

South Korea and the Global Regulatory Landscape

Managing Risks Associated with Sanctions,
Trade Controls, and Supply Chains

AUGUST 2022



South Korea and the Global Regulatory Landscape

Managing Risks Associated with Sanctions,
Trade Controls, and Supply Chains

PRISCILLA KIM, EDMUND XU, J. JAMES KIM, HYEONJUNG CHOI
AUGUST 2022

About

The Asan Institute for Policy Studies is an independent, non-partisan think tank with the mandate to undertake policy-relevant research to foster domestic, regional, and international environments conducive to peace and stability on the Korean Peninsula, East Asia, and the world-at-large.

The Asan Institute was established in commemoration of the late Founder and Honorary Chairman of Hyundai Group, Chung Ju-yung, who left an indelible mark on South Korea's modernization and inter-Korean exchanges towards peace. Named after Chung Ju-yung's pen name, "Asan," Dr. Chung Mong Joon founded the Asan Institute on February 11, 2008, in an effort to build a world-class think tank that mirrors South Korea's place on the world stage.

Kharon is a leading provider of risk management solutions driven by proprietary research and data analytics. Kharon rigorously investigates and curates complex data around matters situated at the intersection of global security and commerce — powering financial crimes, sanctions, trade, and export control compliance, supply chain security, and legal and reputational risk mitigation. With teams of multilingual subject matter experts, data scientists, and software engineers, Kharon generates enriched data covering the commercial networks of restricted actors and their related parties — facilitating effective, informed decision-making through critical insights that are accessible and actionable. Kharon's integrated solutions are designed to merge seamlessly with existing screening and analytics environments, due diligence and investigative functions, and training requirements.

Kharon is founded and led by former senior officials of the U.S. Department of the Treasury and experienced technology professionals. Our clients include first-tier international financial institutions, corporates, and public sector entities.

Disclaimer

The views expressed herein are solely those of the authors and do not necessarily reflect those of the Asan Institute for Policy Studies and Kharon.

Authors

Dr. Priscilla KIM is a research analyst for Kharon's Global Knowledge Engagement program, helping build and implement training solutions worldwide. She conducts open-source research on counter-proliferation financing networks, with particular focus on North Korean revenue raising, maritime, and sanctions evasion activity. Priscilla holds a Ph.D from the University of Central Lancashire, focusing on Track II diplomacy between the U.S. and North Korea, and a Master's degree in East Asian Studies from the University of California, Los Angeles (UCLA).

Edmund XU is a senior analyst for Kharon. Edmund co-leads the investigative research unit at Kharon. He is responsible for leading the teams' research into military end use, illicit maritime activity, and other supply chain relationships, diving into networks that trade in weapons of mass destruction, critical infrastructure, and other prohibited and controlled goods. Edmund previously interned with the U.S. Department of State and Carter Center, where he focused on Asia. Edmund holds an M.A. in international relations from Johns Hopkins University (SAIS) and Nanjing University.

Dr. J. James KIM is the director of Center for Regional Studies at the Asan Institute for Policy Studies. He is also a lecturer in the Executive Master of Public Administration program at Columbia University. Previously, Dr. Kim was an assistant professor of political science at the California State Polytechnic University, Pomona. Dr. Kim received a B.S. and M.S. in industrial and labor relations from Cornell University and an M.Phil. and Ph.D. in political science from Columbia University.

Dr. Hyeonjung CHOI is a senior fellow and the director of Public Relations and Publication Department at the Asan Institute for Policy Studies. He is also an adjunct professor of Sustainable Development and Cooperation at Underwood International College, Yonsei University. Previously, Dr. Choi was the Deputy Secretary for Green Growth and the Assistant Secretary for National Agenda at the Presidential Office of the Republic of Korea. Dr. Choi received his B.A. and M.A. from Yonsei University and his Ph.D. in political economy from Purdue University.

Table of Contents

Executive Summary	06
1. Introduction: Implications of the Changing Regulatory Environment for South Korea	08
2. Sanctions Programs	10
2.1. United Nations Security Council	10
2.2. U.S. Government Sanctions and Export Controls	11
2.2.1. <i>China</i>	11
2.2.2. <i>Democratic People's Republic of Korea (DPRK)</i>	13
2.2.2a. <i>Case Study: Supply Chain Risk</i>	15
2.2.3. <i>Iran</i>	15
2.2.4. <i>Russia</i>	16
3. Export Controls	19
3.1. Military End Users	19
3.1a. <i>Case Study: Export to Russian Military End Users</i>	21
3.1b. <i>Case Study: Export to Chinese Military End Users</i>	22

4. Supply Chain Due Diligence	26
4.1. E.O. 14017 “America’s Supply Chains”	26
4.1a. <i>Case Study: Building Resilient Supply Chains</i>	27
4.2. Critical and Emerging Technologies	29
4.2a. <i>Case Study: Technology Protection Strategy</i>	32
4.3. Uyghur Force Labor Prevention Act	34
4.3a. <i>Case Study: Xinjiang Supply Chain</i>	35
5. Strengthening Risk Management Procedures and Processes	38
5.1. Strengthening Sanctions Compliance	38
5.2. Strengthening Export Controls	40
6. Conclusion: Policy Recommendations	42
Appendix: U.S. Critical and Emerging Technology Subfields	45

Executive Summary¹

South Korea and the United States share a long history of bilateral cooperation, forming an important strategic and economic partnership in the Asia Pacific region. South Korea is a significant economic and military force in the region, which draws attention to how the South Korean government, companies, and organizations engage in U.S. Indo-Pacific initiatives, particularly on those that involve China.² The election of Yoon Suk-yeol as the next South Korean president signals an increase in cooperation with the U.S. on issues of mutual security and economic interests, to include addressing North Korea's nuclear weapons ambitions, Iran's nuclear program, China's growth ambitions and human rights policies, Russia's invasion of Ukraine and foreign interference, and more broadly the Indo-Pacific's security and economic stability.

South Korea's trade relations with jurisdictions that are subject to the U.S. and international sanctions and trade restrictions, such as Russia, Iran, and China, increase the significance of U.S. and South Korean cooperation on financial crime and trade controls policies. Exposure to sanctions risk, gaps in anti-money laundering controls and trade in sensitive or restricted technologies raises the need for South Korean financial institutions and multinationals to enhance their capabilities to identify risk and implement controls.

For South Korean companies, staying current on trends and expectations — with respect to global standards, industry best practices, and the U.S. regulatory environment — can be helpful in protecting against enforcement risk and reputational harm. Working towards better alignment with the U.S. and other partners on these regulatory and enforcement matters can also better assist the newly elected Yoon administration

-
1. This report is the result of three-month collaboration in research and writing by a team of experts from both Kharon and the Asan Institute for Policy Studies. While experts from both Kharon and Asan equally contributed to the contents in the body of the report, the case analyses were conducted exclusively by Kharon, and the policy recommendations were made exclusively by experts from the Asan Institute for Policy Studies. The policy recommendations do not necessarily reflect the Asan institute's position.
 2. "U.S.-South Korea Relations," Congressional Research Service, last updated February 24, 2022.

advance South Korea's standing as a well regulated financial and commercial center.”³

This report will provide an overview of U.N. and U.S. sanctions programs relating to China, North Korea, Iran and Russia, and highlight areas of U.S.-South Korea cooperation on sanctions implementation. The report will also discuss U.S. regulations surrounding military end users, and present case studies that highlight how South Korean companies can be exposed to commercial activity that supports military entities in China and Russia. Section four of this report discusses supply chain risk, focusing on U.S. and South Korean regulation on technologies that each country has deemed essential to their respective national security considerations, and the issue of Xinjiang forced labor. This section then introduces case studies that demonstrate possible exposure to the reexport of sensitive technology, and the risk of exposure to forced labor in the global supply chain. Section five discusses strengthening sanctions compliance risk management capabilities.

3. “Yoon Suk Yeol’s Foreign and Security Policy: Confident Diplomacy and Strong National Security (Unofficial Draft Translation),” NK News, March 14, 2022.

1. Introduction: Implications of the Changing Regulatory Environment for South Korea

The U.S.-South Korea alliance has expanded over the years into a comprehensive partnership, with trade and investment ties becoming an important aspect of the bilateral relationship. With the economic growth of South Korea, major U.S. firms are leading investors in the South Korean market. According to figures released by the U.S. government and the International Monetary Fund, after Japan, the U.S. was the second largest source of foreign direct investment in South Korea at over USD 35 billion in 2020,⁴ with key investments in manufacturing, nonbank holding companies, finance and insurance sectors.⁵

In 2020, South Korea was the 7th largest goods export market to the U.S. as well as the 7th largest supplier of imported goods.⁶ South Korean foreign direct investment in the U.S. was over USD 114.1 billion in 2020, an increase of 11% from the prior year.⁷ South Korea also accounted for USD 29.9 billion of technology trade in 2020 with the largest share of that coming to and from the United States at USD 8.43 billion, which accounts for 28.2% of the year's total.⁸

U.S. imports of goods from South Korea totaled \$77.5 billion in 2019, with imports of automobiles, manufacturing and electrical machinery, food products, as well as services in the transport, travel and other sectors, according to figures released by the Office of the U.S. Trade Representative.⁹

4. IMF Coordinated Investment Direct Investment, <https://data.imf.org/?sk=40313609-F037-48C1-84B1-E1F1CE54D6D5&sid=1482331048410>.

5. Ibid.

6. "Korea," Office of the United States Trade Representative, <https://ustr.gov/countries-regions/japan-korea-apec/korea>.

7. IMF Coordinated Investment Direct Investment, <https://data.imf.org/?sk=40313609-F037-48C1-84B1-E1F1CE54D6D5&sid=1482331048410>.

8. "S. Korea's tech trade logs second-highest tally of \$29b in 2020: data," The Korea Herald, January 21, 2022.

With the continuous development of U.S.-South Korea strategic and economic ties, South Korean companies who trade with or in the United States are increasingly exposed to U.S. sanctions and trade controls. As with other foreign companies operating in the U.S. market, South Korean companies must ensure controls are in place to identify sanctions and trade controls exposure, and to implement effective and sustainable policies and procedures to manage risk.

