    - **Protect and strengthen funding for US initiatives** such as the National Science Foundation's SECURE program. The US intelligence community and academia should also restore a forum for discussions about potential concerns such as profiling or academic freedom.
    - **Create a South Korean version** of the NSF SECURE initiative through the National Research Council of Science and Technology (NST).

- **Pursue proposed reforms to South Korean law** so the Korean government can more effectively prosecute theft and espionage conducted on behalf of China. Progress has been made with recent amendments to address S&T companies' concerns, but limitations prevent effective progress.

- **Pursue bilateral efforts** such as US-South Korean exchange programs for counterespionage investigators, and degree programs to develop a skilled workforce of security professionals.

- **Respond to China's whole-of-society strategy with a similar approach,** creating a US-South Korean IP Theft and Espionage Commission to include both countries' high-tech industries, research universities and national laboratories, and federal and national governments.

## Introduction

As the great power competition between the United States (US) and the People's Republic of China (China)[1] continues to intensify, multiple venues for conflict have developed. From trade wars to threats about banning TikTok, strategic competition has seeped into multiple parts of society beyond the traditional security realms. One area which China has used to gain advantages is in the science and technology (S&T) sectors. Technological advantage is an important aspect of military hegemony.[2] In October 2022, former Secretary of State Anthony Blinken noted about this competition: "We are at an inflection point. The post-Cold War world has come to an end, and there is intense competition underway to shape what comes next. And at the heart of that competition is technology."[3]

The Chinese Communist Party (henceforth China) is prioritizing China's increased S&T capabilities to challenge the US on the world stage. One strategy that China has used to achieve a competitive advantage is through legal, extralegal, and illegal acquisition of S&T research, around the world, particularly from liberal democracies that tend to maintain openness of government and academic research in S&T fields. For several years, China has conducted many different strategies of technology transfer from the US and South Korea to China, the most blatant being intellectual property (IP) theft and espionage. In a 2019 Senate hearing, Bonnie S. Glaser noted that, "China was involved in 90 percent of all economic espionage cases the Department [of Justice] handled from 2011 to 2018."[4] In 2020, FBI Director Christopher Wray stated, "We've now reached the point where the FBI is opening a new China-related counterintelligence case about every 10 hours."[5] Despite efforts to address these threats in the US, Chinese acquisition efforts continue. This is taking place across the US, as well as in South Korean societies within private industry, government, and universities. This tactic by China is what scholars place in the "gray zone" category of warfare, or deliberate malign actions that are below the threshold of kinetic conflict.[6]

The primary purpose of this report is to discuss current policy efforts in the US and South Korea to mitigate threats by China to open scientific and technological research. A companion report that we wrote offers an in-depth review of the threats faced by the US and South Korea due to

[1] 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.
[2] Robert L. Paarlberg, "Knowledge as Power: Science, Military Dominance, and US Security," *International Security* 29, no. 1 (2004): 122-151. https://www.jstor.org/stable/4137549.
[3] Anthony J. Blinken, "Remarks to the Press," Speech at Stanford University Encina Hall Steps, Stanford, CA, October 17, 2022. https://2021-2025.state.gov/secretary-antony-blinken-remarks-to-the-press-3/.
[4] *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).
[5] Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Speech at the Hudson Institute, Washington, DC, July 7, 2020.
[6] 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, 47.

Chinese acquisition of S&T research in private industry and academia.[7] The distinct actors and approaches of Chinese acquisition of S&T research in South Korea and the US has necessitated somewhat different approaches to countering such threats since the US is primarily investigating Chinese and Chinese-American individuals, and South Korea is primarily investigating South Korean individuals. Thus, the US government's challenge is viewed from a perspective of targeting foreigners or immigrants, while the South Korean government's challenge is viewed from a perspective of targeting its own citizens who have sold out to China. A report outlining the challenges discussed by US and South Korean experts at a November 2024 conference held at the Baker School provides further insight about the problem, as well as a discussion of current approaches to address the problem and policy recommendations.[8]

In this report, we review and provide assessment of current approaches to the efforts by the governments and academia in the US and South Korea to address threats to the private sector and universities in those countries. The report offers policy recommendations to further defend against S&T acquisition from China, as well as recommendations for bilateral coordination and multilateral efforts among like-minded countries. We conclude with a proposal for a whole-of-society approach in both the US and South Korea, as well as a bilateral commission to address the root of the problem: Chinese efforts to take advantage of open S&T sectors in the US and South Korea.

## US Efforts to Address Threats to the Government and Private Industry

The US government has multiple avenues to defend against China's IP theft and economic espionage targeted at technologies owned by the US military and government, as well as private industry.[9] Most efforts have been through export controls, cybersecurity efforts, banning technology transfers, and listing entities affiliated with the Chinese military. The Department of Defense (DOD), Department of State (DOS), Department of Justice (DOJ), Department of Homeland Security (DHS), Department of Commerce (DOC), as well as US Trade Representative, International Trade Commission, US Customs and Border Protection, US Patent & Trademark Office are all involved in different parts of enforcing efforts to counter S&T acquisition by China. The US is also a party to the UN's World IP Organization and World Trade Organization's Trade-Related Aspects of IP Rights (TRIPS) Agreement. There are many moving pieces and multiple jurisdictions involved in US policy responses to Chinese acquisition of S&T research and development in government and private industry.

Beginning with the administration of President Barack Obama and subsequent Congress in 2013, the US government made some changes to protect the US from IP theft in the *IP*

[7] Sojeong Lee, Jackson Craig Scott, and Krista E. Wiegand, *The Impact and Consequences of Chinese Science and Technology Acquisition on 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).
[8] 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).
[9] Some efforts to defend against espionage threats existed before the current competition with China, such as the Economic Espionage Act, FARA, the Trade Act of 1974 and the Committee on Foreign Investment in the United States.

*Commission Report*, but the changes were not applied evenly. Importantly, the changes impacted Section 1637 of the 2015 National Defense Authorization Act (NDAA), which gave responsibility to the executive branch to analyze cyberespionage and allows the executive branch to sanction foreign entities. However, there is no evidence the Obama administration utilized these policy changes to stop IP theft. In 2016, President Obama signed the Defend Trade Secrets Act and created the Cybersecurity National Action Plan,[10] followed by a 2017 update of the *IP Commission Report*, with details about progress on policy recommendations.

In 2018, the administration of President Donald Trump enacted the Export Control Reform Act, establishing the Export Administration Regulations, which replaced the Export Administration Act of 1979. Throughout 2018, the White House continually released information shedding light on China's economic aggressions and IP theft.[11] In the same year, President Trump signed into law the Cybersecurity and Infrastructure Security Agency under DHS. Its purpose was to work "with partners at every level to identify and manage risk to the cyber and physical infrastructure that Americans rely on every hour of every day,"[12] which included IP theft and economic espionage.[13] Additionally, President Trump created the DHS Cybersecurity and Infrastructure Security Agency, which has published strategies for private industry to adopt to mitigate insider threats.[14]

Efforts by the US Congress have focused heavily on linking defense authorizations to DOD efforts to keep track of Chinese Military Companies (CMCs). Section 1286 of the 2019 NDAA requires DOD to create an initiative to work with academic institutions that work on defense research.[15] Section 1260H of the 2021 NDAA requires the DOD to publish a list of designated CMCs, which are seen as threats to US national security. However, enforcement of these rules has been challenging. Section 1260H and Section 1286 include a list of Chinese entities and call for additional research security if a research project involves one of the entities. However, the policy must be carried out by research institutions, not the government. As noted by one analyst, "This has led to inconsistent application, delayed interventions, and continued access by adversarial entities."[16]

The US Congress has also addressed concerns about Chinese threats to S&T research by focusing on export controls. The House Foreign Affairs Committee recommended a number of

