Maintaining the Technology Edge: Strengthening US and Indo-Pacific Alliances to Counter Chinese Technology Acquisition

By Dr. Satu Limaye and Rose Tenyotkin

Amid the COVID-19 pandemic, global restrictions on foreign direct investments hit a global high in 2020, with countries across Europe, the Indo-Pacific region and the United States enacting greater restrictions on investments in strategic technologies. The pandemic exacerbated concerns of reliable and trustworthy supply chains. The US government is increasingly concerned about China’s attempts to acquire advanced technology from abroad, through illicit and legal activities such as foreign direct investment (FDI), joint ventures and intellectual property (IP) theft. In the Indo-Pacific, key US treaty allies with advanced technology of their own, including Japan, Australia and South Korea, are also grappling with China’s attempts to acquire emerging and advanced technology within their own countries. Similar to the US, these allies are taking measures to balance the benefits of economic cooperation with China while seeking to protect national security industries and interests. Finding the right balance is crucial to maintaining a robust alliance with Washington.

The US cannot continue to address the issue of countering Chinese advanced technology acquisition alone; it needs the assistance of and close policy coordination with Australia, Japan and South Korea. China’s technology acquisition strategies extend to these advanced technology countries, which are key US regional allies. Moreover, US allies have their own specific business interests with China, while simultaneously sharing Washington’s concerns about China’s technology acquisition strategy. As US treaty allies, cooperation among these three countries entails the sharing of data and very sensitive advanced technologies with national security and military applications. Much of this sharing involves civil and military technology research and development, co-production, co-development and joint ventures and partnerships. As such, the US should focus its defense and advanced dual-use technology policy objectives through increased close and continuous consultation and cooperation with its partners and allies in the region. By doing so, such efforts could reduce the potential for critical information and technology leakage and unauthorized transfer of critical technologies to China. This applies to dual-use technologies that can enable Chinese military programs that could ultimately degrade US and allied military advantage in the Indo-Pacific and beyond. A comparison of these three countries, all of which are at different stages in addressing this issue, can help provide insight on where each country is in the process and how multilateral initiatives can be most effective.

Japan

Japan appears to have taken the most proactive measures in the Indo-Pacific region to prevent Chinese acquisition of dual-use and military technologies. In January 2020, Japan’s Ministry of Economy, Trade, and Industry (METI) published a report that highlighted critical technologies of concern and enumerated the sophisticated ways in which “countries of concern” seek to acquire those technologies. Originally designed to promote Japan industries and export commodities internationally, METI focuses on preventing the diversion, exploitation or military-associated end-use of Japanese advanced technologies that could prove detrimental to Japan’s foreign policy priority of a free and open Indo-Pacific.
To prevent the loss of critical technologies, Japan has implemented a variety of policies, ranging from stricter export controls to increased scrutiny of foreign investment. Additionally, Japan’s export control systems are continuously evolving. For example, on April 26, 2019, METI issued several export control reforms, including an expansion of the “end user list” to include 534 additional entities, many of which are Chinese entities with clear defense ties. At the same time, METI also enhanced its controls over items relating to weapons of mass destruction (WMD) by “oblig[ing] exporters to submit an application for an export license for goods that may be used for the development of WMDs, even if they are not subject to export restrictions under international agreements.”

In December 2019, the Japanese Diet revised the Foreign Exchange and Foreign Trade Act, which regulates FDI, to require foreign investors to notify authorities when acquiring stakes of 1 percent or more in an entity that is deemed related to national security. The previous threshold to trigger a review of the investment was 10 percent. This revision, which came into force in June 2020, illustrates how Japan is attempting to balance national security and economic growth. These efforts are similar to recent measures taken by the US in the Export Control Reform Act of 2018 as well as the Foreign Investment Risk Review Mitigation Act of 2018. The latter bolstered the authorities of the Committee on Foreign Investment in the US. Japan continues to have a number of overall security challenges, namely in industrial security. However, these recent policy actions suggest that Japan is taking the initiative in responding to China’s burgeoning technology acquisition strategy with national security implications. This reflects not only Japan’s alignment with US concerns, but its own threat perceptions vis-à-vis its defense and national security policy. Japan’s measures have been nuanced in tone (e.g., not specifically calling out China) and framed as legal and regulatory “upgrading and fine-tuning,” rather than reactions to Chinese assertive economic statecraft or military-civilian fusion objectives.