This report provides a brief overview of international and U.S. sanctions programs and trade controls, including recent enforcement actions and guidance from U.S. and South Korean regulators on best practices for implementing effective risk management policies and procedures. Kharon case studies are used to highlight various typologies of industry exposure to the networks that are subject to international and U.S. sanctions.

9. "U.S. - Korea Free Trade Agreement," Office of the United States Trade Representative, <https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta>.

2. Sanctions Programs

2.1. United Nations Security Council

Economic sanctions are a set of coercive measures applied by governments and international bodies, such as the U.N. and European Union, against individuals, entities, or other governments that are intended to influence, alter, or halt a certain activity or behavior.¹⁰ The U.N. Security Council has 14 ongoing sanctions regimes that focus on supporting the settlement of conflicts, promote nuclear non-proliferation, protect human rights and counter terrorism.¹¹ These sanctions range from comprehensive economic and trade sanctions, to more targeted measures, such as arms embargoes, travel bans, and financial or commodity restrictions.¹²

As a member state of the United Nations, South Korea has enacted national laws and regulations that implement the sanctions measures adopted by the U.N. Security Council, and has established a legal system to fully carry out enforcement decrees or notices to implement specific measures.¹³ For example, U.N. member states were obligated by December 2019 to repatriate North Korean workers, a major foreign currency source for the North Korean government.¹⁴ Through the Inter-Korean Exchange and Cooperation Act, South Korea ensured its compliance with the U.N. resolution by mandating South Korea nationals seeking to hire workers from North Korea to obtain approval from the Ministry of Unification.¹⁵

10. "OHCHR and unilateral coercive measures," United Nation Human Rights Office of the High Commissioner, www.ohchr.org/en/unilateral-coercive-measures.

11. "Sanctions," United Nations Security Council, www.un.org/securitycouncil/sanctions/information.

12. Ibid.

13. Cho Hyun, "Letter dated 20 March 2020 from the Permanent Representative of the Republic of Korea to the United Nations addressed to the Chair of the Committee," March 20, 2020.

14. "Resolutions," 1718 Sanctions Committee (DPRK), www.un.org/securitycouncil/sanctions/1718/resolutions.

15. Cho Hyun, "Letter dated 20 March 2020 from the Permanent Representative of the Republic of Korea to the United Nations addressed to the Chair of the Committee," March 20, 2020.

2.2. U.S. Government Sanctions and Export Controls

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces over 35 economic sanctions programs.¹⁶ Similar to the U.N. programs, U.S. sanctions can be either comprehensive or targeted, using the blocking of assets or certain restrictions to pursue foreign policy and national security objectives.¹⁷ Comprehensive sanctions generally prohibit trade with a specific country or region, while targeted sanctions impose restrictions that target specific activities.¹⁸ This section will provide a brief focus on OFAC's China, North Korea, Iran, and Russia sanctions programs.

2.2.1. *China*

The U.S. has imposed a series of export control restrictions and sanctions on select Chinese companies, government agencies, military organizations, universities, and individuals over the last several years. Certain Chinese state-owned enterprises, government agencies, officials, and companies are subject to economic sanctions for human rights abuses in Xinjiang,¹⁹ undermining Hong Kong's autonomy (Executive Order 13936),²⁰ and for activities relating to U.S. and U.N. sanctions against North Korea, Iran, and Venezuela.

The U.S. has also imposed investment-related restrictions for certain Chinese military companies, due to concerns regarding China's military-industrial complex and the threat that it poses to U.S. national security. In January 2021, the U.S. government enacted Executive Order 13974, which prohibits all U.S. investors from purchasing or investing in securities of companies that are listed on OFAC's Non-SDN Chinese

16. "Sanctions Programs and Country Information," U.S. Department of the Treasury.

17. *Ibid.*

18. "OFAC Embargoes and Sanctions," Visual OFAC.

19. "Treasury Sanctions Chinese Entity and Officials Pursuant to Global Magnitsky Human Rights Executive Order," U.S. Department of the Treasury, July 31, 2020.

20. "Hong Kong-Related Sanctions," U.S. Department of the Treasury.

Military Industrial Complex Companies List (Non-SDN CMIC List).²¹ Five months later, on June 3, 2021, a new order expanded the criteria for designation beyond Chinese military companies to also include companies in the surveillance technology sector.²² With these new regulations, companies engaged in, or supporting, the mistreatment of Uyghur Muslims in the Xinjiang region of China, and/or the development or sale of human surveillance technology are at an increased risk of sanctions.²³

In the May 2021 U.S.-South Korea summit, the two countries stated their opposition to “all activities that undermine, destabilize, or threaten the rules-based international order” and voiced their commitment to maintain peace and stability and defend international rules and norms in the South China Sea and Taiwan Strait.²⁴ The U.S. think tank Rand commented that the May 2021 joint statement gave the appearance that the U.S. and South Korea had a “coordinated approach on matters concerning China,” but that it “may not be a true indication” that South Korea is aligned with U.S. efforts to counter China.²⁵ Yoon Suk-yeol, the then Presidential candidate of South Korea, wrote in a February 2022 article for Foreign Affairs that “as U.S.-Chinese tensions have grown, South Korea has failed to adapt, maintaining an approach of strategic ambiguity without stating a principled position. Seoul’s reluctance to take a firm stand on a number of issues that have roiled the relationship between Washington and Beijing has created an impression that South Korea has been tilting toward China and away from its longtime ally, the United States.”²⁶

21. Executive Office of the President, “Addressing the Threat from Securities Investments That Finance Communist Chinese Military Companies,” Federal Register, November 17, 2020.

22. “Addressing the Threat from Securities Investments that Finance Certain Companies of the People’s Republic of China,” U.S. Department of the Treasury, June 3, 2021.

23. “Global Magnitsky Designations; North Korea Designations; Burma-related Designations; Non-SDN Chinese Military-Industrial Complex Companies (NS-CMIC) List Update,” U.S. Department of the Treasury, December 10, 2021.

24. Scott A. Snyder, “The U.S.-South Korea Summit: A Relationship Restored?” Council on Foreign Relations, May 25, 2021.

25. Soo Kim, “Takeaways from the Biden-Moon Summit: Three Observations on China,” The RAND Blog, June 7, 2021.

26. Suk-yeol Yoon, “South Korea Needs to Step Up,” Foreign Affairs, February 8, 2022.

2.2.2. Democratic People's Republic of Korea (DPRK)

In February and March 2022, North Korea conducted more than 11 ballistic missile launches, including two tests of a new intercontinental ballistic missile system.²⁷ In response to the two ICBM tests, the U.S. imposed new sanctions against foreign individuals and entities responsible for procuring goods for North Korea's nuclear and ballistic missile programs.²⁸ In March 2022, the U.S. sanctioned two Russian individuals and three entities based in Russia for assisting the proliferation efforts of North Korean national Pak Kwang Hun. Pak, who was sanctioned by the U.S. in January 2018, is a representative of Korea Ryonbong Corporation, which specializes in acquisitions for North Korea's defense industries and support for military-related sales. On April 1, the U.S. sanctioned North Korea's Ministry of Rocket Industry and four related companies for supporting the country's weapons development programs.²⁹

Since June 2008, the U.S. has implemented unilateral sanctions against North Korea that target a larger list of individuals and businesses than the U.N. sanctions.³⁰ Under the Trump administration, the U.S. implemented a campaign designed to impose "maximum pressure"³¹ on North Korea to cut off funding to the regime and its weapons development program.³² In September 2017, the Trump administration enacted E.O. 13810, which broadly expanded U.S. sanctions against North Korea, targeting key sectors of its economy, persons doing business with North Korea, aircraft and vessels that have traveled to North Korea, and funds of North Korean persons. Additionally, the E.O. authorizes the imposition of secondary sanctions on foreign financial institutions

27. Amanda Macias, "North Korea is developing a new long-range missile system, U.S. official says," CNBC, March 10, 2022.

28. "Treasury Targets Russian Individuals and Entities Supporting DPRK Weapons of Mass Destruction and Ballistic Missile Programs," U.S. Department of the Treasury, March 11, 2022.

29. "Treasury Targets Democratic People's Republic of Korea (DPRK) Weapons of Mass Destruction Organization and Subsidiaries," U.S. Department of the Treasury, April 1, 2022.

30. "North Korea Sanctions," U.S. Department of the Treasury.

31. "Testimony of Assistant Secretary Marshall S. Billingslea Before House Foreign Affairs Committee on Threat Posed by North Korea," U.S. Department of the Treasury, September 12, 2017.

32. "Remarks by Secretary Mnuchin on President Trump's Executive Order on North Korea," U.S. Department of the Treasury, September 21, 2017.

that engage in transactions involving North Korea.³³

In that same month, the U.N. also imposed new sanctions on North Korea in response to its nuclear test on September 2.³⁴ The sanctions included a limitation on imports of petroleum products to North Korea, and a ban on North Korean textile imports and the provision of work authorizations to North Korean nationals.³⁵ Two months later, the U.N. required member states to repatriate North Korean workers within 24 months from December 22, 2017.³⁶

To assist industry in complying with sanctions, the U.S. Treasury Department and other agencies have released guidance material that highlights sanctions evasion tactics relating to supply chain, illicit shipping practices, and ballistic missile procurement.³⁷

In April 2022, the then President-elect of South Korea, Yoon Suk-yeol, met the visiting U.S. envoy for North Korea to coordinate North Korea policy under the new government. According to a foreign policy platform by Yoon's transition team,³⁸ the Yoon administration aims to bolster the U.S.-South Korea alliance and respond firmly to the North Korean nuclear and missile threat. In addition, Yoon had stated that he would expand South Korea's defense and deterrence capabilities in conjunction with the U.S. alliance.³⁹ He proposed that his administration would make economic aid to North Korea and inter-Korean economic cooperation contingent upon North Korea's denuclearization process.⁴⁰

33. "Executive Order 13810 of September 20, 2017. Imposing Additional Sanctions with Respect to North Korea," U.S. Department of the Treasury, September 25, 2017.

