



INTERSECTIONS

Technology, National Security, and US-China Strategic Competition

Intersections is a news digest that describes the interplay between the People’s Republic of China’s (PRC’s) technology acquisition efforts and US and partner nation responses.¹ This issue covers technology and economic policy developments in China, the US, and US ally and partner nations including new PRC export restrictions, US semiconductor production incentives, European Union (EU) concerns about PRC green energy subsidies, and US ally and partner efforts to screen foreign investments and protect critical technology. We also cover several recent developments in the Australia, United Kingdom (UK), and United States (AUKUS) partnership, a recent UK-hosted global summit on artificial intelligence (AI), and concerns about PRC hacking of US citizens’ data. Click [here](#) to read *Intersections* in your [browser](#).

THIS ISSUE’S CONTENTS

- PRC Regulatory and Policy Measures2
- US Regulatory Actions2
- Recent US Ally and Partner Developments3
 - AUKUS Developments.....3
 - Other US Ally and Partner Developments..... 4
- Advances in Critical and Emerging Tech6
- Illegal Activities7
- China’s National Security Laws7

PRC REGULATORY AND POLICY MEASURES

China bans export of certain rare earth processing technologies. In December 2023, the PRC Ministry of Commerce and the Ministry of Science and Technology jointly issued an update to the Catalog of Technologies Prohibited or Restricted from Export, a list of key technologies that is one of the PRC government's primary means of imposing export controls.² In a change from the previous version issued in 2020, the December 2023 catalog lists as export-prohibited "rare earth refining, processing, and utilization" technology and, specifically, "rare earth calcium oxyborate preparation" technology.³

The PRC's decision to control the export of [rare earth calcium oxyborate](#) preparation technology could have implications for the US military. This is because rare earth calcium oxyborate materials exhibit unique piezoelectrical properties⁴—the term "[piezoelectric](#)" refers to materials that react to heat, motion, or pressure by generating an electric charge that a computer can then process, making these materials widely used in sensors.⁵ Rare earth calcium oxyborate is potentially a very useful material for aerospace sensors because, unlike many other piezoelectric materials, it retains its piezoelectrical properties when subjected to extreme heat.⁶ Thus, the PRC's decision to prohibit the export of preparation technology for this unique rare earth material is an example of how the PRC's dominant global market share (85 percent) of rare earth processing,⁷ combined with Beijing's willingness to restrict exports of processed rare earth compounds, could deprive the US military of inputs to manufacture key defense technologies.

PRC welcomes US-based Micron Technologies in China despite May 2023 ban. In November 2023, months after the PRC [banned](#) Micron chips from being used in domestic "critical information infrastructure,"⁸ PRC Commerce Minister Wang Wentao told Micron CEO Sanjay Mehrotra that he "welcomed" Micron to "continue to take root" in the PRC market, as long as the US semiconductor chip manufacturer "respects PRC laws and statutes."⁹ The PRC's partial ban on Micron chips, which was allegedly because of cybersecurity concerns but may have been meant to [retaliate](#) against US chip export restrictions,¹⁰ is exacting a noticeable cost on Micron, which has estimated that its revenue could decrease by a [low-double-digit percentage](#) as a result of the ban.¹¹ However, despite the ban, Micron has deepened its engagement in the PRC market. For example, in June 2023, Micron announced that it would invest over [\\$600 million](#) to expand chip manufacturing and packaging at its plant in Xi'an.¹² This dynamic can be understood as an example of how the PRC leverages access to its domestic market in order to [bargain](#) with foreign companies in pursuit of its economic and technological goals.¹³

US REGULATORY ACTIONS

US Department of Commerce to review US reliance on PRC "legacy" chips as part of the effort to boost US domestic chip industry. According to a Reuters [report](#), in December 2023, the US Commerce Department announced that it would "launch a survey of the US semiconductor supply chain and defense industrial base to address national security concerns from Chinese-sourced chips."¹⁴ This survey effort follows a [report](#) published by Commerce that same month that identified numerous challenges facing the US semiconductor industry, including a lack of domestic chip fabrication and assembly capacity, concerns about an adequate supply of materials, skilled labor shortages, and reliance on China as an export market.¹⁵

The survey aims particularly to assess US companies' reliance on the PRC for "legacy" chips, or older-generation chips that are essential for certain uses because of their compatibility with specific equipment,

such as certain military hardware. Commerce plans to use the survey's results to guide awards of some \$39 billion in grants to promote chip manufacturing by the US and close allies, including of defense and dual-use legacy chips, under the [CHIPS and Science Act of 2022](#).¹⁶ For example, also in December, the Biden administration awarded the first CHIPS Act grant to [BAE Systems](#), a UK-based defense contractor whose US subsidiary is a major supplier of "chips used in electronic warfare and aircraft-to-aircraft communications."¹⁷

The survey and awarding of CHIPS and Science Act grants are examples of the newly invigorated US approach to industrial policy in support of US national security. Another example is the US Department of Defense's release in January 2024 of its first-ever [National Defense Industrial Strategy \(NDIS\)](#),¹⁸ which aims to "catalyze generational change... to a more robust, resilient, and dynamic modernized defense industrial ecosystem."¹⁹ CNA will continue to track developments related to the NDIS in future issues.

