MARCH 2025

Understanding U.S. Allies' Current Legal Authority to Implement AI and Semiconductor Export Controls

AUTHORS
Gregory C. Allen
Isaac Goldston

A Report of the CSIS Wadhwani AI Center

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | WADHWANI AI CENTER

Table of Contents

MARCH 2025

Understanding U.S. Allies' Current Legal Authority to Implement AI and Semiconductor Export Controls

By Gregory C. Allen and Isaac Goldston

Executive Summary

Since October 2022, the United States has devoted significant resources to restricting China's access to artificial intelligence (AI) and advanced semiconductor technologies. In the final months of the Biden administration, the Department of Commerce issued four additional far-reaching export control updates. On December 2, 2024, it released **two rules** that added 140 companies to the Entity List, expanded the scope of the Foreign Direct Product Rule (FDPR), and restricted new technology areas such as high-bandwidth memory, among other measures. In the second week of January 2025, the Department of Commerce issued the **AI Diffusion Framework** and the **Foundry Due Diligence Rule**, further shaping the spread of AI and semiconductor technologies throughout the world. Export controls remain front and center for the second Trump administration, which **directed** an effort to "identify and eliminate loopholes in existing export controls—especially those that enable the transfer of strategic goods, software, services, and technology . . . to strategic rivals and their proxies" on its first day in office.

However, countries like the Netherlands, Germany, South Korea, Japan, and Taiwan continue to control key chokepoints in the AI and semiconductor value chain, making unilateral action only so effective. Furthermore, the existing multilateral export control architecture is neither sufficiently flexible nor fast to allow for the kind of sophisticated, targeted controls that the United States has levied on China. The success or failure of the U.S. export control strategy is thus dependent on its allies' ability to implement controls outside of this traditional architecture or U.S. extraterritorial regulations covering allies.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | WADHWANI AI CENTER

This paper provides an in-depth analysis of U.S. allies' export control authorities related to AI and semiconductor technologies and does the same analysis for China. It demonstrates that U.S. allies often do not have equivalents to U.S. export control authorities and tools like the FDPR and Entity List, but that they generally do have the capability to introduce some controls on advanced semiconductor chips and related equipment not covered by multilateral export control regimes. As a result, lack of alignment with the U.S. export control regime cannot necessarily be attributed to a lack of authorities alone. Allies' enforcement capacity and willingness to act are also key ingredients in the implementation of effective export controls and are crucial to the success of U.S. and allied technology competition with China. Accordingly, the recommendations section of this paper addresses each of these three elements.

The paper proceeds as follows. First, it identifies key export control authorities used by the United States to slow the progress of China's AI and semiconductor industries and analyzes which other countries possess these authorities and are thus capable of implementing similar controls. It then surveys the export control policies of key actors, including the European Union, the Netherlands, Germany, Japan, South Korea, Taiwan, and China. It concludes by offering recommendations to U.S. and allied policymakers to make AI and semiconductor export controls more effective.

Overview

In December 2023, then-Secretary of Commerce Gina Raimondo clearly **outlined** the U.S. strategy for China and its AI ecosystem when she said, "America leads the world in artificial intelligence. America leads the world in advanced semiconductor design, period. . . . We're a couple years ahead of China. No way are we going to let them catch up." To achieve this goal, the U.S. national security enterprise has undertaken a massive, multifaceted effort to **choke off** China's access to cutting-edge AI and related technologies.

Export controls on the **high-performance semiconductors** used to **train and inference** state-of-the-art AI models have been at the forefront of this effort so far. On October 7, 2022, the United States enacted a comprehensive set of export controls on advanced semiconductor technologies. Although these controls marked the **reversal** of nearly 30 years of trade policy, they did not achieve all of their intended goals. U.S. chip designers like Nvidia **continued** to provide Chinese customers with slightly lower-performance chips, which according to the U.S. Department of Commerce's Bureau of Industry and Security (BIS), provided "nearly comparable AI model training capability." In October 2023, the United States **updated** these controls to cover a much larger set of chips and semiconductor manufacturing equipment (SME). As noted in a **previous CSIS report**, "The United States is firmly focused on retaining control over so-called 'chokepoint' . . . technologies in the global semiconductor technology supply chain." The United States issued major export control updates in December 2024 and January 2025 that continued in this vein.