34. "Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Including Bans on Natural Gas Sales, Work Authorization for Its Nationals," United Nations, September 11, 2017.

35. Ibid.

36. "Resolutions 1718," United Nations Security Council.

37. "North Korea Sanctions," U.S. Department of the Treasury.

38. Arius Derr and Chaewon Chung, "Yoon lays out plans for Seoul to 'lead' North Korea sanctions implementation," NK News, March 14, 2022.

39. Ye Hee Lee and Min Joo Kim, "Under new, conservative president, South Korea is poised to adopt a more hawkish foreign policy," The Washington Post, March 10, 2022.

40. Ibid.

2.2.2a. Case Study: Supply Chain Risk

The U.S. prohibits the import of “any goods, wares, articles, and merchandise mined, produced, and manufactured wholly or in part” by North Korea. According to the U.S. Customs and Border Protection, Chinese sportswear brand Li-Ning Sports Goods uses North Korean labor in its supply chain.⁴¹

The website of Li-Ning Sports Goods states that it “successfully established design and development centers” in China, Hong Kong, the U.S., and South Korea.⁴² Li-Ning branded shoes and other attire can be purchased on various South Korean e-commerce platforms.⁴³

In November 2021, a media reported that clothing manufacturing orders made by South Korean companies are being processed by North Korean workers in China.⁴⁴ According to a July 2018 U.S. advisory, one of the heightened risks for businesses with supplier connections to North Korea is suppliers shifting manufacturing to a North Korean factory without telling the customer.⁴⁵

2.2.3. Iran

The Biden administration has engaged in multilateral dialogue with the EU, U.K., China, Russia, and Iran to pursue a return to the Joint Comprehensive Plan of Action (JCPOA), the 2015 agreement that provided partial sanctions relief to Iran in return for Iran’s compliance with restrictions on its nuclear program.

In May 2018, the U.S. announced its withdrawal from the JCPOA, and since August

41. “Risks for Businesses with Supply Chain Links to North Korea,” U.S. Department of the Treasury, July 23, 2018.

42. “Brand History,” Li-Ning Sports Goods, <https://lining.com/mobile/history.html>.

43. Korean records, documents held by the author.

44. Seulkee Jang, “N. Korean workers in China are making clothes for South Korea,” Daily NK, November 3, 2021.

45. “Risks for Businesses with Supply Chain Links to North Korea,” U.S. Department of the Treasury, July 23, 2018.

2018, has reinstituted and, in some cases, expanded sanctions against Iran that were in place prior to the JCPOA. The U.S. placed prohibitions on large swaths of Iran's industries, including its energy, automotive, banking, metals and mining sectors in addition to organizations involved in Iran's nuclear program. The U.S. has also taken a variety of actions focused on isolating Iran's maritime industry by prohibiting the provision of maritime services by bunkering agents, ports, and other related entities that may provide services to vessels affiliated with the Iranian government or sanctioned actors. In March 2022, the U.S. sanctioned an Iran-based procurement agent and its network of companies that sought ballistic missile propellant-related materials for the Islamic Revolutionary Guard Corps Research and Self Sufficiency Jihad Organization.⁴⁶

OFAC has published industry-specific advisories related to Iran sanctions risk, including civil aviation and maritime trade supply chain. The advisories discuss schemes to evade sanctions and facilitate transactions prohibited by the U.S.⁴⁷

In January 2022, the U.S. approved an exemption to South Korea, allowing for the payment of USD 63 million in overdue damages to an Iranian government-linked company, Dayyani Holdings.⁴⁸ The decision emerged from talks to restore the 2015 nuclear deal. A month later, South Korea and Iran held working-level talks on resuming imports of Iranian crude oil and unfreezing Iranian funds held in South Korea.⁴⁹ The two countries discussed the trading of oil and oil products, on the condition that sanctions are lifted as progress is made in nuclear negotiations.

2.2.4. Russia

In response to Russia's invasion of Ukraine in February 2022, the U.S., EU, U.K. and other governments, including South Korea, imposed a wide range of sanctions and trade restrictions, which can be broken into five broad categories:

46. "Treasury Sanctions Key Actors in Iran's Ballistic Missile Program," U.S. Department of the Treasury, March 30, 2022.

47. "Iran Sanctions," U.S. Department of the Treasury.

48. Golnar Motevalli and Patrick Sykes, "U.S. Allows South Korea to Send Funds to Iran in Talks Success," Bloomberg, January 12, 2022.

49. "South Korea, Iran discuss resuming oil trade, unfreezing funds," Reuters, February 16, 2022.

1. Russia's Central Bank and its sovereign wealth fund;
2. Russia's largest financial institutions;
3. Russian military and government officials;
4. Oligarchs and key business elites, as well as their family members; and
5. Russian state-owned companies and entities operating in the defense, aerospace, maritime, coal and other key sectors of the Russian economy.

On April 7, the U.S. designated Russian state-owned enterprises Public Joint Stock Company Alrosa and United Shipbuilding Corporation.⁵⁰ A week prior, the U.S. announced sanctions targeting Russia's technology sector to impede the procurement of critical western technology.⁵¹ In addition, the U.S. enhanced and expanded sanctions that apply to the aerospace, marine and electronics sector of the Russian economy.⁵² The U.S. also prohibited the import of Russian-origin fish, seafood, alcohol, and non-industrial minerals, as well as the export of luxury goods to Russia, and a broad ban on new investment in the Russian economy.⁵³

On March 15, the EU announced a prohibition on transactions with some Russian state-owned enterprises linked to the military and defense sector, a ban on new investments in the Russian energy sector, and a moratorium on the import of Russian steel and the export to Russia of luxury items, including automobiles, jewelry and designer products.⁵⁴ The EU adopted a fifth package of sanctions on April 8, which introduced new sectoral measures targeting the Russian economy.

In February, the South Korean Foreign Affairs Ministry stated that South Korea would implement U.S. and European sanctions on Russian imports and exports, but that

50. "The United States Sanctions Major Russian State-Owned Enterprises," U.S. Department of the Treasury, April 7, 2022.

51. "Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," U.S. Department of the Treasury, March 31, 2022.

52. Ibid.

53. "Executive Order on Prohibiting Certain Imports, Exports, and New Investment with Respect to Continued Russian Federation Aggression," The White House, March 11, 2022.

54. "Western Governments Approve New Round of Sanctions Against Russia," The Kharon Brief, March 17, 2022.

South Korea would not impose its own separate sanctions measures.⁵⁵ Strategic items that would be banned include supplies of electronics, semiconductors, computers, information and communication, sensors and lasers, navigation and avionics, and marine and aerospace equipment.⁵⁶ South Korea also joined the U.S., Canada, and the EU in calling for the blocking of key Russian banks from the SWIFT international payment system.⁵⁷ On March 1, the finance ministry said it would suspend financial transactions with seven Russian banks (Sberbank, VEB, PSB, VTB, Otkritie, Sovcom and Novikom) and their subsidiaries.⁵⁸

55. Eunice Kim, "South Korea to Join Russia Sanctions, But Won't Lodge Its Own," Voice of America, February 25, 2022.

56. Hyonhee Shin and Cynthia Kim, "South Korea bans exports of strategic items to Russia, joins SWIFT sanctions," Reuters, February 28, 2022.

57. "In rare stand, South Korea, Singapore unveil sanctions on Russia," Al Jazeera, February 28, 2022.

58. "South Korea sets out sanctions on Russian banks, state bonds," Channel News Asia, March 1, 2022.

3. Export Controls

3.1. Military End Users

In December 2020, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) amended the Export Administration Regulations (EAR) by adding a new Military End User (MEU) list.⁵⁹ The EAR seeks to control exports of dual use and commercial commodities, software, and technology that originate in the U.S. as well as items developed or manufactured outside the United States, for those that comprise sensitive U.S.-origin components, software, or technology.

For items developed or manufactured outside the U.S., the de minimis rule determines if the item is subject to the EAR. Under the de minimis rule, a foreign-made commodity is subject to the EAR based upon the percentage by value of U.S.-origin controlled content in the foreign-made item.⁶⁰ For instance, if a non-U.S.-made commodity contains more than 25% of controlled U.S.-origin content by value, it is subject to the EAR.⁶¹

The MEU rule (military end use/military end user) restricts the transfer of items in situations that the BIS has determined may be destined for military end uses in restricted countries, as well as the transfer of covered items to foreign entities engaged in military end use activities. Countries covered by the MEU rule include Myanmar (Burma), Cambodia, China, Russia, and Venezuela.

Goods restricted under the "military end use" rule include those incorporated into military items described in the U.S. Munitions List (USML) or under the Export

59. U.S. Department of Commerce Bureau of Industry and Security, "Addition of 'Military End User' (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List," Federal Register, December 23, 2020.

60. Sharron Cook and Nancy Kook, "De minimis & Direct Product Rules," U.S. Department of Commerce Bureau of Industry and Security, December 16, 2015.

61. "De minimis Rules and Guidelines," U.S. Department of Commerce Bureau of Industry and Security, as modified on November 5, 2019.

Control Classification Numbers, which can include any item that supports or contributes to the operation, installation, maintenance, repair, overhaul, refurbishing, development, or production of said military items destined for covered countries.⁶²

Entities restricted under the “military end user” rule include a covered country’s national armed services (i.e., army, navy, marine, air force, or coast guards) and national police, government intelligence or reconnaissance organizations, or any person or entity whose actions or functions are intended to support military end uses described under the military end use restrictions above.⁶³

Following the invasion of Ukraine, BIS implemented stricter restrictions on the export of covered items to Russia, expanding the definition of covered items to include any item subject to the EAR except for food and medicine.⁶⁴ For Russian “government end users” and state-owned enterprises, presumably including military end users, all items subject to the EAR, even food and medicine, now require a license for export.