RECENT US ALLY AND PARTNER DEVELOPMENTS

AUKUS DEVELOPMENTS

The AUKUS [partnership](#), announced in September 2021, continues to make progress. It is meant to deepen security cooperation among Australia, the United Kingdom and the United States by integrating defense technological, scientific, and industrial bases and supply chains.²⁰ This section covers a meeting of AUKUS heads of defense to discuss trilateral progress in implementing these measures; the establishment of a trilateral network of defense investors; and New Zealand's interest in joining a portion of AUKUS.

AUKUS heads of defense discuss defense pact progress. In December 2023, Australian Minister for Defense Richard Marles, UK Secretary of State for Defense Grant Shapps, and US Secretary of Defense Lloyd Austin III met in California to [discuss](#) the AUKUS defense partnership. They discussed the progress made on AUKUS Pillar I (see box below) since March 2023, including the following:

- The graduation of the first class of Royal Australian Navy officers from the US Nuclear Power School
- The first group of Australian industry personnel beginning work at UK and US shipyards to develop the skills necessary to build and sustain nuclear-powered submarines²¹
- An increased frequency in US Navy nuclear-powered submarine visits to Australian ports²⁶

AUKUS Pillars I and II

The AUKUS partnership consists of two pillars:

- **Pillar I:** Providing Australia with conventionally armed, [nuclear-powered submarines](#) at the "earliest possible date," according to a White House fact sheet on AUKUS implementation.²² The "[optimal pathway](#)," announced in March 2023, provides a framework and timeline for Australia to receive this submarine capability, as well as the expertise to operate and maintain it, as soon as the early 2030s.²³
- **Pillar II:** Developing [advanced capabilities](#) by increasing defense technology collaboration between AUKUS countries, including a focus on technology protection.²⁴ Under Pillar II, the three nations plan to cooperate trilaterally on "emerging tech areas."²⁵

The AUKUS heads of defense also announced a number of [developments](#) under Pillar II (see box above). As discussed in [Issue 4](#) of *Intersections*, the three AUKUS nations have already identified a total of eight areas—four advanced capabilities, and four other areas—on which they intend to focus their collaboration.²⁷ At the December 2023 meeting, the heads of defense specified technologies on which they plan to collaborate, including quantum positioning, navigation, and timing, as well as undersea systems.²⁸ The three nations also committed to the following:

- Holding a “Maritime Autonomy Experimentation and Exercise Series” to enhance trilateral interoperability and capability development in autonomous maritime systems
- Launching a series of “AUKUS Innovation Challenges,” which will allow companies from all three AUKUS countries to compete for common innovation challenge prizes
- Strengthening cybersecurity among critical naval suppliers²⁹

AUKUS Defense Investor Network established. In December, the US-based innovation advisory firm BMNT announced the formation of the [AUKUS Defense Investor Network](#) (DIN) from more than 400 private Australian, UK, and US investors.³⁰ The AUKUS DIN aims to [accelerate](#) AUKUS Pillar II by investing in companies developing key dual-use technologies.³¹ According to Heather Richman, a co-chair of the AUKUS DIN, the group is meant to act as a forum in which investors can learn from one another and through which government and military stakeholders will be better able to communicate technology priorities to investors.³²

New Zealand expresses interest in joining AUKUS Pillar II. In mid-December 2023, New Zealand Prime Minister Christopher Luxon said that his government would [explore](#) joining AUKUS Pillar II.³³ Whether New Zealand should join AUKUS has been a [contentious issue](#) among New Zealand leaders. According to Dr. Anna Powles of New Zealand’s Massey University, some New Zealand leaders fear that associating the country with AUKUS could damage the credibility of the country’s efforts to be seen as independent from its traditional US, UK, and Australian partners.³⁴ New Zealand banned nuclear weapons and nuclear-powered vessels from its territory in the mid-1980s in solidarity with Pacific Islands nations subjected to nuclear tests in the region and in compliance with the Treaty of Rarotonga.³⁵ New Zealand’s policy effectively barred US Navy vessels from New Zealand’s ports and led to the US suspending its mutual-defense commitment to New Zealand under the Australia-New Zealand-US (ANZUS) treaty. Despite this historical legacy, however, according to *Breaking Defense*, New Zealand’s leadership has become wary of the PRC’s growing military capabilities and views joining AUKUS Pillar II as a way to obtain valuable defense technology and enhance New Zealand’s interoperability with its closest ally, Australia.³⁶

OTHER US ALLY AND PARTNER DEVELOPMENTS

PRC and EU leaders meet to discuss subsidies to green technologies, including electric vehicles (EVs).