Australia

In its recent policy shift, the Australian government has been much more vocal and active against Chinese attempts to acquire technology within Australia. This shift comes amid broader Australian pushback against Chinese economic coercion. On April 27, 2020, Australian Foreign Minister Marise Payne warned China against threats of “economic coercion” as a response to Australia’s call for an international investigation into the COVID-19 pandemic.

Some recent measures against Chinese influence operations illustrate Australia’s shifting posture on these issues. Because of domestic political scandals and the growing influence of the United Front Work Department (the Chinese Communist Party organ responsible for coordinating influence operations both at home and abroad), Australia has also begun to overhaul its espionage laws to prohibit foreign government influence in Australian politics. The Australian Strategic Policy Institute also thoroughly tracks and documents the People’s Liberation Army involvement in research collaboration with Australian universities.

The Australian government recently increased oversight of foreign investments in critical infrastructure. The Security of Critical Infrastructure Act 2018 and The Telecommunications and Other Legislation Amendment Act of 2017 enable Australia’s Critical Infrastructure Centre to gather information on owners and operators of critical infrastructure in the sensitive sectors of electricity, water, ports, gas and carrier services. These steps toward greater oversight appear to be in response to accumulation of malfeasance over multiple years.
Moreover, Australia has recently blocked a number of China-based companies from investing in Australian infrastructure projects. For example, in 2018, the Australian government blocked Hong Kong-based Cheung Kong Infrastructure’s (CKI) 13 billion AUD takeover of Australian gas pipeline company APA Group, Australia’s largest gas transmission company. The takeover was blocked on national security grounds at the recommendation of the Foreign Investment Review Board and Critical Infrastructure Centre.

On 5 June, in response to the COVID-19 crisis, Dr. Steven Kennedy, the Secretary of the Australian Treasury, announced reforms to Australia’s foreign investment review system. According to the announcement, “the reform package includes measures to strengthen the existing framework with: enhanced national security review of sensitive acquisitions; extra powers and resources to ensure foreign investors comply with the terms of their approval.” Earlier, in March, the Australian government announced it would review all proposed foreign investment in order to protect Australian interests in a time of economic insecurity caused by the global pandemic. These temporary measures are slated to last for up to six months.

Despite these measures, China remains Australia’s largest trading partner, accounting for almost 35 percent of Australia’s exports mostly natural resource commodities. Australia’s dependence on China for its service exports, such as education and tourism, is also massive. Thus, Australia continues to balance its need for a favorable commercial relationship with China with its national security concerns about protecting advanced technology.

The Republic of Korea (ROK)

Within South Korea, there appears to be a growing sense of economic and political vulnerability to China. In 2016, China implemented heavy coercive economic measures in response to the US and South Korea’s decision to deploy a US Terminal High Altitude Area Defense (THAAD) antimissile battery in South Korea. China’s economic coercion pressured South Korea to abandon the THAAD deployment. Additionally, as China’s economy continues to expand and modernize, there is heightened concern among South Korea policy circles that China is emerging as an economic competitor in key sectors, especially electronics, where South Korea has long been a world leader. As South Korean investment professionals noted, “our biggest customer [China] has become our competitor. The only thing holding up right now is semiconductors.” In part as a result of these growing concerns, the ROK government has established robust FDI laws to counter technology leakage and has cracked down on Chinese IP theft.

South Korea has a robust legal code designed to prevent attempts at technology acquisition. For instance, multiple sectors of its economy remain completely closed to FDI, including nuclear energy and TV/radio broadcasting. The government also places limitations of the amount of foreign ownership of firms in specific sectors, such as water, thermal energy, newspaper publication, and telecommunication services, which range from 25 percent to 49 percent. Moreover, any foreigner seeking to invest in a defense industry company in the ROK must obtain approval from the Minister of Trade, Industry and Energy. Each one of these measures stymies the leakage or illicit or unauthorized transfer of sensitive technologies.