With the creation of the MEU list, BIS indicates that it considers the listed parties to be military end users, and that a license is required when an entity on the MEU list is a party to a transaction. However, the U.S. government has noted that the initial BIS MEU list “is not exhaustive, and exporters, reexporters, and transferors must still conduct due diligence for parties not on the list.”⁶⁵ BIS notes that the establishment of this MEU List “does not imply that other parties, not included on the list, are

62. U.S. Department of Commerce Bureau of Industry and Security, “Expansion of Export, Reexport, and Transfer (in-Country) Controls for Military End Use or Military End Users in the People’s Republic of China, Russia, or Venezuela,” Federal Register, April 28, 2020.

63. “§ 744.21 Restrictions on certain <military end use> or <military end user> in Belarus, Burma, Cambodia, the People’s Republic of China, the Russian Federation, or Venezuela,” Code of Federal Regulations, up to date as of May 18, 2022.

64. U.S. Department of Commerce Bureau of Industry and Security, “Implementation of Sanctions Against Russia Under the Export Administration Regulations (EAR),” Federal Register, March 3, 2022.

65. U.S. Department of Commerce Bureau of Industry and Security, “Addition of ‘Military End User’ (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List,” Federal Register, December 23, 2020.

not subject to [similar] controls under EAR,” indicating that the U.S. exporters are responsible for conducting due diligence regarding their transactions involving exports to countries like China and Russia.⁶⁶

The legal repercussions of an MEU listing are different from those under comprehensive financial sanctions in that it does not mean a ban on commercial or financial activity. The goal is to restrict the trade of certain goods with military end users or for military end uses in designated countries by requiring companies to obtain licenses from the BIS for these transactions.

3.1a. Case Study: Export to Russian Military End Users

A review of procurement records and trade data shows that South Korean companies have sold sensitive items to suppliers operating on behalf of Russian and Chinese military end users.

In January 2019, Russia-based Joint Stock Company Concern Sea Underwater Weapon Gidropribor signed a contract with a Russian supplier to obtain South Korean-origin CNC metal cutting tools, worth over RUB 5 million.⁶⁷ According to the tender document, the contract was signed with Russia-based JSC IPK Finval, a leading supplier of engineering solutions, industrial machinery, gear, tools and equipment.

On their website, Finval says that they “supply” equipment from several multinational corporations around the world, including those from South Korea.⁶⁸ Trade data shows that one South Korean manufacturer shipped over USD 9 million worth of CNC metal machining equipment to Finval from January 2018 to January 2022.⁶⁹ The product types in these shipments are similar to those ultimately sold to JSC Concern Sea Underwater Weapon Gidropribor.

66. Ibid.

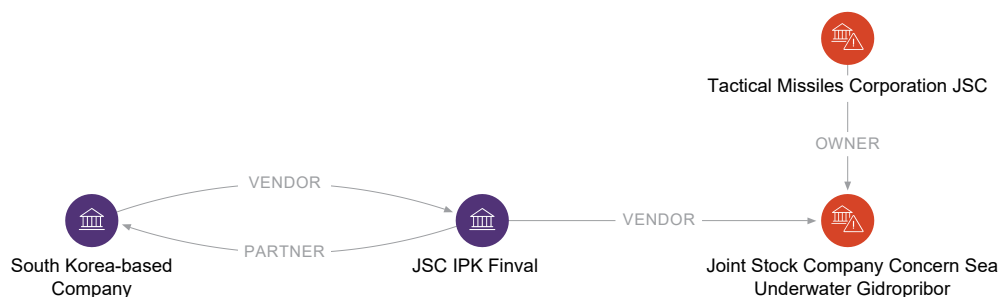
67. Russian records, documents held by the author.

68. “Structure and Governing Bodies of an Educational Organization,” Training Center FINVAL Group of Companies, <https://finval.ru/edu/sveden/struct>.

69. Trade data, documents held by the author.

JSC Concern Sea Underwater Weapon Gidropribor is a scientific production center that develops and manufactures underwater weapons and special-purpose assets for the Russian and foreign navies.⁷⁰ The company was sanctioned by the U.S. on March 24, 2022 for being a part of Russia’s defense-industrial base and producing weapons that have been used in Russia’s invasion of Ukraine.⁷¹

JSC IPK Finval, the intermediary supplier of the South Korean equipment, has not been sanctioned or publicly listed as subject to trade restrictions. In many cases, procurement agents, distribution partners, and other trade intermediaries who are involved in acquiring goods and technology present a challenge in identifying military end use or end user risk.



3.1b. Case Study: Export to Chinese Military End Users

In December 2021, Shennan Circuits Co., Ltd., a China-based company principally engaged in the design, development and manufacture of printed circuit boards, issued a bid for an “automatic optical inspection machine”⁷² made by a South Korean developer and supplier of inspection equipment.⁷³

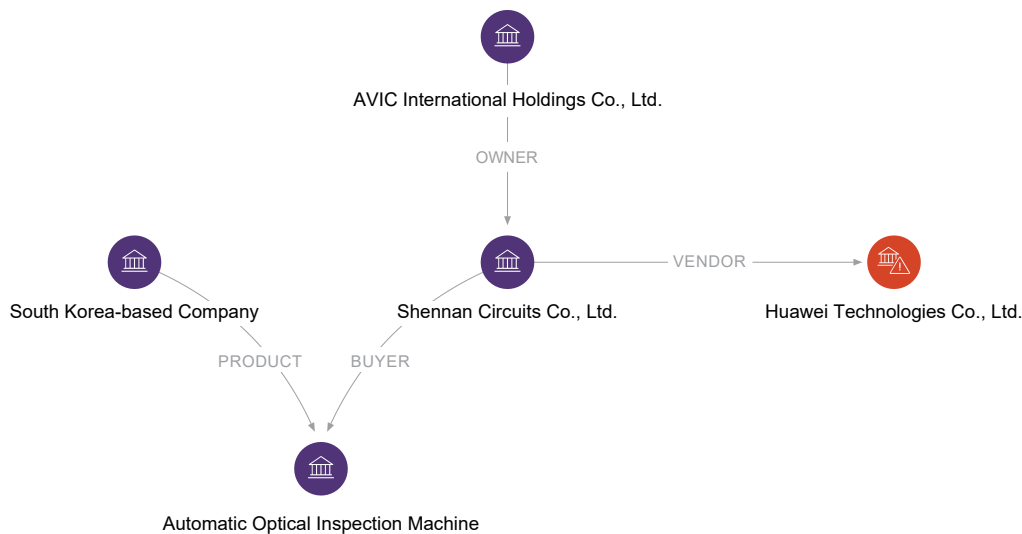
70. “History,” JSC “Concern Sea Underwater Weapon-Gidropribor,” <https://www.gidropribor.ru/en/home/history/>.

71. “U.S. Treasury Sanctions Russia’s Defense-Industrial Base, the Russian Duma and Its Members, and Sberbank CEO,” U.S. Department of the Treasury, March 24, 2022.

72. Chinese records, documents held by the author.

73. Korean records, documents held by the author.

The controlling shareholder of Shennan Circuits is AVIC International Holdings Co., Ltd, which was added to the BIS Military End User List in December 2020. According to Shennan Circuit's 2019 annual report, Huawei Technologies Co., Ltd. was an "important" and "strategic customer" of Shennan Circuits.⁷⁴ The 2019 annual report highlights that Shennan Circuits was the recipient of "Huawei's 'Golden Core Supplier' for seven consecutive years."⁷⁵



Huawei Technologies was listed on the BIS Entity List in May 2019.⁷⁶ The U.S., Australia, Sweden, and the U.K. have banned Huawei from their 5G networks due to concerns that China could use Huawei equipment as a conduit for espionage.⁷⁷

74. "Shennan Circuits Co., Ltd. 2020 Annual Report," Shenzhen Stock Exchange, March 2021.

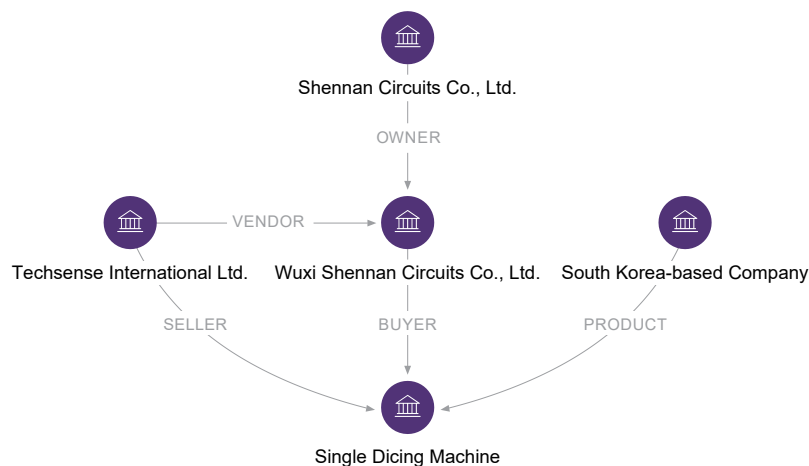
75. Ibid.

76. U.S. Department of Commerce Bureau of Industry and Security, "Addition of Entities to the Entity List," Federal Register, March 21, 2019; "Huawei Entity List Frequently Asked Questions (FAQs)," U.S. Department of Commerce Bureau of Industry and Security, last updated December 3, 2020.

77. Jordan Robertson and Jamie Tarabay, "Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack," Bloomberg, December 16, 2021.

Effective May 2020,⁷⁸ the U.S. Commerce Department expanded the Foreign Direct Product Rule (FDPR), preventing Huawei from receiving any foreign-produced items that incorporate or are produced with controlled U.S.-origin technology or software, unless a license is obtained.⁷⁹

In November 2021,⁸⁰ Shennan Circuits' subsidiary, Wuxi Shennan Circuits, issued a bid for a single dicing machine produced by a South Korean company that produces "essential semiconductor/display equipment."⁸¹ The South Korean company is one of two in the country that make etching equipment, a national core technology of South Korea.⁸² The bid was won by Shanghai-based Techsense International Ltd., which according to its website is a "first-class supplier of semiconductor automation equipment."⁸³



78. Kay C. Georgi et al., "BIS Expands the Huawei Foreign Direct Product Rule to Capture a Wide Swath of COTS Products," ArentFox Schiff, August 19, 2020.