[10] *The Theft of American IP: Reassessments of the Challenge and United States Policy*, Update to the IP Commission Report (Seattle, Washington: National Bureau of Asian Research, 2017), 3.
[11] White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and IP of the United States and the World*, (Washington, DC: White House, 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.
[12] Cybersecurity and Infrastructure Security Agency, "About CISA," Cybersecurity and Infrastructure Security Agency, accessed April 7, 2025, https://www.cisa.gov/about.
[13] Cybersecurity and Infrastructure Security Agency, *Insider Threat Mitigation Guide*, (Washington, DC: Cybersecurity and Infrastructure Security Agency, 2020), https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide.
[14] Cybersecurity and Infrastructure Security Agency, *Insider Threat Mitigation Guide*, (Washington, DC: Department of Homeland Security, 2020).
[15] Ibid, 314-315.
[16] LJ Eads, *Undermining Deterrence: The Case for a Total Ban of DoD Research Involving Chinese Military Companies*, (Beavercreek, OH: Parallax Advanced Research, 2025), 2.

strategies including investing in innovation, denying and delaying access to critical technologies from China, and utilizing export controls.[17] The Committee report highlighted technological weaknesses China has in this sector and noted that the US and a few of its treaty allies should take advantage of these gaps.[18] The Committee report also recommended a myriad of measures to be taken by the DOC. For example, it states that the Department's Bureau of Industry and Security needs organizational structure reform and that the export control regime should be updated to stop the leaking of US technology to China.[19]

In 2022, the Biden administration indirectly addressed threats to US S&T companies by instituting several export controls targeting China's artificial intelligence and semiconductor industries. These export controls restricted certain products sold to China as a whole, instead of placing restrictions on exports of advanced semiconductor products to China based on military use. This aspect of the controls changed 25 years of US export policy.[20] The policy changed from trying to slow down an adversary's technological advancement to purposefully trying to degrade it. Additionally, these export controls were geographic in nature and unilateral, which was a new strategy for US industrial policy.[21] Also in 2022, President Biden signed into law the Protecting American IP Act of 2022. This law imposes sanctions on "certain foreign individuals and entities involved in the theft of trade secrets belonging to a US individual or entity." The US president must periodically submit a list of foreign individuals engaged in economic espionage along with the CEOs or board members of any foreign institutions engaged in the same. Then, the president "shall impose property- and visa-blocking sanctions on individuals named in the report; and property- or export-blocking sanctions, including denial of certain financial assistance, on entities named in the report."[22] President Biden also signed into law the CHIPS and Science Act of 2022, which states, "[The Department of Energy] shall develop and maintain tools and processes to manage and mitigate research security risks…to facilitate determinations of the risk of loss of US IP or threat to the national security of the United States..."[23]

Other efforts to counter threats to S&T research for use by the US military and government, as well as private industry include the executive order by President Biden to stop the transfer of national security technologies and products to untrustworthy countries. It requires "United States persons to provide notification of information relative to certain transactions involving covered foreign persons (notifiable transactions) and that prohibit United States persons from engaging in certain other transactions involving covered foreign persons (prohibited transactions).[24] In the same year, the Department of Justice created a Disruptive Technology Strike Force in an attempt "to target illicit actors, strengthen supply chains and protect critical

[17] Ibid, 4.
[18] Ibid.
[19] Ibid, 13.
[20] Gregory C. Allen, *China's New Strategy for Waging the Microchip Tech War*, (Washington, DC: CSIS, 2023), 1.
[21] Gregory C. Allen, Emily Benson, and William Alan Reinsch, *Improved Export Controls Enforcement Technology Needed for US National Security*, (Washington, DC: CSIS, 2022), 2.
[22] Protecting American IP Act of 2022, Pub. L. No. 117-336 (01/05/2023). https://www.congress.gov/bill/117th-congress/senate-bill/1294.
[23] Ibid, § 10114.
[24] Exec. Order No. 14105, 88 FR 54867 (2023), https://www.federalregister.gov/documents/2023/08/11/2023-17449/addressing-united-states-investments-in-certain-national-security-technologies-and-products-in.

technological assets from being acquired or used by nation-state adversaries." It is led by the Department of Justice's National Security Division and Department of Commerce's BIS, and brings together exports from varying parts of the government including the FBI, Homeland Security Investigations, and 14 US Attorney's Offices in 12 metropolitan regions around the US.[25]

At the start of Trump's second administration, the government quickly moved to prioritize responding to the Chinese threat to S&T research and development by the US military, government, and private industry. In March of 2025, the Commerce Department's Bureau of Industry and Security added 80 companies to the Entity List from China, South Africa, Iran, and Taiwan.[26] Secretary of State Marco Rubio also exempted "all efforts, conducted by any agency of the federal government, to control the status, entry, and exit of people, and the transfer of goods, services, data, technology, and other items across the borders of the United States, [which] constitute a foreign affairs function of the United States under the Administrative Procedure Act."[27] This broad public notice means that agencies dealing with the aforementioned topics are exempt from the notice-and-comment process of administrative rulemaking. Most recently, in June 2025, the House Select Committee on the Chinese Communist Party sent a letter to Secretary of Defense Pete Hegseth urging stronger vetting of defense contractors, as pursuant to the Defense Federal Acquisition Regulation Supplement (DFARS) rule mandated by Section 847 of the 2020 NDAA passed by Congress.[28] As noted in the letter, the DFARS rule has not been implemented as effectively as it should have been, allowing for Chinese acquisition from defense contractors working with Chinese entities.

An ongoing problem for US government policy responses to counter Chinese threats to US S&T research is that since technology transfers can take many forms, there are overlapping and confusing aspects to enforcement, such as jurisdiction. For example, IP theft can include trademark infringement, copyright piracy, counterfeiting, trade secret theft, patent infringement and cybertheft. Each of these issues requires different approaches from different agencies.[29] As with other federal government efforts to address a major threat, the lack of coordination among agencies, the different ideological perspectives of presidential administrations, and limited government funding all serve to hinder effectively countering China's acquisition of S&T research in the US.

---

[25] Office of Public Affairs, "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force," *US Department of Justice* (Washington, DC), February 16, 2023. https://www.justice.gov/archives/opa/pr/justice-and-commerce-departments-announce-creation-disruptive-technology-strike-force.

[26] Bureau of Industry and Security, "Commerce Further Restricts China's Artificial Intelligence and Advanced Computing Capabilities," (Washington, DC: US Department of Commerce, 2025), https://www.bis.gov/press-release/commerce-further-restricts-chinas-artificial-intelligence-advanced-computing-capabilities?utm.

[27] N.A., "Rubio Issues Broad Declaration on Foreign Affairs Exception of the Administrative Procedure Act," *Economic Policy Institute* (Washington, DC), March 19, 2025, https://www.epi.org/policywatch/rubio-issues-broad-declaration-on-foreign-affairs-exception-of-the-administrative-procedure-act/.

[28] House Select Committee on the Chinese Communist Party sent a letter to Secretary of Defense Pete Hegseth, June 16, 2025, https://cdn01.dailycaller.com/wp-content/uploads/2025/06/Letter-to-DoD_DFARS-Sec-847.pdf.

[29] Alec Goodrich, "International IP Theft: Background Framework for Private Enforcement," *International Law and Policy Brief* (2022), https://studentbriefs.law.gwu.edu/ilpb/2022/11/11/international-intellectual-property-theft-background-framework-for-private-enforcement/.