The South Korean government is also cracking down on IP theft, another vector through which foreign countries can obtain sensitive technologies. In 2018, for example, Samsung was the target of espionage by Chinese chip manufacturers. One official involved in the case stated the following:
Samsung Electronics and SK Hynix have become the target of industrial espionage by Chinese memory chip manufacturers. In semiconductors, patents are critical to the cost structure. The companies have to protect what they have spent decades building. The result is Chinese companies are attempting to infringe on Samsung and SK patents.24

Samsung is also pursuing another case, begun in 2018, in which a Chinese company illegally procured propriety Samsung equipment from a Samsung supplier. The South Korean government charged nine individuals and two companies with illegally transferring flexible 3D screen lamination blueprints to a Chinese entity.25

Despite well-publicized cases of Chinese IP theft prosecution and increased scrutiny by the ROK government over potential foreign investment in Korean technology firms, Seoul has been relatively muted in its public response to Chinese attempts to acquire Korean technology. While concerns about Chinese activities have grown, China remains South Korea’s largest trading partner and a key intermediary for dealings with North Korea. In 2019, China accounted for 25 percent, or $136 billion, of South Korea’s exports, more than South Korean exports to the US and Japan combined.26 Given this situation, South Korea, which often refers to itself as a “shrimp among whales,” will continue to seek out ways to protect its own national interests while trying to maintain commercial relations with Chinese firms for the benefit of its economy.

The Multilateral Way Forward

Australia, Japan and the ROK have all sought to maintain a careful balance of trade and national security by cooperating with China on economic issues in order to further economic growth, while also addressing national security concerns of advanced technology loss. However, as China’s efforts to acquire foreign advanced technology have expanded, this balance has become increasingly difficult to maintain. With China seeking leverage its economic advantage by undercutting and playing allies against each other, all three countries have taken specific, calculated and focused measures to address the national security implications of China’s acquisition of foreign technology.

Japan, ROK and Australia each have adopted policies aimed at preventing China’s technology acquisition strategies, which include investment restrictions, greater scrutiny of export control lists, and preventing the exploitation of human capital. Impressively, Australia’s and Japan’s increased scrutiny on foreign investment in critical technologies parallels the requirements set forth by the US Committee on Foreign Investments (CFIUS). While these allies may not frame their measures as “great power competition” or “military-civil fusion,” these countries’ fears about China’s economic statecraft are increasingly aligning with US concerns—even if they do not express them in the same terms or as prominently.

Japan, Australia and South Korea, in addition to being Organisation for Economic Co-operation and Development (OECD) members and advanced technology economies with world-class scientific and technical bases, are also members of key multilateral export control regimes that prohibit the trade of sensitive technologies—The Australia Group, Missile Technology Control Regime, Nuclear Suppliers Group, and the Wassenaar Arrangement. Incidentally, China is only party to one of these regimes, the Nuclear Supplies Group. All three countries align their domestic regulations and laws with the requirements of these regimes. The US should take advantage of its own leadership in these regimes to push for greater technology security policy harmony and alignment.
If the US seeks to maintain its technological advantage—and the advantages of its allies—it must engage in sustained, close coordination in an advanced technological alliance framework to create common objectives for advanced defense and dual-use technology. The US, by cooperating closely with allies, can not only stop the leakage of national security technologies to China, but further strengthen and network its alliances in the Indo-Pacific region.

Dr. Satu Limaye is Vice President of the East-West Center. He is also a Senior Advisor at CNA.

Rose Tenyotkin is an Associate Research Analyst at the CNA. Her areas of expertise include Chinese economic statecraft, sanctions and export controls, and China’s nuclear weapons program.

The views expressed in this article are those of the authors and do not reflect the official policy or position of CNA or the US Navy.

3 An end-user is the entity who will ultimately use the purchased item. For more, see: “15 CFR § 772.1 - Definitions of terms as used in the Export Administration Regulations (EAR),” Legal Information Institute, January 19, 2020, https://www.law.cornell.edu/cfr/text/15/772.1.
4 Ibid.
7 Ibid.
8 Ibid.
12 Ibid.
14 Ibid.
20 Ibid.
22 Ibid.