In December 2023, EU and China leaders held a summit to discuss China’s industrial policy, exports of EVs, and EU concerns about PRC state subsidies.³⁷ The China-EU summit comes on the heels of the EU’s Anti-Subsidy Probe into Vehicle Imports from China, which was launched in October 2023 (discussed in [Issue 7](#)). The European Commission initiated the investigation to determine whether there is evidence that PRC state subsidies comply with “strict EU state-aid rules.”³⁸

The investigation is examining whether PRC subsidies have unfairly advantaged Chinese firms and led to the country's dominance of the lithium-ion battery market. Subsidies are one of the mechanisms by which the PRC government [incentivizes](#) firms to align their activities with Beijing's technological priorities. According to the *Economist*, China produces "70 percent of the world's lithium-ion batteries," and between 2016–2022, the PRC government provided subsidies worth an estimated \$57 billion USD to domestic EV companies.³⁹ If the EU determines that the subsidies are contrary to EU rules, officials could levy countervailing tariffs.⁴⁰ PRC officials appear to be adopting a mixed response to the prospect of EU tariffs. For example, on January 18, the PRC vice minister of industry and information technology said the country would rein in some EV production.⁴¹ However, also in January, Beijing initiated an investigation against France for cognac sales, possibly in retaliation for the EU investigation.⁴²

UK launches review of foreign investment screening measures. On November 13, 2023, the UK government launched a review of the country's National Security and Investment (NSI) Act.⁴³ The act, which went into effect in January 2022, established a regime for screening foreign investments in UK companies for potential national security risks. It lists 17 sensitive sectors of the economy—including advanced robotics, AI, defense, energy, and data infrastructure—in which companies are legally required to notify the government of acquisitions by foreign entities.⁴⁴ According to a January 2024 call for public comments on the act, the UK government is considering removing certain reporting requirements and narrowing the number of industries to which the investment screening regime applies. The review is also considering refining the scope of the AI category to remove activities assessed as not posing risks to national security.⁴⁵

The move to review the NSI Act comes amid a slump in UK corporate mergers. In the first half of 2023, the country's firms saw an estimated 22 percent decline in mergers and acquisitions and a 55 percent drop in the value of these deals.⁴⁶ The review also comes amid public criticism from Beijing that the act unfairly targets PRC investment. In July 2023, a spokesperson for the PRC Embassy in the UK accused the UK government of "discriminatory practices" and "wanton suppression" of PRC firms in implementing the act.⁴⁷

Taiwan's Executive Yuan announces national core technologies list to protect key projects. In November 2023, the Taiwan Executive Yuan identified an initial list of 22 specific technologies in need of "urgent protection."⁴⁸ A new government committee, the National Core Key Technologies Review Committee, is responsible for managing this list, and individual government agencies are able to make submissions of technologies that should be included.⁴⁹ The new list has been developed based on provisions in Taiwan's National Security Act, which was amended in June 2022.⁵⁰ The law was revised to strengthen protections for critical technologies and "impose criminal penalties on economic espionage."⁵¹ Five technical areas are included in the list announced by the review committee: defense, aerospace, agriculture, semiconductors, and information communications technology.⁵² If any technical secrets are leaked, cases will be investigated according to legal procedures as laid out in the National Security Act.⁵³

The Taiwan government's creation of a critical technology list follows recent trends in the US (discussed in [Issue 1](#)), Australia, and the EU (discussed in [Issue 3](#)) to use these types of lists to help industry understand which technologies are critical for national security. The new list also comes amid allegations that information about Taiwan's submarine program was leaked, as discussed in [Issue 7](#).

New South Korean government commission aims to offset domestic supply chain vulnerabilities. On December 11, the Republic of Korea (ROK) government announced that by June 2024 it would establish a commission to coordinate and oversee national policies on critical industrial supply chains. The government-wide commission will work to identify and mitigate risks to supply chains that are highly

dependent on specific countries, including China. Speaking at an inter-ministerial meeting, the ROK finance minister warned that supply chain risk factors are mounting for items directly related to core ROK industries. At-risk items identified by the finance minister include urea, diammonium phosphate, and graphite (all of which have been subject to PRC export controls). Urea is widely used to reduce emissions in diesel vehicles, while diammonium phosphate and graphite are raw materials essential to the production of fertilizers and batteries. The ROK government seeks to hedge against related supply chain risks through approaches that include diversifying procurement sources, stockpiling critical supplies, and fostering domestic production.⁵⁴

US officials raise concerns that a United Arab Emirates (UAE) firm is transferring sensitive emerging technologies and data from US companies to the PRC. On November 27, the *New York Times* [reported](#) on a months-long US government campaign to persuade an ascendant UAE technology company to distance itself from China. The company in question, G42, is an Abu Dhabi-based AI firm established in 2018 as part of the UAE's efforts to diversify revenue streams beyond oil income. G42 has grown rapidly in recent years, establishing partnerships with US tech giants such as Microsoft, Dell Technologies, and OpenAI.⁵⁵ At the same time, G42 has also reportedly been expanding its business with PRC technology companies, which the US views as a threat to national security. Per the *Times* report, specific issues of concern flagged by US intelligence agencies include G42's digital infrastructure, which, according to the report, was built with the assistance of Huawei and other PRC firms. The report also notes US officials' concern about G42's access to US citizens' genetic data and fear that such data could end up in PRC government hands.⁵⁶