### *Policy Recommendations*

While the US government has pursued mitigation attempts at preventing and countering China's acquisition of S&T research, these efforts remain ineffective in preventing the transfer of US S&T research to CMCs in China. One way to make these efforts more effective would be to enforce a "categorical ban" on DOD funding projects involving CMCs.[30] Other efforts the DOD could pursue would be to create an Office for Research Security Enforcement and to screen "covered individuals and institutions against the 1260H and 1286 lists, as well as the BIS Entity List and EO 14032" before grants are awarded.[31] Additionally, the US government could expand designations and sanctions for entities involved in research exploitation. The Departments of Commerce and Treasury could expand the BIS Entity List, the Specially Designated Nationals list, and EO 14032 Annex. The expansion could "include academic research programs, labs, and People's Liberation Army-affiliated think tanks to co-publish or co-develop dual-use technologies with [US] institutions."[32]

Another policy area that could be tightened relates to the US government's research security standards for its private industry contractors, which are currently focused primarily on cybersecurity, data breaches, and software supply chain integrity. For example, in October 2024, DOD clarified the requirements for defense contractors to ensure that their computer networks and cybersecurity practices are secure enough to defend against threats from adversaries.[33] The focus on cybersecurity for defense and other contractors is critical, but Federal Acquisition Regulations should be broadened and specified to cover other areas of security for research and development, background investigations for personnel working in these companies, and a business culture of mutual concern about IP theft and espionage from China. Further government support should also be provided to US companies working in science and technology to deter and respond to Chinese acquisition of research and development. For example, a proposed bill by then Senator Kamala Harris (D-CA), Deterring Espionage by Foreign Entities through National Defense Act of 2018, would have allowed the government to help American companies respond to Chinese espionage through civil action "for the misappropriation of a trade secret," but this bill was ultimately only referred to committee and was not passed. The recent urging by the House Select Committee on the CCP to vet defense contractors more effectively is another important step in mitigation efforts.

## US Efforts to Address Threats to Academia

The US university system is built upon openness and intellectual endeavors, and China has exploited this open system through extralegal transfers of knowledge, recruitment of scholars to share data, and IP theft in science and technology research areas. Efforts to address S&T

[30] LJ Eads, *Undermining Deterrence: The Case for a Total Ban of DoD Research Involving Chinese Military Companies*, (Beavercreek, OH: Parallax Advanced Research, 2025), 9-10.
[31] Ibid, 9.
[32] Ibid, 10.
[33] C. Todd Lopez, "DOD Simplifies Process for Defense Contractors to Comply With Cybersecurity Rules," U.S. Department of Defense (Washington, DC, October 17, 20204), https://www.defense.gov/News/News-Stories/Article/Article/3938314/dod-simplifies-process-for-defense-contractors-to-comply-with-cybersecurity-rul/.

acquisition in US academia date to the Reagan Administration.[34] Today, Chinese threats to S&T research at universities are substantial. Most security initiatives have come from government mandates for private federal contractors, but there are more recent efforts by the National Science Foundation (NSF) to provide clearer guidelines and requirements for academia.

One of the last policies of the first Trump administration was presidential memorandum NSPM-33, which sought to "strengthen protections of United States Government-supported Research and Development (R&D) against foreign government interference and exploitation."[35] As a main government agency that funds science and technology in the US, NSF has similarly adopted initiatives to assist with research security issues. The agency has pursued countering and deterring research security in several ways. Addressing the problem directly, as of February 2023, NSF had suspended 50 awards, terminated 20 awards, cancelled a final payment to one organization on one award, issued government-wide suspensions for nine researchers and four entities, debarred five researchers and two entities, had five researchers and one entity agree to voluntary exclusions due to NSF proposals, and barred 17 researchers from serving as reviewers for proposals. With the help of its Office of Inspector General, NSF has recovered $15 million in grant funds.[36]

The 2018 China Initiative is perhaps the best-known effort to address Chinese threats to research in academia. Created to reflect "the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy," the initiative was led by the DOJ's National Security Division, which is responsible for countering foreign country threats to the US.[37] The China Initiative was very effective in raising awareness of the problem in the US and highlighting how China's acquisition of S&T research affects U.S. national security. Under this initiative, the DOJ indicted or prosecuted several dozen individuals who had been sharing sensitive information with the Chinese government or Chinese universities closely affiliated with the Chinese government. While effective, the China Initiative was criticized for what was considered to be profiling of Chinese and Chinese-Americans, creating an atmosphere of fear among Asian researchers at US universities working in S&T fields, regardless of whether they were Chinese, Chinese-American, or even working on research that might be deemed high priority for the Chinese government. The initiative was officially shut down by President Joe Biden's administration but continued in other forms and strategies that were recalibrated to

[34] White House, *National Policy on the Transfer of Scientific, Technical and Engineering Information* NSDD-189 (Washington, DC: White House, [1985,] [2001,] 2010), https://irp.fas.org/offdocs/nsdd/nsdd-189.htm.
[35] White House, *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy* NSPM-33 (Washington, DC: White House, 2021), https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.
[36] National Science Foundation, "Research Security at the National Science Foundation," *National Science Foundation* (Washington, DC), February 2023, https://www.nsf.gov/research-security#mftrp.
[37] "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," Department of Justice (Washington, DC), November 19, 2021, https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related. See James Mulvenon, Didi Kirsten Tatlow, and Alex Joske, "Mitigation Efforts to Date," in *China's Quest for Foreign Technology: Beyond Espionage*, eds. William C. Hannas and Didi Kirsten Tatlow (Milton Park, Abingdon, Oxon: Routledge, 2021) for further discussion.

continue investigating potential sources of China's acquisition of S&T research.[38] There are calls for the second Trump administration to revise several aspects of the China Initiative, mainly from Congress.

The CHIPS and Science Act of 2022 includes multiple policies and strategies to mitigate IP theft and increase research security for academia. For example, it established the NSF SECURE Center, which is led by the University of Washington, supported by nine other universities. NSF SECURE serves as a clearinghouse for information to "empower the research community to identify and mitigate foreign interference that poses risks to the US research enterprise."[39] The CHIPS and Science Act also requires NSF to maintain a Research Security and Policy office that is mandated to "coordinate all research security policy issues across the NSF."[40] Further, the FBI is engaged in the College and University Security Effort (CAUSE) which is an effort to form relations with institutions of higher education to "protect research, products, and personnel from foreign intelligence threats."[41]

The National Counterintelligence and Security Center has published multiple resources and strategies for research security on its website.[42] In March 2024, NSF released the latest report, *Safeguarding the Research Enterprise*, produced by the independent science advisory group, JASON, as required by the CHIPS and Science Act. In the report, the advisory group emphasized that recipients of federal funding must be responsible in engaging in and protecting US interests. This is a more proactive stance than the original 2019 report, which highlighted the need for academia and the US government to have a common understanding of the best means of protecting US interests. The 2024 report recommended "highlighting the importance of fostering a culture of research security awareness within the scientific community by providing substantive information to researchers about real risks, making resources available and encouraging continuous engagement with researchers and their institutions about the efficacy of research risk mitigation and control efforts."[43] In US universities, there seems to be more awareness of US national security interests and the importance of research security measures in the past few years since the CHIPS and Science Act was passed. This increased awareness is likely due to combined efforts by NSF, universities, the China Initiative, and the CHIPS and Science Act.

[38] Josh Gerstein, "DOJ Shuts Down China-focused Anti-Espionage Program," *Politico* (Virginia), February 23, 2022, https://www.politico.com/news/2022/02/23/doj-shuts-down-china-focused-anti-espionage-program-00011065.
[39] National Science Foundation, "NSF-backed SECURE Center Will Support Research Security, International Collaboration," *National Science Foundation* (Washington, DC), July 24, 2024, https://www.nsf.gov/news/nsf-backed-secure-center-will-support-research.
[40] CHIPS and Science Act of 2022, Pub. L. No. 117-167 § 10331, (2022). https://www.congress.gov/bill/117th-congress/house-bill/4346.
[41] FBI, *The FBI's College and University Security Effort*, (Washington, DC: FBI, n.d.), https://ucr.fbi.gov/investigate/counterintelligence/us-academia.
[42] National Counterintelligence and Security Center, "Research Security," National Counterintelligence and Security Center, accessed April 16, 2025, https://www.dni.gov/index.php/safeguarding-science/research-security.
[43] "NSF announcement on JASON report: Safeguarding the Research Enterprise," *U.S. National Science Foundation* (Washington, DC), March 21, 2024, https://www.nsf.gov/news/nsf-announcement-jason-report-safeguarding. An initial report produced by JASON was published in 2019.