Despite the significant resources successive administrations have devoted to restricting China's access to AI and semiconductor technologies, China's AI ecosystem remains competitive with the United States'. In May 2024, Chinese AI company DeepSeek released a best-in-class open-weight model reportedly **trained** on Nvidia A100 chips stockpiled before the October 2022 controls went into effect. The even more impressive Deepseek-R1 reasoning model was **trained** on Nvidia H800 chips, which were not **restricted** before October 2023. The performance of DeepSeek-R1 was so far beyond what the financial

analyst community had expected a Chinese firm to be capable of that the tech-heavy Nasdaq **dropped** 3.1 percent in one day as a result of its release. This **previous CSIS paper** provides an in-depth analysis of DeepSeek and its implications for U.S. export controls.

Key U.S. AI and Semiconductor Export Control Authorities and Related Tools

At the core of the U.S. chip war strategy is a group of iteratively developed and highly sophisticated export control tools. Authorities granted in the **Export Control Reform Act of 2018** (ECRA), **Export Administration Regulations** (EAR), and **executive orders** offer the U.S national security community a range of options to control the export, reexport, transit, or transfer of select military, dual-use, and purely commercial items and technologies. In the House Committee on Foreign Affairs markup of ECRA, then-committee chairman Congressman Edward Royce **stated** that ECRA "closes gaps in our export controls that could permit transfers of cutting-edge technology like artificial intelligence and advanced semiconductors to potential adversaries such as Beijing." More accurately, ECRA represented the codification of U.S. export control powers that had previously relied on **authorities** in the International Emergency Economic Powers Act (IEEPA) and had a **novel focus on emerging technologies**.

The U.S. export control regime divides the responsibilities for administering and enforcing export controls on dual-use and military goods and technologies. The Department of Commerce is responsible for regulating the flow of dual-use technologies and less sensitive military items, which covers advanced semiconductors and related technologies, through the BIS. Meanwhile, the **Directorate of Defense Trade Controls** (DDTC) within the U.S. Department of State oversees and licenses weapons and munitions that are covered by the **International Traffic in Arms Regulations** (ITAR). **The Office of Foreign Assets Control** (OFAC) at the Treasury Department oversees restrictions on exports based on financial **sanctions**.

The four kinds of U.S. export controls most relevant to the **Trump** and Biden administrations' efforts to choke off China's access to AI are described below.

- **List-based controls**: List-based controls impose restrictions on specific commodities, software, and technologies. The United States primarily implements this kind of control through the **Commerce Control List** (CCL). The CCL includes dual-use items described by Export Control Classification Numbers (ECCNs), which may require licenses to export. Maintained by BIS, the CCL has played a crucial role in both the Trump and Biden administration's controls. For example, in October 2022 BIS **created** four new unilateral ECCNs related to high-performance chips and related SME and software. Meanwhile, the January 2025 **AI Diffusion Framework** created ECCN 4E091 to control AI model weights, which had not previously been controlled. To determine whether a license is granted for an item on the CCL, BIS also takes into consideration its intended end-user, the destination of the export, and its end-use.
- **End-user controls:** End-user controls impose restrictions on the export, reexport, and transfer of items destined for specific actors. BIS primarily implements this kind of control via the Entity List. The **Entity List** refers to people, companies, facilities, and government institutions that participate in "activities contrary to the national security or foreign policy interests of the United States" and are subject to a license requirement. With each export control update, the

United States has added Chinese firms to the Entity List including major AI and semiconductor companies like **Huawei**, **YMTC**, and **Naura Technology Group**.