On January 9, the chairman of the US Congress's House Select Committee on the Chinese Communist Party sent a letter to the secretary of the Department of Commerce calling for her department to closely examine G42 and its subsidiaries for inclusion on the department's Entity List.⁵⁷ According to a separate *Times* report, the letter claimed that G42 is affiliated with an "expansive network" of PRC entities that support PRC military advances.⁵⁸ In response, G42 issued a January 11 [statement](#) in which the company denied allegations of any connections to the PRC government and PRC military-affiliated entities. The statement claims that since 2022, the company has committed to "fully align with our US partners" in the field of advanced technologies and "not to engage with Chinese companies" in these matters.⁵⁹ Relatedly, in December 2023, G42's CEO Peng Xiao told the *Financial Times* that G42 would cut ties with PRC entities in response to US concerns.⁶⁰

ADVANCES IN CRITICAL AND EMERGING TECH

Twenty-eight countries and the EU attend AI safety summit in the UK. In November 2023, leaders from 28 countries and the EU attended the first-ever global AI safety [summit](#) in the UK.⁶¹ The summit's first day featured such topics as how to identify the risks inherent in AI systems and how to mitigate these risks while leveraging AI's potential to support economic and societal benefits. The [Bletchley Declaration](#), in which the 28 countries and the EU issued a statement of principles regarding AI benefits and risks, was announced at the event.⁶² The second day involved a smaller group of "like-minded countries" discussing how to work together on AI.⁶³ Although the majority of countries were represented by heads of government or similarly high-ranking officials, the PRC sent a comparatively low-ranking official: Vice Minister of Science and Technology Wu Zhaohui. According to a Reuters [report](#), Wu attended the summit's first day but was absent from the more exclusive second day events.⁶⁴

Apart from its participation in the UK summit, Beijing appears to be pursuing its own separate approach to AI governance. For example, in October 2023, the PRC Ministry of Foreign Affairs issued a "Global

Governance Initiative” statement outlining Beijing’s approach to AI governance. The statement calls for countries to adopt a “responsible attitude to... application of AI technologies in the military field.”⁶⁵

ILLEGAL ACTIVITIES

PRC uses hacking to acquire data and software for AI development, enabling improved hacking. In December 2023, the *Wall Street Journal* released an investigative report on how the PRC’s [theft of AI software](#) enhances its efforts to acquire and process sensitive information. According to the report, the amount of personal data that the PRC has already obtained through hacking is so large that it could not feasibly be processed without advanced AI technology.⁶⁶ Moreover, after the PRC uses AI software to process large volumes of information, it can then use insights derived from this AI-enabled processing to refine its selection of hacking targets. As noted in the report, evidence from a 2021 attack on Microsoft’s email service indicates that the PRC may have already begun to refine its targeting of hacking by using AI-processed data obtained from previous hacking efforts. A National Public Radio [investigation](#) of the same cyber-attack on Microsoft argues that the hack may have been intended to obtain a volume of data substantial enough to support training of AI models.⁶⁷

CHINA’S NATIONAL SECURITY LAWS

Under Chinese Communist Party leadership, the PRC uses [national security laws](#) to assert PRC interests, including modernizing China’s military and controlling critical technology. From 2014 to 2023, the PRC government passed or revised over a dozen laws related to national security. PRC leaders use these laws to justify a range of restrictions, demands, and punitive actions against PRC and foreign firms and individuals. The laws are vaguely worded and could be expansively interpreted by PRC officials, potentially posing risks for foreign governments, companies, and individuals in China and abroad. For example, in its decision to bar certain PRC companies from purchasing Micron Technologies’ chips (covered in this issue, as well as in [Issue 4](#) and [Issue 5](#)), the PRC government cited China’s Cybersecurity Law as the legal basis for its actions.⁶⁸

Major PRC national security legislation:



Note: the dates show the month and year that each law came into force

*The law’s full title is the “Law on Safeguarding National Security in the Hong Kong Special Administrative Region of the PRC”

PRC national security laws provide justification for China to accomplish the following:

- Access data or encryption keys held by foreign firms with operations in the PRC
- Detain foreign nationals living, working, or traveling throughout the PRC and possibly beyond
- Prevent PRC entities and individuals from sending “sensitive” data abroad
- Require PRC citizens to assist in intelligence-gathering activities

For more on PRC national security laws and their global implications, see CNA's new [two-page handout](#).⁶⁹

NOTES

¹ *The People's Republic of China Uses Diverse Tools to Access Foreign Technology and Critical Infrastructure*, CNA, Apr. 2022, <https://www.cna.org/quick-looks/2022/PRC-USES-TOOLS-TO-ACCESS-FOREIGN-TECHNOLOGY.pdf>.