Another proactive move taken by US universities is closure of Confucius Institutes – Chinese government funded language and culture institutes – located on their campuses. While there were 100 Confucius Institutes at US universities in 2019, today there are only five remaining institutes.[44] While some universities acted on their own initiative, most universities closed the institutes due to threats to federal funding, based on a 2018 Congressional act. Other factors included government pressure, concern for reputation, and concerns for Chinese government policies.[45] The closure of the Confucius Institutes at universities across the US indicates a proactive effort by universities, mainly responding to US government pressure and threats of funding, to prevent an easy means of Chinese government influence on US academia.

Some universities have led initiatives to create research security strategies, including some focused particularly on working with Chinese universities. MIT has established multiple strategies to balance obtaining Chinese talent while protecting research from IP theft. [46] There are now guiding principles that MIT scholars adhere to related to not hosting researchers and visiting students that are employed by the Chinese military and security institutions or who have graduated from China's civilian national defense universities; not joining research collaborations with China's military oriented institutions; not collaborating with Chinese business entities that assist the Chinese military or assist the Chinese government in suppressing human rights in China; and not participating in Chinese talent recruitment programs that are created to obtain US technology and transfer it to China.[47] The guidelines also advise scholars about technology licensing, data protection, and travel to China.[48] MIT also proposed strategies to protect IP without eroding open scientific research.[49]

Another example of effective policies to prevent Chinese acquisition of S&T research is the Texas A&M Research and Innovation Security and Competitiveness (RISC) Institute. The RISC Institute leads in securing research efforts within academia and industry.[50] It also spearheads the Academic Security & Exploitation Annual Training Seminar. The institute's programs and partners include the Critical & Emerging Technology Protection Program (CETPP), the University Research Security Professional Association (URSPA), the National Science Foundation SECURE – Analytics, and the National Science Foundation SECURE – Southwest.[51]

[44] "China: With Nearly All U.S. Confucius Institutes Closed, Some Schools Sought Alternative Language Support, US Government Accountability Office, October 30, 2023, https://www.gao.gov/products/gao-24-105981.
[45] Ibid.
[46] Richard Lester et. al, "University Engagement with China: An MIT Approach," (Cambridge: Massachusetts Institute of Technology, 2022).
[47] Ibid.
[48] Ibid.
[49] Ibid, 248.
[50] RISC Institute, "Mission," Home, Research and Innovation Security and Competitiveness Institute, accessed April 16, 2025, https://risc.tamus.edu/home/.
[51] RISC Institute, "Current Programs and Partners," Programs and Partners, Research and Innovation Security and Competitiveness Institute, accessed April 16, 2025, https://risc.tamus.edu/.

## *Policy Recommendations*

Experts have suggested several approaches to mitigate threats within US academia. Hannas, Mulvenon, and Puglisi suggest creating a more thorough system to track foreign exchange students because the Student and Exchange Visitor System is inadequate.[52] They also highlight the interesting point that collaboration with China on science and technology is also something that China values. It assists them in creating or strengthening capabilities with which they need help, which the US could leverage.[53] Puglisi emphasizes the need for the US to invest in STEM education and training. This could include university scholarships and stipends, since some university students cannot afford to take lower paying lab or research assistant jobs if they must pay their own way through school.[54] Furthermore, there should be greater cooperation amongst countries like the EU and Japan to foster development of emerging technologies but also create an alternative to stop China's coercive practices.[55] While the recent order to ban Chinese students at U.S. universities is well intended, it is so broad that it impacts students in fields unrelated to sensitive areas of research who could contribute to U.S. academia and the U.S. economy in other ways. A more targeted means of issuing student visas to Chinese students would be advisable. Below we provide a few additional recommendations for addressing threats to S&T research in academia.

First, we recommend continued funding and pursuit of NSPM-33 by the government to continue proactively preventing and pre-empting Chinese threats to US academic S&T research and development. University personnel in academic research offices need to provide efficient and effective research security training for scholars and students. Although individual universities and university systems can provide their own research security training and guidelines, a federally-supported, coordinated effort to enhance research security would provide a more streamlined approach. Currently, only grants funded by Department of Energy (DOE) require research security training for scholars. [56] This should be expanded for all federally funded grants from all agencies. Providing some resources directly to NSF and universities to create further resources and research security training for universities to use would be much more cost effective than other existing responses. It is also a very worthy investment, given the critical role that academic science and technology research plays in strengthening US national security and global competitiveness directly and indirectly. Initiatives such as NSF Secure and other recommended policies to address academic research security threats need to be fully funded and protected from threats of funding cuts, given the national security value.

Second, we recommend that universities require research security training for all scholars in science and technology fields if possible, and certainly for those whose research is federally funded. It must be acknowledged that universities generally are not interested in serving as

[52] William C. Hannas, James C. Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (London: Routledge, 2013), 246-247.
[53] Ibid, 247.
[54] Anna B. Puglisi, "Chinese Students, Scholarship, and US Innovation," in *China's Quest for Foreign Technology: Beyond Espionage*, eds. William C. Hannas and Didi Kirsten Tatlow (Milton Park, Abingdon, Oxon: Routledge, 2021), 284-285.
[55] Ibid, 285.
[56] "Research Security Training Requirement," Office of International Affairs, U.S. Department of Energy, https://www.energy.gov/ia/research-security-training-requirement.

research security police, and the negative response to the Department of Justice's China Initiative intimidated academics. However, scholars can protect their research while still maintaining their academic freedom. Starting May 1, 2025, only researchers receiving federal grant funds from DOE and National Nuclear Security Administration are required to conduct mandatory research security training in order to receive funding for their research projects.[57] Free training is provided by DOE, taking four hours.[58] Universities such as our home institution – University of Tennessee – are enacting a requirement for faculty to complete mandatory research security training if they receive funding from any federal agency, not only DOE. Such training should not be too much of a burden compared to the many other regulations such as Institutional Review Board reviews, grant proposal requirements and reporting guidelines, and similar activities scholars are used to following for their research.

The more that scholars are aware of both US national security interests and research security threats from China, the more proactive they can be in preventing threats to their research in the first place. Even if scholars think their own research is not of high value, there is still a need for greater awareness and coordinated efforts with their universities and federal funding agencies. Another recommendation is a reversal of policy to reestablish the FBI National Security Higher Education Advisory Board, which "served as a forum between the U.S. intelligence community and U.S. academic institutions regarding foreign nations' academic espionage," and was cancelled in 2018.[59] Reviving this board could help ease or forestall cultural clashes when the FBI and Department of Justice engage with academics.

## South Korean Efforts to Address Threats to the Government and Private Industry

South Korea has strengthened its ability to protect technology in private industry since major Supreme Court cases in 2014 and 2015 (*Toshiba v. SK Hynix* and *Nippon Steel v. POSCO*). However, these cases were not against China. South Korea continues to strengthen its IP and economic security apparatus by maintaining a list of key technologies and increasing the maximum punishment for international information leaks about those technologies.[60] South Korea has also created a "National Strategic Technology Nurture Plan" to ensure that important research information is not leaked to researchers and others in non-ally countries. South Korea has also stated it plans to create research guidelines to help researchers.[61]

---

[57] Ibid.

[58] Ibid.

[59] US House Committee on Science, Space, and Technology, "SST Committee Questions FBI's Disbanding of National Security Higher Education Advisory Board," *US House of Representatives* (Washington, DC), April 26, 2018, https://science.house.gov/2018/4/sst-committee-questions-fbi-s-disbanding-national-security-higher-education#:~:text=SST%20Committee%20Questions%20FBI's%20Disbanding%20of%20National%20Security%20Higher%20Education%20Advisory%20Board,-115th%20Congress.

[60] Ibid.