- **End-use controls**: End-use controls impose restrictions on otherwise uncontrolled items for certain end-uses. For example, EAR sections **744.2**, **744.3**, and **744.4** impose license requirements on almost any item that might be used in the creation of weapons of mass destruction (WMDs). In the context of AI chips and related technologies, BIS **created a new license restriction** based on whether items would be used in the production of advanced node semiconductors—defined as logic chips at or below 16 nanometers (nm), DRAM memory chips at or below 18 nm, and NAND storage at or above 128 layers—as part of the October 2022 controls. This definition was changed as part of the December 2024 export control update and then again in January 2025.
- **Services controls**: Services controls **impose** restrictions on the activities of companies or individuals when the underlying commodities, software, and technologies involved in the service are not otherwise controlled. BIS implements this type of control under the **U.S. Persons Rule**. This authority controls the activities of U.S. companies or citizens when they are in support of certain end-uses found in EAR section **744.6**. Traditionally, the U.S. Persons Rule applied license requirements to "U.S. persons," defined as both people and firms, if they were engaging in activities **supporting** the development, production, or use of WMDs, even in situations not involving items subject to the EAR (i.e., wholly foreign-origin technology). However, as part of the October 2022 controls, BIS **informed** all "U.S. persons" that any activities in support of advanced node semiconductor production in China required a license. In doing so, BIS **made** the **novel** judgment that the act of supporting the development or production of advanced node semiconductors and related equipment "could involve 'support' for . . . weapons of mass destruction-related end-uses."

In addition to these four export control types, there are three further export control features that require explanation to understand U.S. AI and semiconductor export controls.

- **Multilateral regime-based versus unilateral or plurilateral:** Most allied countries' export control systems are grounded in multilateral agreements primarily focused on WMD nonproliferation like the **Wassenaar Arrangement**, which is the successor to the Cold War–era Coordinating Committee for Multilateral Export Controls (COCOM); the **Nuclear Suppliers Group**; the **Australia Group**; and the **Missile Technology Control Regime**. These regimes provide lists of commodities, software, and technology unanimously agreed on by members that should be subject to license requirements, in addition to end-use and services controls related to WMDs. However, the Trump and Biden administrations' AI and semiconductor export controls have focused on items not included in multilateral agreements and were initially implemented **unilaterally**, and then as a part of a plurilateral agreement (as in the case of the **reported deal** between the United States, Netherlands, and Japan).
- **Country-specific application:** The U.S. list-based, end-use, and services controls also can apply on a country-specific basis. For example, the October 2022 controls **introduced** measures banning the sale of high-end AI chips to any entity operating in China. Similarly, the October 2022 controls introduced a U.S. Persons Rule that applied on a China-specific basis.

- **Extraterritoriality:** In some cases, U.S. controls apply to foreign-produced items located outside the United States if they are a direct product of U.S. technology or software, or if they were produced by equipment that was the direct product of such technology or software. BIS implements this type of control through the **Foreign Direct Product Rule (FDPR)**. This authority allowed the United States to address a loophole in the pre-October 2022 controls. Namely, Chinese firms **were accessing** controlled SME, components, and spare parts from U.S. companies without a license via foreign headquartered and domiciled partners. By applying the FDPR more broadly with each export control update, BIS, at least in theory, addressed this challenge. In the December 2024 controls, BIS dramatically expanded the FDPR yet again, **meaning** that foreign-produced SME "that contain any amount of U.S.-origin integrated circuits" are subject to U.S. controls. Per this version of the rule, U.S.-origin integrated circuits includes any such chips manufactured with U.S. machines, meaning that effectively all chips on earth are considered U.S. origin. This authority was also central to the export control updates issued in January 2025. For example, the **AI Diffusion Framework** rule expanded the FDPR to AI model weights.

The United States has also employed a range of other economic security tools to restrict China's access to advanced semiconductor technologies. For example, in August 2023 the Biden administration used IEEPA to issue an executive order directing the U.S. Treasury Department to **establish a program** to review outbound investments in national critical sectors such as AI and semiconductors. This measure **followed** reporting that U.S. firms were investing in Chinese AI companies that were on the Entity List. On October 28, 2024, the U.S. Treasury Department **issued** its final rule on the implementation of the executive order, which went into effect on January 2, 2025, but is now subject to review as a result of the Trump administration's **America First Trade Policy memorandum**.

The Need for Allies

However vigorously the United States pursues its own export control strategy, it will be unable to achieve success without changing the behavior of other countries. While the United States holds a **strong position** in certain parts of the semiconductor value chain like chip design, other countries such as the Netherlands and Japan also play crucial roles in areas like SME. For example, Dutch company ASML is the **sole provider** of the latest generation of extreme ultraviolet (EUV) lithography machines needed to make cutting-edge AI chips. The consulting firm Accenture **estimated** that the inputs to a typical semiconductor chip "could cross international borders approximately 70 or more times before finally making it to the end customer." In other words, the United States does not control all the relevant chokepoints required to execute its export control strategy. In comments after the October 2022 controls went into effect, one U.S. official **told** Reuters, "We recognize that the unilateral controls that we are putting in place will lose effectiveness over time if other countries don't join us." At the December 2024 Reagan National Defense Forum, Gina Raimondo reiterated this sentiment, albeit more forcefully, **saying**, "When I set the rules, I have to make damn sure China can't just buy this stuff from Japan or Korea or the Europeans, so that's why we have to work with them."