² "Catalog of Technologies Prohibited or Restricted from Export" (中国禁止出口限制出口技术目录), Ministry of Commerce and Ministry of Science and Technology of the People's Republic of China, Dec. 2023, <https://www.most.gov.cn/tztg/202312/W020231221620858841394.pdf>.

³ "Catalog of Technologies Prohibited or Restricted from Export" (中国禁止出口限制出口技术目录); "Catalog of Technologies Prohibited or Restricted from Export" (中国禁止出口限制出口技术目录), Ministry of Commerce and Ministry of Science and Technology of the People's Republic of China, Aug. 2020, http://www.gov.cn/zhengce/zhengceku/2020-08/29/content_5538299.htm.

⁴ Fapeng Yu, Xiulan Duan, Shujun Zhang, Qingming Lu, and Xian Zhao, "Rare-Earth Calcium Oxyborate Piezoelectric Crystals $\text{ReCa}_4\text{O}(\text{BO}_3)_3$: Growth and Piezoelectric Characterizations," *Crystals* (2014), 4(3), pp. 241-261, <https://doi.org/10.3390/cryst4030241>.

⁵ James Holler, Douglas Skoog, and Stanley Crouch, *Principles of Instrumental Analysis (6th ed.)*, Cengage Learning, p. 9, 2007, <https://search.worldcat.org/title/principles-of-instrumental-analysis/oclc/423542548>.

⁶ Fapeng Yu, Xiulan Duan, Shujun Zhang, Qingming Lu, and Xian Zhao, "Rare-Earth Calcium Oxyborate Piezoelectric Crystals $\text{ReCa}_4\text{O}(\text{BO}_3)_3$: Growth and Piezoelectric Characterizations."

⁷ Lara Seligman, "China Dominates the Rare Earths Market. This US Mine Is Trying to Change That," *Politico*, Dec. 14, 2022, <https://www.politico.com/news/magazine/2022/12/14/rare-earth-mines-00071102>.

⁸ Eleanor Olcott and Demetri Sevastopulo, "China Bans Micron's Products from Key Infrastructure Over Security Risk," *Financial Times*, May 21, 2023, <https://www.ft.com/content/e6a8e034-cbc2-4267-9b41-b7670db7d130>.

⁹ "Minister Wang Wentao Meets with Micron Chairman and CEO Sanjay Mehrotra" (王文涛部长会见美光科技公司总裁兼首席执行官桑杰·梅赫罗特拉), Ministry of Commerce of the People's Republic of China, Nov. 3, 2023, <http://www.mofcom.gov.cn/article/xwfb/xwbldhd/202311/20231103450989.shtml>.

¹⁰ "China's National Security Laws: Implications Beyond Borders," CNA, Dec. 2023, <https://www.cna.org/quick-looks/2023/China-national-security-laws-implications-beyond-borders.pdf>.

¹¹ "Micron Warns of Bigger Revenue Hit from China Ban," Reuters, June 16, 2023, <https://www.reuters.com/technology/micron-says-half-china-headquarter-revenue-risk-due-ban-2023-06-16/>.

¹² Brenda Goh, "Micron Says It Is Committed to China, Invests \$602 Million Plant," Reuters, June 16, 2023, <https://www.reuters.com/technology/micron-invest-603-mln-factory-chinas-xian-over-next-few-years-2023-06-16/>.

¹³ Rose Tenyotkin, April Herlevi, Alison Kaufman, and Anthony Miller, *Economic Statecraft: How China Legally Accesses Foreign Technologies to Build Military Capabilities*, CNA, June 1, 2020, <https://www.cna.org/reports/2020/08/economic-statecraft-china>.

¹⁴ David Shepardson, "China Import Concerns Spur US to Launch Semiconductor Supply Chain Review," Reuters, Dec. 21, 2023, <https://www.reuters.com/technology/us-launching-semiconductor-supply-chain-review-boost-national-security-2023-12-21/>.