[61] Ministry of Science and Information and Communication Technology, "Korea to Announce National Strategy to Become a Technology Hegemon," *Ministry of Science and ICT* (Seoul), April 16, 2025, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=746&searchOpt

South Korea has enacted multiple policies to defend against Chinese S&T acquisition, particularly in the areas of national core technologies, which are considered those that technologies that would have major adverse impact on the national security of South Korea if they were stolen by a foreign adversary. These efforts to counter Chinese threats to national core technologies, produced by the South Korean government institutions and private industry, are narrower than US efforts, partially due to the different nature of the threat in South Korea. In an effort to combat espionage, in 2020, the South Korean government created new departments to help increase public awareness and educate workers on best practices. In 2023, the government created a database of chip engineers who work for South Korean companies so they can monitor their international travel. The South Korean government has also created investigative institutions, passed laws to increase punishments, and made it easier to report potential violations.[62] Also in 2023, the government established the Korean Industrial Technology Protection Act and Korean-Pan Government Technology Leak Joint Response Team that includes 10 government ministries, intelligence services, and investigative agencies.[63] In June of that year, the government indicted a former Samsung executive who stole computer chip IP and used it to build a chip manufacturing plant in China.[64] Around the same time, South Korean national police arrested 77 people who were charged with 35 cases of industrial espionage. Similar operations led to around the same number of cases in 2022. Of the 35 cases, 27 were due to technology leaks between companies in South Korea. Eight of the cases dealt with international IP theft; this includes the Samsung executive case.[65] Despite the arrests, as of 2023 only a small percentage of defendants accused of leaking technology had been convicted because proving this type of crime is difficult.[66] In February of 2023, seven people in South Korea were sentenced to prison for giving stolen technologies to a Chinese company. Some of these seven South Koreans worked for a Samsung subsidiary.[67]

In 2024, the Amendments to the Unfair Competition Prevention and Trade Secrets Protection Act of Korea and the Patent Act of Korea was passed to specifically address "alleged theft of IP by overseas companies and governments," as requested by South Korean companies that had experienced theft by Chinese companies.[68] The revisions increased criminal fines, extended the statute of limitations, and increased punitive damages in civil cases for infringement of IP rights. Despite these efforts, there remain limitations to South Korea's ability to effectively counter and deter Chinese threats. Article 98 of the Criminal Act in its current form hinders the government's ability to prosecute economic espionage from an enemy state since the article

=ALL&searchTxt=#:~:text=Korea%20to%20announce%20national%20strategy%20to%20become,Korea%20Institute%20of%20Science%20and%20Technology%20(KIST).

[62] Ibid.

[63] Lee Dong-hwan, "Unified government response to 'technology leak'… Launch of joint government-wide technology leak response team," *Yonhap News* (Seoul), November 8, 2023, https://www.yna.co.kr/view/AKR20231108165500001.

[64] Scott Briscoe, "South Korea Cracks Down on IP Thefts," *ASIS International* (Alexandria, VA), June 12, 2023, https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2023/june/ip-thefts-on-the-rise/.

[65] Ibid.

[66] Davies and Jung-a.

[67] Ibid.

[68] Sean Hayes, "Korea Fighting Chinese Company Espionage through Revisions to Unfair Competition Prevention & Trade Secrets Protection Act of Korea," *IPG Legal* (Seoul), September 9, 2024, https://www.thekoreanlawblog.com/2024/09/korean-espionage-crime-enforcement.html.

currently lists only North Korea as an enemy state. Several politicians have called for reforms to Article 98, calling for China to be added to the list of enemy states so that the government can more effectively prosecute espionage conducted on behalf of China.[69]

### *Policy Recommendations*

While many of the crimes in South Korea within the economic espionage arena are difficult to prove, the South Korean government could help address this challenge by clarifying existing laws. Additionally, forming and expanding programs like the Korean-Pan Government Technology Leak Joint Response Team could assist in economic leaks by promoting cooperation between the government and private industry. Another area that the South Korean government could further address is one of South Korea's greatest threats from Chinese theft and espionage – elite capture. At the most fundamental level, people follow money, making it difficult to stop active workers and retirees from South Korean S&T firms from going to work for a Chinese firm. The South Korean government could create alternative incentives to make workers and retirees more likely to turn down Chinese offers to engage in theft and espionage. A first step could be the creation of a Science and Technology Policy Advisory Board chaired by former highly skilled S&T executives. The board would advise the South Korean government on different S&T policies, economic espionage, and IP theft. A second step would be to start consultant programs in which these former corporate executives are employed by the government to advise private firms on how to enhance their security protocols. These consultants could also work at universities to help educate younger generations on topics such as entrepreneurship, business leadership, economic security, science and technology, etc.

## South Korean Efforts to Address Threats to Academia

In South Korea, the National Research Council of Science & Technology (NST), an organization overseen by the South Korean Ministry of Science and ICT (Information, Communication, and Technology), provides support to 23 government funded research institutes in the fields of science and technology (GRIs). One of the functions of NST is nurturing a culture of research ethics and safety. This includes promoting lab safety and discussions among the GRIs, improving the research safety environment, supporting research facilities and equipment systems to be more secure, and helping to improve procedures based on amended government policies.[70] Similar to the NSF in the US, the National Research Foundation of Korea (NRF) promotes "responsible research" that is useful for academia and society, as well as strong research management.[71] This year, NRF became an associate member of Horizon Europe, an EU research funding program, which among many functions provides guidelines for concerns about dual-use technologies, i.e. those that have applications for both civilian and military purposes.[72] Other

[69] Ben Forney, "Changing South Korea's Espionage Law is Good for Business," KEI (Washington, DC), September 24, 2024, https://keia.org/the-peninsula/changing-south-koreas-espionage-law-is-good-for-business/.
[70] National Research Council of Science & Technology, "Project Management," NST Function, accessed May 5, 2025, https://www.nst.re.kr/eng/contents.do?key=151
[71] "NRF 2019-2020," National Research Foundation of Korea, https://www.nrf.re.kr/resources/file/2019_nrf_eng_intro.pdf.
[72] Yumi Jeung and Yojana Sharma, "South Korea on Track to Join Horizon Despite Turmoil," University World News (London), December 13, 2024, https://www.universityworldnews.com/post.php?story=20241213104547435.

NRF accomplishments include training in research ethics for over 86,000 individuals in the past three years and 471 cases of expanded safety guidance and inspections at research facilities.[73]

Other efforts to address research security concerns in South Korean academia include the Industrial Technology Protection Committee (ITPC). Established under the Ministry of Trade, Industry and Energy, it implements the Act on Prevention of Divulgence and Protection of Industrial Technology, passed in 2011. In its 2024 meeting, the ITPC discussed plans to bolster the security level at vulnerable universities through support for security infrastructure and security consulting services.[74] In 2020, the South Korean government passed the National Research and Development Innovation Act, a comprehensive legal framework designed to enhance South Korea's research and development, which includes the establishment of research support systems at R&D institutions. [75] As mandated by this Act, the Ministry of Science and ICT must ensure through monitoring that the head of a research and development institute, such as a university, formulates and implements security measures "to prevent leakage of important information." [76]

A unique effort to train South Koreans in the field of counter-theft of IP and counterespionage is a 2021 memorandum of understanding between the National Intelligence Service (NIS) and Myongji University, agreeing to cooperate in education programs in the counterespionage and security fields. This agreement aims to help train skilled manpower, as the university plans to create master's and doctorate degrees in defense and security.[77]

Some Korean universities have also been pursuing their own efforts to improve research security. Seoul National University (SNU) has created guidelines for research and development project security management.[78] These guidelines establish standards and procedures to create and implement security measures for research and development projects conducted by SNU professors, as well as researchers affiliated with SNU. The guidelines identify the security level of research and development projects based on four categories: 1) projects related to the development of world-class technology products; 2) projects being promoted for domestic production due to the refusal of technology transfer from foreign countries, or that are recognized as future core technologies and require protection; 3) projects related to national core technologies as defined in Article 2, Paragraph 2 of the Act of Prevention of Leakage and Protection of Industrial Technology; and 4) projects related to strategic technologies under

[73] "About the NRF," National Research Foundation of Korea, accessed Marc 3, 2025, https://www.nrf.re.kr/eng/page/ea516249-2e9a-49f6-a970-edecb77bd1e6.
[74] Ministry of Trade, Industry and Energy, "Trade Minister Chairs 58th Industrial Technology Protection Committee Meeting," *Ministry of Trade, Industry and Energy* (Seoul), December 27, 2024, https://www.korea.net/Government/Briefing-Room/Press-Releases/view?articleId=7765&type=O&insttCode=.
[75] Republic of Korea, "National Research and Development Innovation Act," January 6, 2022, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=62484&type=part&key=18.
[76] Ibid.
[77] "Spy Agency Partners with University for Counterespionage, Security Education Program," *The Korea Herald* (Seoul), October 14, 2021, https://www.koreaherald.com/article/2706493.
[78] "Seoul National University National Research and Development Project Security Management Guidelines," *Seoul National University* (Seoul), June 19, 2009, https://snurnd.snu.ac.kr/rndext/node_view.php?nid=667.