Fully aware of this reality, Chinese officials have repeatedly threatened countries considering going along with the U.S. controls. For example, in a March 2022 interview, Tan Jian, China's ambassador

to the Netherlands, **said**, "This will not be without consequences. I'm not going to speculate on countermeasures, but China won't just swallow this," in response to the Netherlands's increasing alignment with the United States on export controls.[1]

Unfortunately, U.S. allies have not kept pace with the United States' increasingly restrictive export controls vis-à-vis China. While the U.S. export control system is designed to be able to keep up with technological developments and to be responsive to changing geopolitical circumstances, the regimes of its allies are generally not. As noted in the previous section, other countries with significant semiconductor industries have export control systems **grounded** in multilateral agreements primarily focused on WMD nonproliferation. These arrangements are significantly less agile than the U.S. system. For example, to add items to a Wassenaar Arrangement control list **requires** consensus from all participating countries, and opportunities for additions typically occur only once per year. As Wassenaar also includes Russia, which has obstructionist geopolitical goals, finding **consensus** on issues with geopolitical implications is unfeasible. In total, it can take up to **three years** to add a new item to Wassenaar control lists, even under favorable circumstances. Furthermore, Wassenaar explicitly prohibits controls targeting an individual country, **noting** in its founding document: "This arrangement will not be directed against any state or group of states." Limited improvements have been made to export control coordination between U.S. allies, such as the informal "**Wassenaar minus one**" approach, an effort by like-minded countries to harmonize controls on items and technologies not listed in traditional multilateral agreements.

But the existing multilateral export control architecture remains inadequate for U.S. national security requirements. As a result, understanding allied countries' unilateral export control authorities is crucial to the success or failure of the U.S. and allied technology competition with China.

The AI and Semiconductor Export Control Authorities Landscape

Allied countries possess significantly less comprehensive export control authorities than the United States. For the most part, they do not have an equivalent to key parts of the U.S. AI and semiconductor export control tool kit discussed in the previous sections like the FDPR, U.S. Persons Rule, Entity List, and restrictions that apply on a country-wide basis. This stands in radical contrast to China, which has **passed** no fewer than five laws since 2020 devoted to building a more sophisticated arsenal of economic security tools. In fact, China's most recent update to its Export Control Law **replicated** several key U.S. export control authorities. The following sections compare U.S., allied, and Chinese export control authorities across list-based, end-user, end-use, and services controls.

LIST-BASED CONTROLS

All U.S. allies implement the list-based controls found in the traditional four multilateral export control regimes. However, as shown in Table 1, they generally do have the ability to implement list-based controls outside of those regimes as well. For example, while the European Union does not have the power to require the imposition of export controls on semiconductor technologies, under **Article 9 of EU Dual-Use Regulation 2021/821**, EU member states are empowered to implement unilateral controls on otherwise uncontrolled items for "reasons of public security, including the prevention of acts of terrorism," or for "human rights considerations." The Netherlands specifically referenced Article 9 authorities when it issued its **Regulation on Advanced Production Equipment for**

1 The authors would like to thank an external reviewer who prefers to remain anonymous for their assistance in translating this quote.

Semiconductors in June 2023, which introduced a license requirement on the export of previously uncontrolled SME from the country. Similarly, when the Japanese government revealed its plans to place license requirements on 23 types of SME in 2023, it did so with authorities granted under its **Foreign Exchange and Foreign Trade Act** that was originally passed in 1949.