79. Kelley Drye & Warren LLP, "Commerce Department Consolidates and Clarifies the Foreign-Made Direct Product Rules Amid Rising Tensions with Russia," JD Supra, February 8, 2022.

80. Chinese records, document held by the author.

81. Korean records, document held by the author.

82. Han, JY, "National core technology designation for semiconductor and display production equipment to be delayed to December," The Elec, April 17, 2019.

83. "About Us," Techsense International Ltd, <https://www.techsense.cn>.

Wuxi Shennan Circuits is focused on its high-end flip chip packaging substrate project, according to media reports.⁸⁴ Flip chip technology is often applied to military and defense environments.⁸⁵

84. "IC Substrate Industry Research Report: Unbalanced Supply and Demand Accelerates Domestic Substitution, IC Substrate Industry Development," Min News, May 21, 2022.

85. "Flip Chip Technology Market - Growth, Trends, COVID-19 Impact, and Forecasts (2022 - 2027)," Global News Wire, February 18, 2022.

4. Supply Chain Due Diligence

Concerns over supply chain security first emerged publicly in the debate surrounding the U.S.-China strategic competition as early as 2018, but its significance has escalated with the onset of the COVID-19 pandemic as countries and suppliers struggled to secure adequate quantities of personal protective equipment (PPE), medical supplies, and eventually other consumer goods and products. As a result, the U.S. and South Korean government engaged in a comprehensive review of their respective supply chains that are critical to their economic and national securities.⁸⁶

4.1. E.O. 14017 “America’s Supply Chains”

On February 24, 2021, the U.S. President Joe Biden signed Executive Order 14017: “Securing America’s Supply Chains” directing government-led supply chain reviews of industries deemed critical to America’s economic and national security in agriculture, defense, energy, IT, minerals and mining, public health and transportation.⁸⁷ The first review announced in June 2021 examined vulnerabilities in four key sectors: semiconductor manufacturing and advanced packaging, large capacity batteries, critical minerals and materials, and pharmaceuticals and active pharmaceutical ingredients.⁸⁸

Following some of the report’s recommendations, the Biden Administration has worked with the private sector to expand investment and loans for the manufacturing of medical supplies and semiconductors as well as batteries and sustainable rare earth mineral production outside of China. A second set of reviews released in February 2022 provided insights into the administration’s policies in energy,⁸⁹ transportation,⁹⁰ agriculture,⁹¹ public health,⁹² information and communications technology,⁹³ and the defense industry.⁹⁴ Together, these reports recommend further addressing long term supply chain vulnerabilities by revitalizing domestic manufacturing and American

86. “South Korea to create a fund to cope with supply chain challenges,” Reuters, February 13, 2022.

87. “Executive Order on America’s Supply Chains,” The White House, February 24, 2021.

88. “Fact Sheet: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities,” The White House, June 8, 2021.

labor through the combined use of federal spending, reinforced trade regulations, and cooperation with allies and partners.

4.1a. Case Study: Building Resilient Supply Chains

National Defense Authorization Act (NDAA) Section 889, which went into effect August 13, 2020, prohibits U.S. government agencies, federal contractors, and federal grant/loan recipients from purchasing or using “telecommunications and video surveillance services or equipment” from a specified list of Chinese technology companies as well as their subsidiaries and affiliates.

Hytera Communications Co., Ltd. is subject to NDAA Section 889 restrictions as a Chinese manufacturer of surveillance technology. Hytera Communications Co., Ltd. owns 100% of Canada-based Norsat International Inc., according to a 2020 Shenzhen Stock Exchange disclosure.

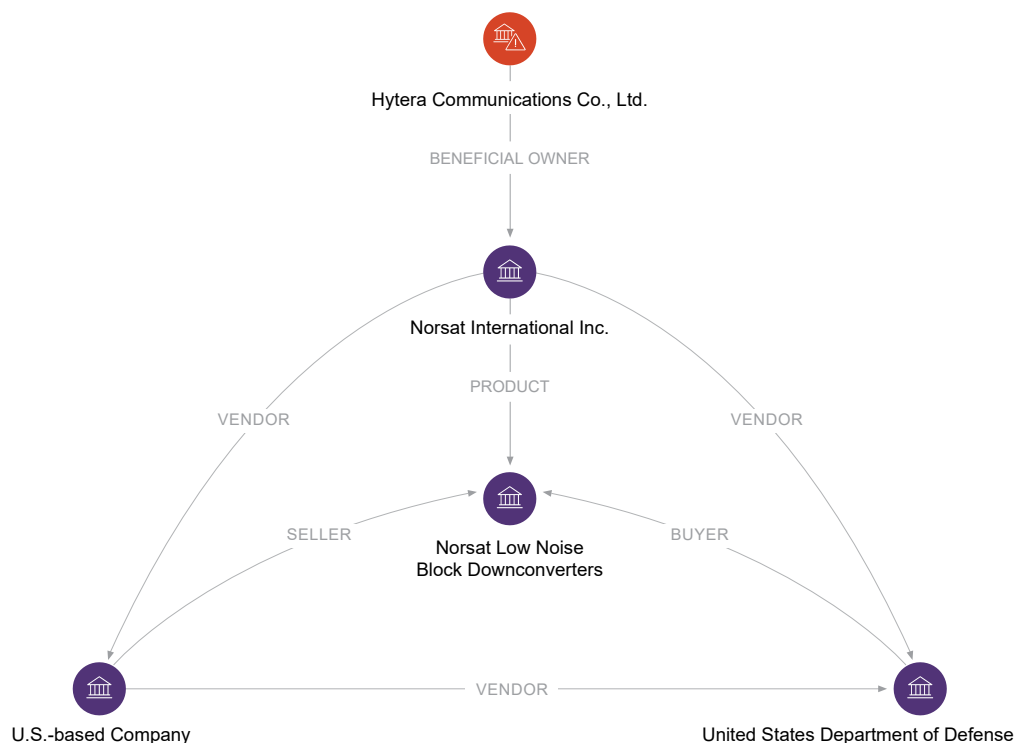
Norsat International Inc. is a provider of communication solutions that enable the transmission of data, audio, and video for remote applications. Norsat’s products and services include customizable satellite components, portable satellite terminals, maritime solutions, and satellite networks.

A website for Norsat International advertises that its products and services are used

-
89. “America’s Strategy to Secure the Supply Chain for a Robust Clean Energy Transition,” U.S. Department of Energy, February 24, 2022.
 90. “Supply Chain Assessment of the Transportation Industrial Base: Freight and Logistics,” U.S. Department of Transportation, February 2022.
 91. “USDA Agri-Food Supply Chain Assessment: Program and Policy Options for Strengthening Resilience,” U.S. Department of Agriculture, February 2022.
 92. “Public Health Supply Chain and Industrial Base One-Year Report,” U.S. Department of Health & Human Services, February 2022.
 93. Prepared by U.S. Department of Commerce and U.S. Department of Homeland Security, “Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry,” U.S. Department of Homeland Security, February 23, 2022.
 94. “Securing Defense-Critical Supply Chains,” U.S. Department of Defense, February 2022.

extensively by telecommunications services providers, emergency services and homeland security agencies, military organizations, health care providers, news organizations and Fortune 1000 companies.⁹⁵

In 2008, Norsat International opened a research and development facility in Daejeon, South Korea.⁹⁶ The R&D facility focuses specifically on components for the company's microwave products and satellite systems business units.



In October 2020, a department of the U.S. government issued a contract for Norsat manufactured satellite telecommunication products.⁹⁷ The contract was won by a U.S.-based global satellite equipment distributor and integrator, which advertises on

95. "About Norsat," <https://www.norsat.com/pages/about-us>.

96. "NII Norsat Int'l to open R&D centre in South Korea," <https://www.iitp.kr/en/2/notice/globalNews/view.it?identifier=0000333525>.

97. Contract Award, documents held by authors.

its website that it is an exclusive distributor of Norsat products. Other distributors of Norsat products include a U.S.-based telecommunications company, which also won a contract issued by the U.S. government in June 2021 for Norsat satellite telecommunication products.

4.2. Critical and Emerging Technologies⁹⁸

In February 2022, the U.S. National Science and Technology Council (NSTC) released an updated list of Critical and Emerging Technologies (CETs), which is a subset of advanced technologies that are potentially significant to U.S. national security.⁹⁹ The initial list of priority CETs was introduced in the National Strategy for Critical and Emerging Technologies published in October 2020.¹⁰⁰ According to the 2021 Interim National Security Strategic Guidance,¹⁰¹ the U.S. government defines three national security objectives: safeguarding the security of the U.S. citizens, expanding economic prosperity and opportunity, and defending democratic values. The CETs in the updated list could help meet those objectives. The updated list of CETs includes (See *Appendix* for details):

- Advanced Computing
- Advanced Engineering Materials
- Advanced Gas Turbine Engine Technologies
- Advanced Manufacturing
- Advanced and Networked Sensing and Signature Management
- Advanced Nuclear Energy Technologies
- Artificial Intelligence
- Autonomous Systems and Robotics
- Biotechnologies
- Communication and Networking Technologies

98. National Science and Technology Council, “Critical and Emerging Technologies List Update,” The White House, February 2022.

99. Ibid.

100. “National Strategy for Critical and Emerging Technologies,” Trump White House Archives, October 2020.

101. “Interim National Security Strategic Guidance,” The White House, March 2021.

- Directed Energy
- Financial Technologies
- Human-Machine Interfaces
- Hypersonics
- Networked Sensors and Sensing
- Quantum Information Technologies
- Renewable Energy Generation and Storage
- Semiconductors and Microelectronics
- Space Technologies and Systems

The February 2022 report on critical and emerging technologies states that this updated list would inform future efforts to prioritize across CETs and their component subfields, but should not be interpreted as a priority list for either policy development or funding.¹⁰²

South Korea maintains its own guidance and regulations for technologies that are significant to the national security of South Korea, many of which overlap with what the U.S. deems as critical. Under the Prevention of Divulgence and Protection of Industrial Technology Act (PITA), South Korean companies that hold technology designated as a National Core Technology (NCT) are required to take appropriate protective measures, including at least the following:¹⁰³

- Setting up mechanisms for protecting NCTs;
- Specifically appointing a person or persons in charge of managing NCTs;
- Reporting to the Minister of Trade, Industry, and Energy (MOTIE) when exporting an NCT or when a foreign inventor is acquiring an NCT that was developed using Korean government funding;
- Obtaining approval from MOTIE when exporting an NCT that was developed using Korean government funding

102. National Science and Technology Council, “Critical and Emerging Technologies List Update,” The White House, February 2022.