Article 2, Paragraph 4 of the "Act on Promotion of Technology Development." [79] SNU also maintains IP Rights Management Regulations to encourage the creation of IP by SNU faculty and staff.[80]

### *Policy Recommendations*

As with the US, there should be increased efforts in South Korean academia to train scholars and students about research security, potential recruitment efforts, transfers of technology, and threats of IP theft. Information campaigns about those who commit IP theft are important. When a famous academic was sentenced to two years in prison for sharing information of national importance with researchers abroad as a part of the Thousand Talents Program, this was a wake-up call that scientists need to start being protective about their data.[81]

South Korean researchers need to understand what is at stake and how China steals academia's IP. While efforts by the government and academia to address research security in South Korea are growing, they are geared primarily toward general research security, not with specific focus on Chinese threats to S&T research. Likewise, South Korean efforts are not as extensive as those in the US. to address the challenges to S&T research. Such initiatives could be expanded, particularly to include more direct training about the connection between research security and South Korean national security. The NRF is starting to address research security concerns more directly for academia in South Korea, but it would be beneficial for the NRF to create its own version of the NSF SECURE initiative, or to join the US in a joint bilateral initiative, since there is already growing success in the US NSF SECURE Analytics program.

## Whole-of-Government Efforts & Domestic Coordination with Private Industry and Academia in the US and South Korea

While the governments and academia in both the US and South Korea are addressing the challenges of Chinese S&T acquisition in private industry and universities, the most effective means of success require whole-of-government approaches and cooperation by private industry and academia. Certain policies have been put in place to establish this type of strategy in both countries, but to a limited degree. Many of the US measures against China's predatory practices in S&T, in addition to supply chains, will not be successful unless other US allies who lead the industry join in and work together.[82] This is why the US has been working closely with its allies and partners like Japan, South Korea, and Taiwan who possess cutting-edge technologies in critical sectors, such as semiconductors.

The US government has proposed multiple strategies for a whole-of-government approach and efforts to include private industry and academia in addressing Chinese threats to S&T research,

[79] Ibid.
[80] "Seoul National University IP Rights Management Regulations," *Seoul National University* (Seoul), August 29, 2024, https://snurnd.snu.ac.kr/rndext/node_view.php?nid=729.
[81] WooJung Jon, "South Korea Data-Sharing Case is a Wake-up Call," *Nature* 631 (2024): 9.
[82] Cha, Victor D. 2022. "How to Stop Chinese Coercion: The Case for Collective Resilience." *Foreign Affairs,* December 14.

but few, if any, have been implemented. In 2015, President Obama signed an executive order establishing Information Sharing and Analysis Organizations (ISAOs), which "may be organized on the basis of sector, sub-sector, region, or any other affinity, including members that may be drawn from the public or private sectors, or consist of a combination of public and private industry organizations. Recognizing the nationwide threat, the House Committee on Oversight and Accountability Majority Staff recommended in 2024 that, "Federal agencies must strengthen personnel and training to foster the acumen, judgment, language skills, and expertise needed to identify, counter, and defeat CCP political warfare."[83] In addition to government mitigation efforts, the committee staff suggested that the US government should include "fostering the depth of knowledge needed to defeat unrestricted warfare; and (4) engaging the American people about the CCP threat and providing resources when appropriate that thwart CCP ambitions."[84]

In South Korea, as early as 2003, the government pursued whole-of-government approaches to mitigate industrial spying.[85] However, while these efforts happened across government entities, they were not yet coordinated amongst those entities, which means they are not truly whole-of-government. More recently, South Korea has pursued collaboration with the biotechnology industry through the creation of a council including the National Intelligence Service Industrial Confidentiality Protection Center and KoreaBio for the protection of important national technologies. The National Intelligence Service, the Ministry of Trade, Industry and Energy, the Ministry of SMEs and Startups, and the National Police Agency have realized the vitality of industrial security and have strengthened the relationship between public and private entities as well.[86] South Korea has also made strides to engage with likeminded countries for research. They completed negotiations to join the European Union's Horizon Europe, a program to assist with research funding. New Zealand and Canada also joined.[87] This is an effective example of countries aligning with other likeminded nations to get funding for research for young people, researchers, farmers, micro- to medium-sized companies, public bodies, and NGOs, amongst other entities.[88]

While efforts in the US and South Korea have attempted some degree of whole-of-government approaches and collaboration with private industry and academia, there are several limitations to these efforts. The first hurdle is rooted in the most important strength for the US and South Korea - liberalism and the ability for private industry and universities to do the research that they want to do. These entities can support national security priorities and recommendations,

[83] House Committee on Oversight and Accountability Majority Staff, *CCP Political Warfare: Federal Agencies Urgently Need a Government-Wide Strategy* (Washington, DC: House of Representatives, 2024), vi, https://oversight.house.gov/wp-content/uploads/2024/10/CCP-Report-10.24.24.pdf.
[84] Ibid.
[85] Jungbin Lim and Dongkyu Kim, "Future Security Threats: Study on the Human Factor of Industrial Security for the Prevention of Security Leaks in South Korea," *Webology* 19 no. 4 (2022): 298.
[86] Ibid, 297.
[87] David Matthews, "South Korea Joins Horizon Europe in Multi-Billion Euro Push to Globalise Science," *Science Business* (Brussels), March 25, 2024, https://sciencebusiness.net/news/horizon-europe/south-korea-joins-horizon-europe-multi-billion-euro-push-globalise-science.
[88] European Commission, "Eligibility: Who Can Get Funding?," *European Commission*, accessed April 10, 2025, https://commission.europa.eu/funding-tenders/how-apply/eligibility-who-can-get-funding_en.

but they do not have to do so. For example, the governments may receive considerable push back if they mandate private companies to track malign influence from China. Secondly, because China is an authoritarian regime with a significant number of state owned enterprises, the regime can more easily persuade or coerce many parts of Chinese society to engage in irregular competition because the regime has much more control of all sectors of society.[89] The most difficult part in the overall strategic competition with China for the US and South Korea is for these countries to maintain their open societies, while China competes at a different level in the irregular competition space.

A third challenge to efforts mainly pertains to the US, but to some extent to South Korea too. Whole-of-government approaches face logistical challenges. This is because the US federal government is so large that it is nearly impossible to effectively coordinate among agencies. Additionally, turf wars tend to arise when one department believes its responsibilities are being given to another department. Fourth, irregular competition impacts many agencies not traditionally affiliated with national security. The US government has generally limited national security responsibilities to the traditional security departments and agencies, but this limitation is a problem; "irregular warfare alone, implemented primarily by the security sector, is not enough."[90] In this new era of irregular competition, the Department of Education, Department of Energy, Department of Commerce, Department of Treasury, NSF, NIH, and Center for Disease Control and Prevention, among others, are all a part of a whole-of-government approach to national security efforts to counter Chinese threats to S&T research in the US. In South Korea, several agencies should be directly or indirectly involved in countering the threats to S&T research in South Korea. This means training what to look for and track will need to be implemented in the nontraditional security government departments and ministries, universities, and private industry.