-
- ¹⁵ *Assessment of the Status of the Microelectronics Industrial Base in the United States*, Office of Technology Evaluation, Bureau of Industry and Security, US Department of Commerce, Dec. 2023, <https://www.bis.doc.gov/index.php/documents/technology-evaluation/3402-section-9904-report-final-20231221/file>.
- ¹⁶ "Chips for America," National Institute of Standards and Technology, accessed Jan. 10, 2024, <https://www.nist.gov/chips>.
- ¹⁷ Ana Swanson, "Biden Administration Chooses Military Supplier for First Chips Act Grant," *New York Times*, Dec. 11, 2023, <https://www.nytimes.com/2023/12/11/business/economy/biden-chips-bae-systems.html>.
- ¹⁸ "DOD Releases First-Ever National Defense Industrial Strategy," US Department of Defense, Jan. 11, 2024, <https://www.defense.gov/News/Releases/Release/Article/3643326/dod-releases-first-ever-national-defense-industrial-strategy/>.
- ¹⁹ "DOD Releases First-Ever National Defense Industrial Strategy."
- ²⁰ Tom Corben, Ashley Townshend, and Susannah Patton, "What is the AUKUS Partnership?" United States Studies Center, Sept. 16, 2021, <https://www.usssc.edu.au/explainer-what-is-the-aukus-partnership>.
- ²¹ "AUKUS Defense Ministers Meeting Joint Statement," US Department of Defense, Dec. 1, 2023, <https://www.defense.gov/News/Releases/Release/Article/3604511/aukus-defense-ministers-meeting-joint-statement/>.
- ²² "FACT SHEET: Implementation of the Australia- United Kingdom – United States Partnership (AUKUS)." The White House, Apr. 5, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/>.
- ²³ "Optimal Pathway," Australian Submarine Agency, <https://www.asa.gov.au/aukus/optimal-pathway>.
- ²⁴ "FACT SHEET: Implementation of the Australia- United Kingdom – United States Partnership (AUKUS)." The White House, Apr. 5, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/>.
- ²⁵ Bonnie Denise Jenkins, "AUKUS: A Commitment to the Future," Remarks at the Atlantic Council, Washington DC, Nov. 27, 2023, <https://www.state.gov/aukus-a-commitment-to-the-future/>.
- ²⁶ Lloyd Austin III, Richard Marles, and Grant Shapps, "AUKUS Defense Ministers Joint Press Briefing," US Department of Defense, Dec. 1, 2023, <https://www.defense.gov/News/Transcripts/Transcript/Article/3604674/aukus-defense-ministers-joint-press-briefing/>.
- ²⁷ These eight areas are: undersea capabilities, quantum technologies, AI and autonomy, advanced cyber, hypersonic/counter-hypersonic capabilities, electronic warfare, innovation, and information sharing. See: "FACT SHEET: Implementation of the Australia- United Kingdom – United States Partnership (AUKUS)." The White House, Apr. 5, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/>.
- ²⁸ Lloyd Austin III, Richard Marles, and Grant Shapps, "AUKUS Defense Ministers Joint Press Briefing"; "AUKUS Defense Ministers Meeting Joint Statement," US Department of Defense, Dec. 1, 2023, <https://www.defense.gov/News/Releases/Release/Article/3604511/aukus-defense-ministers-meeting-joint-statement/>.
- ²⁹ "AUKUS Defense Ministers Meeting Joint Statement."
- ³⁰ Courtney Albon, "Investors Form Alliance to Bolster AUKUS Military Partnership," C4ISRNET, Jan. 10, 2024, <https://www.c4isrnet.com/battlefield-tech/2024/01/10/investors-form-alliance-to-bolster-aukus-military-partnership/>.