103. “Changes to List of National Core Technologies Subject to Export Restrictions in Korea,” Kim & Chang, November 8, 2019.

The latest list of NCTs updated on July 14, 2021, includes 73 technologies in 12 sectors such as semiconductor, display, electrical and electronics, automobile and railway, steel, shipbuilding, nuclear power, information and communication technology, space technology, biotechnology, machinery, and robotics.¹⁰⁴

On August 20, 2019, an amendment to the PITA was promulgated and came into effect on February 21, 2020. The PITA amendment is intended to reflect the South Korean government's "Measures to Eradicate Leakage of Industrial Technologies" announced on January 3, 2019. The new amendment is likely to affect technology companies as the scope of NCTs under PITA has been broadly defined by the South Korean government.¹⁰⁵ In particular, the amended PITA strengthens regulations that apply to domestic companies in possession of NCTs and to foreign companies' acquisition of domestic companies having NCTs. The amendment also includes increased sanctions for infringements such as leakage, misuse, and misappropriation of NCTs. The key points of the PITA amendment are as follows:¹⁰⁶

- Expanded obligations of companies that have or manage NCTs;
- MOTIE's stricter regulation of mergers and acquisitions by foreign companies of domestic companies having NCTs that have been developed with or without R&D funding from the South Korean government;
- Punitive damages for infringement of industrial technologies;
- National Intelligence Service (NIS)'s jurisdiction to investigate industrial technology infringement cases;
- Increased punishment for the leakage of NCTs outside of South Korea;
- Stronger protections for right-holders during judicial proceedings related to industrial technologies

In addition, a new Act on Special Measures for Strengthening and Protecting the

104. MOTIE, "Notification on the Designation of National Core Technologies, etc. (No. 2021-130)."

105. Lee & Ko, "Korea Strengthens Protection of National Core Technology And Industrial Technology (Amendment Of The Prevention of Divulgence And Protection Of Industrial Technology Act)," Legal500, October 2, 2019.

106. "Act on Prevention of Divulgence and Protection of Industrial Technology," Korea Legislation Research Institute, last updated August 20, 2019.

Competitiveness of the National High-Tech Strategic Industry was established on February 3, 2022 and is scheduled to take effect on August 4, 2022. The new Act explicitly states that the reason for the enactment is due to the hegemony dispute between the U.S. and China that is expanding beyond the trade sector to the high-tech sector, causing the technology of high-tech industries to become a key factor in determining the direction of future economic and security hegemony.¹⁰⁷ Apart from the existing NCTs, the National High-Tech Strategic Technologies (NHSTs) will be selected in consideration of the following requirements:¹⁰⁸

- Significant impacts on national and economic security, such as stabilization of the supply chain, and on the national economy, such as export and employment;
- Growing potential, technical difficulty and industrial importance;
- Significant ripple effects on related industries;
- Industrial importance

4.2a. Case Study: Technology Protection Strategy

China has prioritized efforts to acquire the materials, equipment, intellectual property, and knowledge necessary to accelerate the development of its domestic semiconductor industry, and has been accused of using controversial technology transfer practices in pursuit thereof.

In 2021, the U.S. and South Korean regulators stopped the acquisition of Magnachip Semiconductor, a South Korea-based chip manufacturer, by Chinese private equity firm Wise Road Capital. In June 2021, Magnachip was also notified by the South Korean Ministry of Trade, Industry, and Energy requesting Magnachip to apply for an approval for the merger.¹⁰⁹ A month later, Magnachip Semiconductor Corporation

107. "Act on Special Measures for Reinforcement and Protection of National High-tech Strategic Industry Competitiveness," Korean Law Information Center, August 4, 2022.

108. "Korea Announces Comprehensive 'Technology Protection Strategy' for Core Technologies and Infrastructure," Kim & Chang, March 10, 2022.

109. Simon Lester and Huan Zhu, "CFIUS and Korean Government Finishing up Security Review of Chinese Purchase of Korean Semiconductor Company," China Trade Monitor, September 17, 2021.

received a communication from the Committee on Foreign Investment in the United States (CFIUS) asking the firm to pause the deal on grounds of national security concerns.¹¹⁰ The halting of the merger highlights U.S. and South Korean scrutiny of foreign acquisitions of critical national technologies on national security grounds.

According to the Korea Intellectual Property Office (KIPO) and National Intelligence Service (NIS), South Korea has seen 121 cases of technology leaks over the past five years.¹¹¹ The outflow of technology stems from foreign countries poaching retired technology and science professionals.¹¹²

In August 2021, the Hebei Semiconductor Research Institute, also known as the 13th Research Institute of China Electronics Technology Group Corporation, issued a bid for a set of an “automatic lens measurer”¹¹³ made by a South Korean packaging solution provider for the electronics manufacturing industry.¹¹⁴ Hebei Semiconductor Research Institute, the buyer of the South Korean product, was added to the U.S. BIS Entity List in August 2018 for being “involved in the illicit procurement of commodities and technology for unauthorized military end use in China.”¹¹⁵ The bid was won by Schain Group China Limited, the Hong Kong office of Shanghai Schain Electronic Technology Co., Ltd, a reseller of equipment used in the semiconductor industry.¹¹⁶

In April 2021, Shanghai Schain Electronic Technology won a bid to acquire a micro-assembled AOI system on behalf of Shanghai Aerospace Electronic and Communication Equipment Research Institute, which belongs to the 8th Research

110. Magnachip Semiconductor Corporation, Form 8-K, U.S. Securities and Exchange Commission, August 27, 2021.

111. Kotaro Hosokawa, “South Korea to track travel by chip engineers as tech leaks grow,” Nikkei Asia, February 5, 2022.

112. Bang-Hyun Kim, “New programs aim to keep retired tech professionals from being poached,” Korea JoongAng Daily, January 23, 2022.

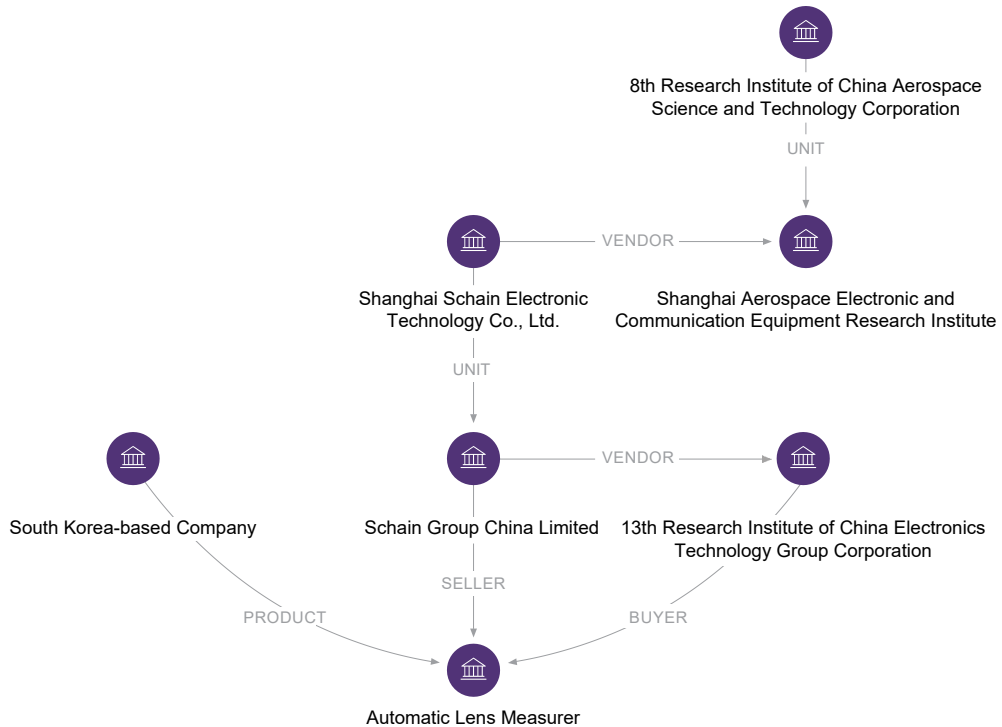
113. Chinese records, documents held by the author.

114. Korean records, documents held by the author.

115. U.S. Department of Commerce Bureau of Industry and Security, “Addition of Certain Entities; and Modification of Entry on the Entity List,” Federal Register, August 1, 2018.

116. Shanghai Schain Electronic Technology Co., Ltd., <http://schain.cn/contact.asp>.

Institute of China Aerospace Science and Technology Corporation (CASC). The 8th Academy of CASC was added to the U.S. BIS Entity List in May 1999.



4.3. Uyghur Force Labor Prevention Act

On December 23, 2021, President Biden signed the Uyghur Forced Labor Prevention Act, which calls for a strengthened enforcement strategy to prohibit the import of goods made through forced labor from the Xinjiang Uyghur Autonomous Region (XUAR) in China.¹¹⁷ The U.S. Customs and Border Protection (CBP) is responsible for restricting imports from Xinjiang into the U.S., unless an importer can demonstrate that it is in full compliance with the Forced Labor Enforcement Task Force’s (FLETF) guidance and corresponding regulations; completely and substantively responds to all

117. “The Signing of the Uyghur Forced Labor Prevention Act,” U.S. Department of State, December 23, 2021.

of CBP's inquiries regarding the imported items; and establishes clear and convincing evidence that goods were not mined, produced, or manufactured wholly or in part from forced labor.¹¹⁸

The CBP issues Withhold Release Orders on goods suspected to be produced with forced labor in Xinjiang, which include all cotton, cotton products, tomatoes, and tomato products, as well as certain garments, hair products, apparel, computer parts, and other goods.¹¹⁹

The Act also calls for a report identifying foreign persons, including Chinese government officials, that the U.S. president determines are “responsible for serious human rights abuses in connection with forced labor with respect to Uyghurs, Kazakhs, Kyrgyz, or members of other persecuted groups, or other persons in the Xinjiang Uyghur Autonomous Region.”¹²⁰

4.3a. Case Study: Xinjiang Supply Chain

The fashion and electronics industries must exercise proper due diligence to ensure that raw materials are not sourced from companies in Xinjiang engaged in activities that suggest the presence of forced labor.