Fifth, a unique problem for the US is that the government system of federalism causes problems when including states in national security. The US Constitution clearly states that the federal government's responsibility is to provide for national defense; that is not a state responsibility. However, this distinction does not matter to China. As a result, China will exploit state and local governments and those entities struggle to respond because that is not their constitutional responsibility, they are not well prepared, and they lack the resources. Relatedly, another limitation is that while some US state-level initiatives have been strong, they are not necessarily coordinated with other states or with the federal government, or with US allies like South Korea, who are similarly being targeted by China. This is an area of growth that both the US and South Korea could pursue. The positive signs are that most of the governmental entities want to protect against extra-legal and illegal S&T acquisition by China. On the other hand, private industry and academia are less open to government intrusion on what they may see as institutional autonomy. While awareness and willingness to cooperate with the governments in both the US and South Korea is growing, it is at a slow pace and there is still room for policy improvements. The success of defending against Chinese S&T acquisition in the US hinges on

[89] Lumbaca, 46.
[90] Ibid, 50.

the "ability of the US law enforcement and intelligence apparatus to shift organizational culture and support private industry, academia, and state level governments."[91] While some places have pushed back against government policies for a number of reasons, the Texas A&M University and several other institutions have implemented strategies to mitigate Chinese S&T acquisition.

### *Domestic Coordination Recommendation*

The most obvious area of change is improved coordination amongst the different actors involved in the sectors being targeted to counter Chinese acquisition of S&T research. The main entities that need better coordination would be the federal and national governments, research universities and national laboratories, and the high-tech private industry in the US and South Korea. Thus, a holistic platform where these institutions can coordinate, learn from each other, and help each other would provide a much more effective defense and deterrence against Chinese acquisition of S&T research in these countries.

## Bilateral and Multilateral Coordination between the US and South Korea

In 2023, the national security advisors of each country highlighted "the crucial importance of aligning and adapting our technology protection toolkits, including the recently announced Disruptive Technology Protection Network and investment screening mechanisms, as an important effort to prevent the leakage of sensitive and dual-use technologies."[92] Multiple research agreements between the two countries have been completed and while these do not specifically address IP theft and economic espionage, they can help to alleviate some of the Chinese threats. The US and South Korea are global leaders in science and technology and a part of this success comes from their robust research communities.

Completely stopping international collaborative research simply because of the threat from China is not the solution. However, continuing and expanding the research ties between the US and South Korea can help permit advancement in the science and technology realms while also excluding Chinese threats. Recent examples of cooperation include the 2019 memorandum of understanding (MOU) for a "bilateral partnership for deeper cooperation on science and technology research and development of solutions to disasters such as fire, storm, flood and earthquake and issues closely related to public safety such as security and infectious disease" should be continued.[93] The two countries signed another MOU in 2023 for "enhancing domestic security capabilities through the exchange of information and applications of emerging technologies."[94] In addition, "The Department of Homeland Security (DHS) Science and

[91] Eftimiades, 179.
[92] The White House, *JOINT FACT SHEET: Launching the US-ROK Next Generation Critical and Emerging Technologies Dialogue* (Washington, DC: White House), December 08, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/08/joint-fact-sheet-launching-the-u-s-rok-next-generation-critical-and-emerging-technologies-dialogue/.
[93] US Department of Homeland Security, "News Release: US, Republic of Korea to Partner in Science, Technology, and Information Communication Technology," *Department of Homeland Security* (Washington, DC), October 24, 2019.
[94] US Department of Homeland Security, "News Release: DHS and Republic of Korea Sign Agreement for Homeland Security Research and Development," *Department of Homeland Security* (Washington, DC), March 20, 2023. https://www.dhs.gov/science-and-technology/news/2023/03/20/dhs-and-republic-korea-sign-agreement-homeland-security-research-and-development.

Technology Directorate (S&T) signed a Joint Statement of Intent (JSoI) for collaborative research, development and foreign technical exchanges with the Republic of Korea's Ministry of Science and Information Communication Technology (MSIT). This statement reaffirmed the aforementioned 2019 Memorandum of Understanding and validated with a mutually signed Project Arrangement for Safety and Security Research and Development Collaboration."[95] At the 2024 Camp David Accords with South Korea and Japan, the three countries announced a tri-lateral Disruptive Technology Protection Network. This will "expand collaboration on technology protection measures, including expanding information-sharing and the exchange of best practices across the three countries' enforcement agencies."[96] This coordination is consistent with expert recommendations for the US government to partner with likeminded countries. In addition to coordination and cooperation with South Korea and Japan, the US worked with the EU to create the US-European Union Trade and Technology Council.[97] Other coordination has seen some success with India, Israel, Taiwan, and the United Kingdom.[98]

One area that significantly lacks collaboration between the US and South Korea is export controls. While the US uses export controls for a myriad of reasons, including mitigating IP theft, it inadvertently hurts South Korean firms with foreign direct investment in China, as noted earlier. This is particularly true for Samsung and SK Hynix.[99] Another area that needs to be jointly addressed is how US policy responses have inadvertently created hurdles and difficulties for US allies such as South Korea. Because the CHIPS and Science Act attempts to reshore semiconductor manufacturing to the US, this effort could create problems between the US and South Korea. This is because the act allows the US to investigate South Korean plants if they deem it necessary for US national security. US export controls initiated by the Biden administration have already pushed South Korean industries to focus their R&D and production of technology domestically rather than continuing to invest in their existing factories and labs in China.[100] South Korea is incurring a certain amount of immediate costs, no matter whether such costs are tolerable or not. Even though South Korean firms might not incur direct costs or damages, uncertainty will increase for South Korean industry.[101] For South Korean battery manufacturers that have joint ventures with US companies, South Korea has given "'unofficial guidance'" to South Korean companies requesting only South Korean staff be involved with major technologies at the joint plants.

[95] US Department of Homeland Security, "News Release: DHS and Republic of Korea Sign Joint Statement to Advance Mutual Digitalization Goals," *Department of Homeland Security* (Washington, DC), March 21, 2023. https://www.dhs.gov/science-and-technology/news/2023/03/21/dhs-and-republic-korea-sign-joint-statement-advance-mutual-digitalization-goals.
[96] White House, "FACT SHEET: The Trilateral Leaders' Summit at Camp David," White House (Washington, DC) August 18, 2023, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/08/18/fact-sheet-the-trilateral-leaders-summit-at-camp-david/.
[97] Andrew B. Kennedy, "The Resilience Requirement: Responding to China's Rise as a Technology Power," *Survival* 65 no. 1 (2023): 121.
[98] Ibid, 123.
[99] Jungmin Pak, Hyunsoo Joo, and Haeyoon Chung, "The Impact of Export Controls on South Korean Companies and Pathways to Plurilateral Cooperation," in US-ROK Tech Cooperation: Export Controls, Data Policy, and Artificial Intelligence, eds. Gwanhoo Lee and Doug Strub (Seattle, WA: National Bureau of Asian Research, 2024), 19.
[100] Gregory C. Allen, *China's New Strategy for Waging the Microchip Tech War* (Washington, DC: CSIS, 2023).
[101] Martin Chorzempa, *How US Chip Controls on China Benefit and Cost Korean Firms*, 23-10 (Washington, DC: Peterson Institute for International Economics, (2023), https://www.piie.com/publications/policy-briefs/2023/how-us-chip-controls-china-benefit-and-cost-korean-firms.

Additionally, the two countries face slightly different problems regarding IP theft and economic espionage; however, as they become more intertwined, South Korean problems will become US problems.[102] Continually, US chip controls on China also create difficulties for South Korea. The October 2022 Biden administration export restrictions on advanced semiconductors have created a challenging situation for South Korean firms that have factories in China.[103] As the US attempts to stop IP theft and economic espionage, China has become more aggressive toward South Korea for legal and illegal transfers of IP. China has also targeted Japan and European countries due to US efforts.[104]

## *Recommendations for US-South Korean Coordination*

### *Investigation Exchanges*

Both countries deal with different problems regarding espionage and IP theft from China. Thus, a relatively easy bilateral effort would be to create exchange programs for each country to participate in a month-long investigation experience in the other country. All relevant agencies and offices could be involved. For example, the FBI could send a counterespionage agent to the National Intelligence Service and vice versa for a one-month workforce rotational program. This would help with learning about different threats from China and how each department defends against those threats. It would also foster bilateral collaboration and deepen ties across the governments.