-
- ³¹ BMNT, "AUKUS Defense Investor Network Launches," PR Newswire, Dec. 5, 2023, <https://www.prnewswire.com/news-releases/aukus-defense-investor-network-launches-302006167.html>.
- ³² "Investors Form Alliance to Bolster AUKUS Military Partnership."
- ³³ Renju Jose and Lucy Craymer, "New Zealand to Explore AUKUS Benefits, Boost Security Ties with Australia," Reuters, Dec. 19, 2023, <https://www.reuters.com/world/asia-pacific/new-zealands-luxon-talk-defence-economy-australia-2023-12-19/>.
- ³⁴ Tim Fish, "New Zealand in AUKUS? The Political Kiwi Conundrum over Pillar 2 Membership," *Breaking Defense*, June 2, 2023, <https://breakingdefense.com/2023/06/new-zealand-in-aukus-the-political-kiwi-conundrum-over-pillar-2-membership/>.
- ³⁵ Tess McClure, "Aukus Submarines Banned from New Zealand as Pact Exposes Divide With Western Allies," *Guardian*, Sept. 15, 2021, <https://www.theguardian.com/world/2021/sep/16/aukus-submarines-banned-as-pact-exposes-divide-between-new-zealand-and-western-allies>. The Treaty of Rarotonga is more formally known as the South Pacific Nuclear Free Zone Treaty, which was signed in 1985 and came into force in 1986. See: *South Pacific Nuclear-Free Zone (Treaty of Rarotonga)*, Aug. 6, 1985, https://media.nti.org/documents/treaty_of_rarotonga.pdf.
- ³⁶ Tim Fish, "New Zealand in AUKUS? The Political Kiwi Conundrum over Pillar 2 Membership."
- ³⁷ Joe Leahy, Henry Foy, Andy Bounds, Andy Lin, "China's Xi Jinping Meets EU Leaders for High Stakes Talks," *Financial Times*, Dec. 6, 2023, <https://www.ft.com/content/527e4822-b89c-4c98-81d5-92a01ca875b6>.
- ³⁸ European Parliament, "EU Anti-Subsidy Probe into Electric Vehicle Imports from China," Oct. 2023, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/754553/EPRS_ATA\(2023\)754553_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/754553/EPRS_ATA(2023)754553_EN.pdf).
- ³⁹ *Economist*, "Western Firms Are Quaking as China's Electric-Car Industry Speeds Up," Jan. 11, 2024, <https://www.economist.com/briefing/2024/01/11/western-firms-are-quaking-as-chinas-electric-car-industry-speeds-up>.
- ⁴⁰ European Parliament, "EU Anti-Subsidy Probe into Electric Vehicle Imports from China."
- ⁴¹ William Sandlund and Edward White, "China Vows to Rein in Capacity in Electric Vehicle Industry," *Financial Times*, Jan. 18, 2024, <https://www.ft.com/content/bf4aa7c8-5eb9-4927-909f-b37d18674988?shareType=nongift>.
- ⁴² Edward White, Adrienne Klasa, and Madeleine Speed, "China Targets French Brandy Imports in Escalating Trade Dispute," *Financial Times*, Jan. 5, 2024.
- ⁴³ "Call for Evidence - National Security and Investment Act," GOV.UK, Nov. 13, 2023, <https://www.gov.uk/government/calls-for-evidence/call-for-evidence-national-security-and-investment-act/call-for-evidence-national-security-and-investment-act>.
- ⁴⁴ "12 December 2023 - NSI Act 2021: Annual Report 2022-2023 - Oral Evidence," UK Parliament, Dec. 12, 2023, <https://committees.parliament.uk/event/20006/formal-meeting-oral-evidence-session/>.
- ⁴⁵ "Call for Evidence - National Security and Investment Act."
- ⁴⁶ Matthew Field, "Dowden to Water Down National Security Takeover Rules After Collapse in Dealmaking," *Telegraph*, Nov. 13, 2023, <https://www.telegraph.co.uk/business/2023/11/13/rishi-sunak-dowden-national-security-takeover-rules-china/>.
- ⁴⁷ "Embassy Spokesperson on the UK's Intervention in Chinese Investment in the UK on the Grounds of National Security," Embassy of the People's Republic of China in the United Kingdom of Great Britain and Northern Ireland, July 12, 2023, http://gb.china-embassy.gov.cn/eng/PressandMedia/Spokepersons/202307/t20230712_11112203.htm.

- ⁴⁸ Republic of China National Science and Technology Council, “Announce National Core Key Technologies and Strengthen Protection of Business Secrets” (公布國家核心關鍵技術加強保護營業秘密), Dec. 5, 2023, <https://www.nstc.gov.tw/folksonomy/detail/ab71317e-c22e-467a-b3a0-7515aa2bfe6e?l=ch>.
- ⁴⁹ Lee Tsai et al., “Formal Implementation of the Legal Regime for National Core Key Technologies (Taiwan),” Lexology, June 30, 2023, <https://www.lexology.com/library/detail.aspx?g=09a72530-abae-40d1-b617-42f94ea3aa45>.
- ⁵⁰ *National Security Act* (全國法規資料庫), Laws and Regulations Database of the Republic of China (Taiwan), June 8, 2022, <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030028>.
- ⁵¹ IAM Trade Secrets, “Amended National Security Act Imposes Stricter Punishments on Trade Secret Misappropriation Following New List of Crucial Tech,” Jan. 17, 2024, <https://www.iam-media.com/article/amended-national-security-act-imposes-stricter-punishments-trade-secret-misappropriation-following-new-list-of-crucial-tech>.
- ⁵² The defense category includes six technologies, aerospace includes eight, agriculture and ICT include three technologies each, and two types of semiconductor manufacturing technology are on the list.
- ⁵³ *National Security Act* (全國法規資料庫).
- ⁵⁴ Park Han-na, “Korea to Set Up Commission to Combat Supply Chain Disruptions,” *Korea Herald*, Dec. 11, 2023, https://www.koreaherald.com/view.php?ud=20231211000677&ACE_SEARCH=1.
- ⁵⁵ Mark Mazzetti and Edward Wong, “Inside US Efforts to Untangle an AI Giant’s Ties to China,” *New York Times*, Nov. 27, 2023, <https://www.nytimes.com/2023/11/27/us/politics/ai-us-uae-china-security-g42.html>.
- ⁵⁶ “Inside US Efforts to Untangle an AI Giant’s Ties to China.”
- ⁵⁷ “Gallagher Calls on USG to Investigate AI Firm, G42, Ties to PRC Military, Intelligence-Linked Companies,” Select Committee on the CCP, Jan. 9, 2024, <https://selectcommitteeontheccp.house.gov/media/press-releases/gallagher-calls-usg-investigate-ai-firm-g42-ties-prc-military-intelligence>.
- ⁵⁸ Edward Wong, Mark Mazzetti, and Paul Mozur, “Lawmakers Push U.S. to Consider Trade Limits with A.I. Giant Tied to China,” *New York Times*, Jan. 9, 2024, <https://www.nytimes.com/2024/01/09/us/politics/ai-china-uae-g42.html>.
- ⁵⁹ “Statement on the New York Times Article and the Letter from the United States Congress House Select Committee on the CCP,” G42, Jan. 11, 2024, <https://www.g42.ai/resources/news/Statement-on-the-New-York-Times-article-and-the-letter-from-the-United-States-Congress-House-Select-Committee-on-the-CCP>.
- ⁶⁰ Michael Peel and Simeon Kerr, “UAE’s Top AI Group Vows to Phase Out Chinese Hardware to Appease US,” *Financial Times*, Dec. 7, 2023, <https://www.ft.com/content/6710c259-0746-4e09-804f-8a48ecf50ba3>.
- ⁶¹ “AI Safety Summit Hosted by the UK,” Government of the United Kingdom, accessed Jan. 11, 2024, <https://www.aisafetysummit.gov.uk/>.
- ⁶² *The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023*, Government of the United Kingdom, Nov. 1, 2023, <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>.
- ⁶³ Brenda Goh and Paul Sandle, “Exclusive: China Took Part in Leaders’ AI Meeting Even Though UK Did Not Acknowledge,” Reuters, Nov. 3, 2023, <https://www.reuters.com/technology/china-took-part-leaders-ai-meeting-even-though-uk-did-not-acknowledge-2023-11-03/>.
- ⁶⁴ Brenda Goh and Paul Sandle, “Exclusive: China Took Part in Leaders’ AI Meeting Even Though UK Did not Acknowledge.”
- ⁶⁵ “Global AI Governance Initiative,” PRC Ministry of Foreign Affairs, Oct. 20, 2023, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202310/t20231020_11164834.html.