In June 2020, Aksu Huafu Textiles Co. was added to the BIS Entity List for engaging in human rights violations and abuses in Xinjiang.¹²¹ Aksu Huafu Textiles is located in the Aksu Textiles Industry City, an industrial park that hosts the Xinjiang Aksu Women's Prison and the Aksu Textile and Apparel Industry Training Center, which states that it uses a “transformational” vocational training model that includes elements

118. Department of Homeland Security, “Notice Seeking Public Comments on Methods to Prevent the Importation of Goods Mined, Produced, or Manufactured with Forced Labor in the People's Republic of China, especially in the Xinjiang Uyghur Autonomous Region, Into the United States,” Federal Register, January 24, 2022.

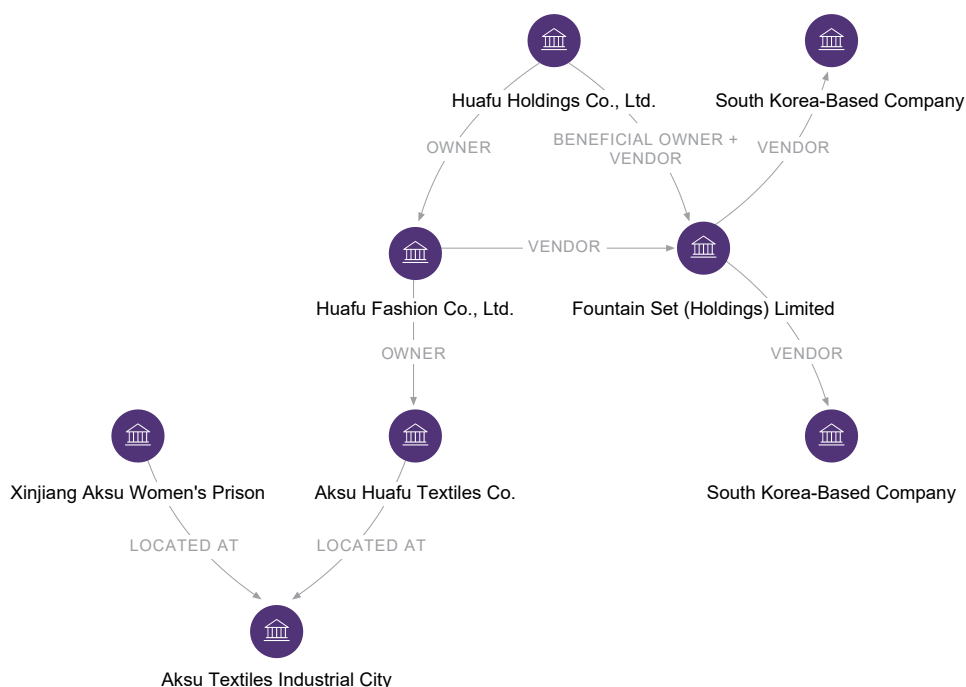
119. “S.65 - Uyghur Forced Labor Prevention Act,” U.S. Congress, July 14, 2021.

120. Ibid.

121. U.S. Department of Commerce Bureau of Industry and Security, “Addition of Certain Entities to the Entity List; Revision of Existing Entries on the Entity List,” Federal Register, June 5, 2020.

of Mandarin language education and skills development to improve the trainees' "character," according to a local government statement.¹²²

Aksu Huafu Textiles' parent companies supply various cotton yarn products to its sister company in China, Fountain Set (Holdings) Limited, for the manufacture of textile products. A South Korean major shoe brand and a fashion and South Korean-based retail conglomerate are clients of Fountain Set (Holdings) Limited, according to its 2021 investor presentation.



Media reports in March 2021 note that the Chinese unit of the major shoe brand confirmed its support for Xinjiang cotton, writing on its Weibo account that it "has always purchased and used cotton produced in China including that from the Xinjiang region."¹²³

122. "Aksu: The innovation mechanism of the textile industry city expands the scale of absorption and employment," The United Front Work Department of the Xinjiang Uygur Autonomous Region Committee of the Communist Party of China, December 23, 2016.

In July 2021, the U.S. published an advisory on Xinjiang forced labor that includes warning signs for potential supply chain exposure to entities suspected of human rights abuses. In a January 2022 event hosted by the U.S. think tank Center for Strategic & International Studies, South Korean Trade Minister Yeo Han-Koo noted that South Korea considers the Xinjiang forced labor issue in the supply chain as “very important.” Trade Minister Yeo stated that South Korea has the intention to prevent forced labor from being incorporated into the supply chain, but the challenge lies in implementation due to the lack of a system that can track forced labor with the various tiers of the supply chain. A South Korean news outlet reported in the same month that President Yoon stated that South Korea should cooperate with the international community’s efforts on the issue of China’s suppression of human rights in Xinjiang.¹²⁴

123. Yim, Hyun-su, “Fila stays silent after Chinese unit vows to continue using Xinjiang cotton,” *The Korea Herald*, March 30, 2021.

124. Beomsu Yang, “Yun Seok-yeol, “We must also participate in international cooperation” in China’s crackdown on human rights in Xinjiang,” *Chosun Biz*, January 24, 2022.

5. Strengthening Risk Management Procedures and Processes

This report demonstrates the importance of conducting due diligence reviews for business ties and transactions involving foreign entities from jurisdictions that are subject to sanctions and trade restrictions. An effective risk management program can help companies avoid penalties and reputational damage, and ensure adherence to industry regulations and best practices. Ensuring proper due diligence can be challenging. The following section discusses crucial elements of an effective sanctions and export control compliance program.

5.1. Strengthening Sanctions Compliance

In April 2020, the Industrial Bank of Korea (IBK) reached settlements with U.S. prosecutors and New York State banking regulators, agreeing to pay USD 86 million to resolve investigations into its anti-money-laundering (AML) compliance program.

According to the U.S. Department of Justice press release, deficiencies in AML compliance, including a lack of staffing and resources at the New York branch, lead the bank to process more than USD 1 billion in transactions that violated U.S. sanctions. The New York branch handled USD 10 million in U.S.-dollar payments from South Korean entities to Iran, according to federal prosecutors. The vast majority of the transactions had cleared through New York financial institutions, including IBK's local branch and at least one other state-regulated bank.¹²⁵

In addition to paying the penalties, IBK strengthened its compliance function. It created two bodies to provide AML and sanctions compliance oversight. The New York branch hired a new compliance officer, who reports directly to the head office's chief compliance officer, as well as a deputy and nine additional staffers. IBK also implemented a new

125. Samuel Rubinfeld, "Industrial Bank of Korea Agrees to Pay \$86 Million to Settle Money Laundering Probes," *The Kharon Brief*, April 21, 2020.

compliance testing program, developed methodologies for reporting, tracking and assessing compliance issues, and reworked its transaction monitoring processes and systems, the federal settlement said.

The action highlights the importance of building and supporting an efficient and effective compliance program, which includes providing adequate resources, staff, and training to the AML compliance function. Customer due diligence policies, procedures, and internal controls are considered to be the cornerstone of a strong compliance program by regulators and enforcement agencies, including OFAC.¹²⁶

In May 2019, OFAC published “A Framework for OFAC Compliance Commitments”,¹²⁷ which outlines essential components of an effective sanctions compliance program. The guidance applies to the U.S. entities, as well as foreign companies or individuals that conduct business in the U.S. or involve U.S. persons or goods.

OFAC’s five essential components of an effective compliance program include:

1. Management Commitment
2. Risk Assessment
3. Internal Controls
4. Testing and Auditing
5. Training

The guidelines acknowledge that while there is no “one-size-fits-all” risk assessment, the exercise should generally consist of a “holistic review of the organization from top-to-bottom and assess its touch-points to the outside world.” According to OFAC’s framework, one of the fundamental components of an effective risk assessment and sanctions compliance program is conducting due diligence on an organization’s customers, supply chain, intermediaries, and counterparties, while taking into consideration factors such as ownership and geographic locations. OFAC lists “improper due diligence on customers/clients” as one of the root causes of compliance breakdowns based on an

126. Morrison & Foerster LLP, “Lessons Learned From OFAC’s 2021 Enforcement Actions So Far,” JD Supra, July 15, 2021.

127. “Office of Foreign Assets Control - Sanctions Programs and Information,” U.S. Department of the Treasury.

assessment of past OFAC enforcement actions.

5.2. Strengthening Export Controls

Following Russia's invasion of Ukraine in February 2022, South Korea announced it would tighten export controls against Russia by banning shipments of strategic items.¹²⁸ The strategic items include electronics, semiconductors, computers, information and communications, sensors and lasers, navigation and avionics, and marine and aerospace equipment.

In response to South Korea's implementation of such export control policies, the U.S. Department of Commerce BIS added South Korea to the nation list of exemption from the U.S. application of the Foreign Direct Product Rule (FDPR) in trade with Russia. According to the FDPR, even if the item is produced outside the U.S., it is regarded as U.S. products if the items are backed by U.S. technology-integrated parts. In effect, South Korea received an exemption from U.S. export restrictions requiring a license for some tech-related exports to Russia.

In January 2017, BIS published Export Compliance Guidelines: The Elements of an Effective Export Compliance Program, which outlines critical elements of an effective export compliance program.¹²⁹ The guidance is meant to assist organizations operate their export activities in accordance with the EAR, and is relevant to South Korean companies in light of the BIS de minimis rule and more recently, South Korea's coordination with the U.S. on export controls for Russia.¹³⁰

BIS identifies eight essential components as critical for an effective compliance program:

128. Shin and Kim, "South Korea bans exports of strategic items to Russia, joins SWIFT sanctions," Reuters, February 28, 2022.