### *Create Higher Education Programs to Train Students to be Private Industry Security Professionals*

The US and South Korea could establish a Center for Economic Security and Counterespionage (CESC) initiative. This could be a joint effort with the US Department of Homeland Security Cybersecurity Infrastructure Security Agency, US Federal Bureau of Investigation, South Korea National Intelligence Service, and major research universities in both countries. Each of the three agencies could fund the curriculum development, professors, and some of the other expenses. Additionally, students from US and South Korean universities could participate in exchange programs to observe and learn about best practices for research security in each other's countries. The end goal would be to train a highly skilled workforce to begin working in security jobs in high-tech companies such as Lockheed Martin or Samsung. Currently, there are few, if any, programs that train students for private industry research security skills beyond physical security and cybersecurity. There are cybersecurity degrees and training, but few non-physical security or insider threat trainings. Additionally, most physical security and insider threat employees are either external consultants or were former government employees. Neither country can or should wait for an FBI agent or police officer to retire in order for universities and companies to achieve the necessary security measures. Both countries could

[102] Christian Davies and Song Jung-a, "South Korea Gets Tough on Tech Leaks to China," *Financial Times* (London), May 16, 2023, https://www.ft.com/content/9e72a96f-5d92-460f-a154-0715c343e7c9.
[103] Martin Chorzempa, *How US Chip Controls on China Benefit and Cost Korean Firms*, 23-10 (Washington, DC: Peterson Institute for International Economics, 2023), 1-2.
[104] Christian Davies and Song Jung-a.

streamline training for young people to go straight into private industry to provide robust economic and IP security measures. This could be called the CESC Program, for which universities could apply for federal funding. This could be similar to the US intelligence community's Centers for Academic Excellence Program. The CESC Program would most likely need to be interdisciplinary with students taking classes from STEM fields, public administration, public policy, and criminology. Each student would graduate with a government approved Economic Security and Counterespionage Certification.

### *Multilateral Effort: The Science, Technology, and Research (STAR) Coalition for Democracy*

There has been some success pursuing S&T security cooperation between likeminded nations around the world. However, something more structured and official could be pursued. The countries in a proposed STAR Coalition could be the United States, the European Union, the United Kingdom, Canada, Israel, Japan, South Korea, Taiwan, the Philippines, Australia, New Zealand, and India. This framework could supplement national government funding agencies for science and technology research at national labs and universities. Research exchanges could highlight research security measures that other countries are using, best practices, and joint efforts to counter IP theft and espionage. Additionally, this could also streamline study abroad options, international student programs, research assistantships, and laboratory work in order to gain experience that may not be available to some students in their home country. Each university, research institution, and national lab that applies for government funding would first have to meet certain benchmarks of research security based on standards agreed upon by all member states. Certain international standards can be used that align with existing initiatives like the EU's toolkit to stop foreign interference in research innovation toolkit.[105] Importantly, there is already momentum for initiatives like the STAR Coalition for Democracy.[106] All these countries could unite under one common cause: creating a secure network of S&T basic research among democracies.

### *Establish a US-South Korean Chinese S&T Acquisition Commission*

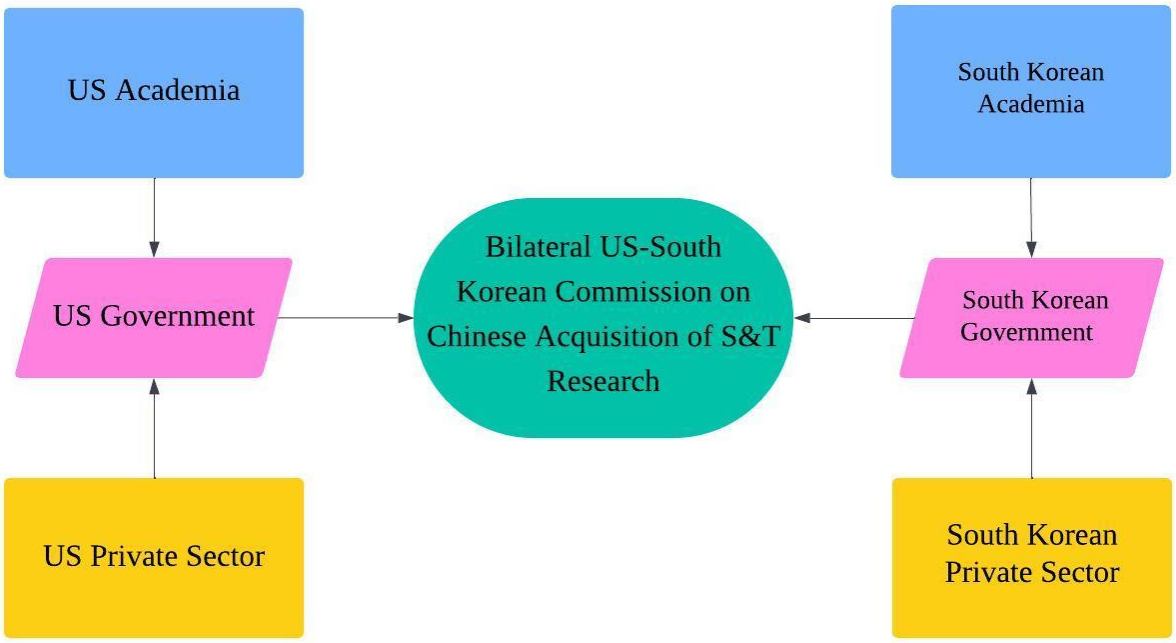
Since both countries have similar and simultaneous experiences with Chinese exploitation and some effective policy approaches, it would be most effective to share information, best practices, shared experiences, and lessons learned. Understanding institutional culture is one aspect that hinders the ability to defend and prosecute Chinese S&T acquisition. To help with this, a bilateral whole-of-society US-South Korean IP Theft and Espionage Commission could be created with an annual summit to be held in South Korea or the US with representatives from governments, private industry, and academia to further discuss findings, trends, and tactics and how the two countries can learn from each other and help each other regarding this problem. At the summit, both countries would have representatives from the state/regional, federal/national governments, private industry, and academia to describe the threats they have

[105] Directorate-General for Research and Innovation, "Commission Publishes a Toolkit to Help Mitigate Foreign Interference in Research and Innovation," *European Commission* (Brussels), January 18, 2022, https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-publishes-toolkit-help-mitigate-foreign-interference-research-and-innovation-2022-01-18_en.

[106] David Matthews and Richard L. Hudson, "G7 Science Ministers Urger Democracies to Unite Research Efforts," *Science Business* (Brussels), June 14, 2022, https://sciencebusiness.net/news/g7-science-ministers-urge-democracies-unite-research-efforts.

been facing and how they have been attempting to mitigate it. Including all members from across society will increase trust and ensure a true whole-of-society approach. Figure 1 outlines the structure of the bilateral commission.

**Figure 1. Bilateral US-South Korean Commission on Chinese Acquisition of S&T Research**




## Conclusion

In a new era of irregular competition, the US and South Korea must protect themselves more effectively from asymmetric threats originating from China. The most comprehensive solution to these problems is a whole-of-government approach and cooperation between government, private industry, and academia. However, this is a major task that requires not only financial investment, but greater awareness and efforts by universities and private industry to work with the governments. While there has been some success in both the US and South Korea to counter and deter Chinese threats to S&T sectors, there are further strategies and policies that can be pursued. Additionally, effective strategies within each government, universities, and private industry can be pursued separately, but these efforts also need to be coordinated as much as possible. Finally, these solutions can be aligned and combined across the two countries and even extended to other like-minded countries. To help the US, South Korea, and their allies win this new era of great power competition, one area that must be effectively addressed is countering the acquisition of S&T research by China through extra-legal and illegal methods.