⁶⁶ Robert McMillan, Dustin Volz, and Aruna Viswanatha, "Beijing Is Stealing AI Secrets to Power Its Spying, US Says," *Wall Street Journal*, Dec. 26, 2023, https://www.wsj.com/tech/ai/china-is-stealing-ai-secrets-to-turbocharge-spying-u-s-says-00413594?mod=politics_lead_pos2.

⁶⁷ Dina Temple-Raston, "China's Microsoft Hack May have had a Bigger Purpose than Just Spying," NPR, Aug. 26, 2021, <https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying>.

⁶⁸ "Micron's Products Sold in China Did Not Pass Cybersecurity Review" (美光公司在华销售的产品未通过网络安全审查), Cyberspace Administration of China, May 21, 2023, http://www.cac.gov.cn/2023-05/21/c_1686348043518073.htm.

⁶⁹ *China's National Security Laws: Implications Beyond Borders*, CNA, Dec. 2023, <https://www.cna.org/quick-looks/2023/China-national-security-laws-implications-beyond-borders.pdf>.

Intersections is produced by CNA's China and Indo-Pacific Security Affairs Division. The division's team of approximately three dozen language-skilled regional specialists has provided sponsors and the public with the context to make informed, data-based assessments about this critical region since 1998.

For additional information, please contact INTERSECTIONS@CNA.ORG.

Approved February 2024: Maryanne Kivlehan-Wise, Research Program Director
China Studies Program, China and Indo-Pacific Security Affairs Division

This work was created in the performance of Federal Government Contract No. N00014-22-D-7001.

DISTRIBUTION STATEMENT A. Cleared for Public Release.

Public Release

2/21/2024

This document contains the best opinion of CNA at the time of issue. The views, opinions, and findings contained in this report should not be construed as representing the official position of the Department of the Navy.

Any copyright in this work is subject to the Government's Unlimited Rights license as defined in DFARS 252.227-7013 and/or DFARS 252.227-7014. The reproduction of this work for commercial purposes is strictly prohibited. Nongovernmental users may copy and distribute this document noncommercially, in any medium, provided that the copyright notice is reproduced in all copies. Nongovernmental users may not use technical measures to obstruct or control the reading or further copying of the copies they make or distribute. Nongovernmental users may not accept compensation of any manner in exchange for copies.

All other rights reserved. The provision of this data and/or source code is without warranties or guarantees to the Recipient Party by the Supplying Party with respect to the intended use of the supplied information. Nor shall the Supplying Party be liable to the Recipient Party for any errors or omissions in the supplied information.

This report may contain hyperlinks to websites and servers maintained by third parties. CNA does not control, evaluate, endorse, or guarantee content found in those sites. We do not assume any responsibility or liability for the actions, products, services, and content of those sites or the parties that operate them.

CNA is a nonprofit research and analysis organization dedicated to the safety and security of the nation. It operates the Center for Naval Analyses—the only federally funded research and development center serving the Department of the Navy—as well as the Institute for Public Research. CNA is dedicated to developing actionable solutions to complex problems of national importance.

DNL-2023-U-037272-Final2

Subscribe or unsubscribe at intersections@cna.org