129. "Export Compliance Guidelines: The Elements of an Effective Export Compliance Program," U.S. Department of Commerce Bureau of Industry and Security, January 2017.

130. "Joint Statement on the Republic of Korea's Partnership on Export Controls for Russia," U.S. Department of Commerce, March 7, 2022.

1. Management Commitment
2. Risk Assessment
3. Export Authorization
4. Recordkeeping
5. Training
6. Audits
7. Handling export violations and taking corrective actions
8. Build and maintain your Export Compliance Program (ECP)

The guidance highlights that the above elements provide the basic structure for an effective export compliance program, but they do not necessarily constitute an exhaustive list. Organizations should tailor their compliance program to reflect their unique export operations and reexport activities.¹³¹ According to BIS, developing an effective compliance program is essential not only for preventing export violations, but also for enabling BIS to differentiate violations by individual employees from larger patterns of corporate noncompliance.¹³²

131. “Export Compliance Guidelines: The Elements of an Effective Export Compliance Program,” U.S. Department of Commerce Bureau of Industry and Security.

132. “Don’t Let This Happen to You,” U.S. Department of Commerce Bureau of Industry and Security, September 2020.

6. Conclusion: Policy Recommendations¹³³

This report outlines important changes in key regulations regarding sanctions compliance and trade controls as well as supply chain security that are crucial for South Korean entities, which can potentially be targets of U.S. regulators and law enforcement. South Korean government and businesses must continue to recognize the significance of these changes and conduct a due diligence review of their business ties and transactions with foreign entities from high-risk jurisdictions, including China and Russia, as the U.S. and other western countries continue their strategy towards tighter regulatory control. History suggests that South Korea's bilateral status with the United States will not provide cover for its legal obligation.

From a policy standpoint, South Korea needs to recognize the benefit of taking proactive measures to harmonize its trade and investment regulation with the United States and its regional allies. Countries like Australia, Canada, Japan, and New Zealand, for instance, have all moved to bring their trade and foreign investment review regimes in line with regulations in the United States.¹³⁴ The long-term prospects and implications of these changes for local businesses, along with national security concerns for all of these countries, seem to have weighed in on their decision. Granted, elites in Seoul often cite South Korea's overall trade dependence with countries like China to explain their reservations about similar policy matters.¹³⁵ In 2021, South Korea's export to China accounted for USD 162.9 billion (25.3% of total South Korean exports) compared to export to the United States (96.3 billion, 14.9%) and Japan (30.1 billion, 4.7%),

133. The recommendations expressed in this chapter are solely those of the experts from the Asan Institute for Policy Studies, and do not reflect Kharon's institutional perspective.

134. This is what allows many of these countries to receive the "excepted foreign states" status by the US Treasury. See "CFIUS Goes Global: New FDI Review Process Proliferate, Old Ones Expand," Skadden's 2022 Insight, January 19, 2022; "Australia and Canada Remain CFIUS Excepted Foreign States; United Kingdom and New Zealand Have Until February 2023 to Fulfill Criteria Necessary to Keep Designations," Clearly Foreign Investment and International Trade Watch, January 10, 2022.

135. Chung Min Lee, "South Korea is Caught between China and the United States," Carnegie Endowment for International Peace, October 21, 2020.

which together stood at USD 126.4 billion (19.6%).¹³⁶ History of Chinese coercion against Korean businesses gives the South Korean government another reason to tread carefully when it comes to above-mentioned regulatory controls.¹³⁷

Bilateral Trade (in billion USD)¹³⁸

Trade Partners	Australia (2020)	Canada (2021)	Japan (2020)	New Zealand (2020)
China	115.7 (33.5%)	23 (4.6%)	163.6 (21.6%)	10.8 (29%)
United States	12.1 (3.5%)	380.4 (75.6%)	135.7 (18%)	3.8 (10.3%)
Taiwan	9.1 (2.6%)	1.32 (0.3%)	54.4 (7.2%)	0.84 (2.2%)
South Korea	21.8 (6.3%)	4.5 (0.9%)	52.5 (6.9%)	1.1 (3%)
Hong Kong	7.2 (2.1%)	2.8 (0.6%)	35.4 (4.7%)	0.747 (2%)

An argument can be made, however, that the risks associated with doing business in China are why South Korea should be more forthcoming about participating in these regimes:

1. Other countries cooperating with the United States to bring their regulations in line with the U.S. are equally (if not more) dependent on their trade with China.
2. The recent example in Ukraine suggests that national security concerns will override any trade or investment concerns if tensions between the U.S. and China deepens.
3. There is a fundamental gap in core values between Seoul and Beijing that cannot be bridged without significant changes within China.

136. Daniel Workman, "South Korea's Top Trading Partners," World's Top Exports, March 2022.

137. Darren Lim, "Chinese Economic Coercion during the THAAD Dispute," The Asan Forum, December 28, 2019.

138. Daniel Workman, "South Korea's Top Trading Partners," <https://www.worldstopexports.com/south-koreas-top-import-partners>.

Policymakers in Seoul must ask whether they see the broader context of great power competition gaining more momentum and which side South Korea will take. Seoul must recognize that delaying this decision will only raise the future cost of this move; hence, it would be wise to act now to map out a prudent path.

Appendix: U.S. Critical and Emerging Technology Subfields

Advanced Computing

- Supercomputing
- Edge computing
- Cloud computing
- Data storage
- Computing architectures
- Data processing and analysis techniques

Advanced Engineering Materials

- Materials by design and material genomics
- Materials with new properties
- Materials with substantial improvements to existing properties
- Material property characterization and lifecycle assessment

Advanced Gas Turbine Engine Technologies

- Aerospace, maritime, and industrial development and production technologies
- Full-authority digital engine control, hot-section manufacturing, and associated technologies

Advanced Manufacturing

- Additive manufacturing
- Clean, sustainable manufacturing
- Smart manufacturing
- Nanomanufacturing

Advanced and Networked Sensing and Signature Management

- Payloads, sensors, and instruments
- Sensor processing and data fusion
- Adaptive optics
- Remote sensing of the Earth

- Signature management
- Nuclear materials detection and characterization
- Chemical weapons detection and characterization
- Biological weapons detection and characterization
- Emerging pathogens detection and characterization
- Transportation-sector sensing
- Security-sector sensing
- Health-sector sensing
- Energy-sector sensing
- Building-sector sensing
- Environmental-sector sensing

Advanced Nuclear Energy Technologies

- Nuclear energy systems
- Fusion energy
- Space nuclear power and propulsion systems

Artificial Intelligence (AI)

- Machine learning
- Deep learning
- Reinforcement learning
- Sensory perception and recognition
- Next-generation AI
- Planning, reasoning, and decision making
- Safe and/or secure AI

Autonomous Systems and Robotics

- Surfaces
- Air
- Maritime
- Space

Biotechnologies

- Nucleic acid and protein synthesis
- Genome and protein engineering including design tools

- Multi-omics and other biometrology, bioinformatics, predictive modeling, and analytical tools for functional phenotypes
- Engineering of multicellular systems
- Engineering of viral and viral delivery systems
- Biomanufacturing and bioprocessing technologies

Communication and Networking Technologies

- Radio-frequency (RF) and mixed-signal circuits, antennas, filters, and components
- Spectrum management technologies
- Next-generation wireless networks, including 5G and 6G
- Optical links and fiber technologies
- Terrestrial/undersea cables
- Satellite-based communications
- Hardware, firmware, and software
- Communications and network security
- Mesh networks/infrastructure independent communication technologies

Directed Energy

- Lasers
- High-power microwaves
- Particle beams

Financial Technologies

- Distributed ledger technologies
- Digital assets
- Digital payment technologies
- Digital identity infrastructure

Human-Machine Interfaces

- Augmented reality
- Virtual reality
- Brain-computer interfaces
- Human-machine teaming

Hypersonics

- Propulsion
- Aerodynamics and control
- Materials
- Detection, tracking, and characterization
- Defense

Quantum Information Technologies

- Quantum computing
- Materials, isotopes, and fabrication techniques for quantum devices
- Post-quantum cryptography
- Quantum sensing
- Quantum networking

Renewable Energy Generation and Storage

- Renewable generation
- Renewable and sustainable fuels
- Energy storage
- Electric and hybrid engines
- Batteries
- Grid integration technologies
- Energy-efficiency technologies

Semiconductors and Microelectronics

- Design and electronic design automation tools
- Manufacturing process technologies and manufacturing equipment
- Beyond complementary metal-oxide-semiconductor (CMOS) technology
- Heterogeneous integration and advanced packaging
- Specialized/tailored hardware components for artificial intelligence, natural and hostile radiation environments, RF and optical components, high-power devices, and other critical applications
- Novel materials for advanced microelectronics
- Wide-bandgap and ultra-wide-bandgap technologies for power management, distribution, and transmission

Space Technologies and Systems

- On-orbit servicing, assembly, and manufacturing
- Commoditized satellite buses
- Low-cost launch vehicles
- Sensors for local and wide-field imaging
- Space propulsion
- Resilient positioning, navigation, and timing (PNT)
- Cryogenic fluid management
- Entry, descent, and landing

South Korea and the Global Regulatory Landscape

Managing Risks Associated with Sanctions,
Trade Controls, and Supply Chains

Priscilla KIM, Edmund XU, J. James KIM, Hyeonjung CHOI

First edition August 2022

Published by The Asan Institute for Policy Studies

Registration number 300-2010-122

Registration date September 27, 2010

Address 11, Gyeonghuigung 1ga-gil, Jongno-gu, Seoul 03176, Korea

Telephone +82-2-730-5842

Fax +82-2-730-5876

Website www.asaninst.org

E-mail info@asaninst.org

Book design EGISHOLDINGS

ISBN 979-11-5570-250-5 93340

Copyright © 2022 by The Asan Institute for Policy Studies & Kharon

All Rights reserved, including the rights of reproduction in whole or in part in any form.

Printed in the Republic of Korea



KHARON



ISBN 979-11-5570-250-5