Table 1: U.S., Allied, and Chinese List-Based Export Control Authorities

	Multilateral Regime-Based				Unilateral or Plurilateral			
	Country-Specific		Not Country-Specific		Country-Specific		Not Country-Specific	
	Extraterritorial	Not Extraterritorial	Extraterritorial	Not Extraterritorial	Extraterritorial	Not Extraterritorial	Extraterritorial	Not Extraterritorial
United States	☐	☐	☐	☑ (tied to WMDs)	☑	☑	☑	☑
European Union	☐	☐	☐	☑ (tied to WMDs)	☐	☐	☐	☐
Netherlands	☐	☐	☐	☑ (tied to WMDs)	☐	☐	☐	☑
Germany	☐	☐	☐	☑ (tied to WMDs)	☐	☐	☐	☑
Japan	☐	☐	☐	☑ (tied to WMDs)	☐	☐	☐	☑
South Korea	☐	☐	☐	☑ (tied to WMDs)	☐	☐	☐	☑
Taiwan*	☐	☐	☐	☑ (tied to WMDs)	☐	☑	☐	☑
China**	☐	☐	☐	☑ (tied to WMDs)	☑	☑	☑	☑

*Taiwan is not an official member of any of the traditional multilateral export control regimes, but it incorporates items listed in multilateral regimes into its control lists.

**China is a member of the Nuclear Suppliers Group but not the Wassenaar Arrangement, Australia Group, or Missile Technology Control Regime.

Note: In this table, and all others in this paper, "Multilateral Regime" is defined as the Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group, and Missile Technology Control Regime.

Source: CSIS analysis of official government statements and documents.

Although allied countries do have the demonstrated ability to implement list-based controls unilaterally, it is misleading to think of their controls as equivalent to those issued by the United States. For example, no allied country has a meaningful equivalent to the FDPR, nor do they have controls on advanced node semiconductors that apply on a China-wide basis, with the **partial exception of Taiwan**. On the other hand, recent **changes** to China's export control system have given Beijing the authority to implement list-based controls that apply on both a country-specific and extraterritorial basis.

END-USER CONTROLS

Multilateral export control regimes do not have an equivalent to the U.S. Entity List. As a result, allies have far less robust end-user restrictions than the United States. For example, the European Union and its member states simply do not have **end-user restrictions** and are **forced** to use sanctions authorities to impose controls on specific entities. Table 2 summarizes the end-user control landscape.

Table 2: U.S., Allied, and Chinese End-User Export Control Authorities

	Multilateral Regime-Based				Unilateral or Plurilateral			
	Country-Specific		Not Country-Specific		Country-Specific		Not Country-Specific	
	Extraterritorial	Not Extraterritorial	Extraterritorial	Not Extraterritorial	Extraterritorial	Not Extraterritorial	Extraterritorial	Not Extraterritorial
United States	☐	☐	☐	☐	☐	☐	☑	☑
European Union	☐	☐	☐	☐	☐	☐	☐	☐
Netherlands	☐	☐	☐	☐	☐	☐	☐	☐
Germany	☐	☐	☐	☐	☐	☐	☐	☐
Japan	☐	☐	☐	☐	☐	☐	☐	☑
South Korea	☐	☐	☐	☐	☐	☐	☐	☑
Taiwan*	☐	☐	☐	☐	☐	☐	☐	☑
China**	☐	☐	☐	☐	☐	☐	☑	☑

*Taiwan is not an official member of any of the traditional multilateral export control regimes, but it incorporates items listed in multilateral regimes into its control lists.

**China is a member of the Nuclear Suppliers Group but not the Wassenaar Arrangement, Australia Group, or Missile Technology Control Regime.

Source: CSIS analysis of official government statements and documents.

While Japan, South Korea, and Taiwan all have the authority to impose end-user restrictions, their end-user authorities are more limited than the U.S. Entity List. For example, Japan's **end-user list** only contains entities involved in the development, production, manufacturing, or storage of WMDs, or certain military end-uses. No allied country has put end-user controls on Chinese AI and semiconductor firms like the United States has, at least not publicly. As with list-based controls, allied countries lag far behind China when it comes to end-user controls. For example, in October 2024, China **released** its new dual-use export control regulation, which **outlined** a U.S. Entity List equivalent. Other regulations such as the **Unreliable Entities List** also give China options to target specific actors.

END-USE CONTROLS

Multilateral export control regimes contain end-use (often referred to as "catch-all") controls related to WMDs and certain military applications. For example, the Missile Technology Control Regime **requires** members to have end-use restrictions "controlling the export of items not included on a control list when they may be intended for use in connection with delivery systems for WMD[s]." Meanwhile, the Wassenaar Arrangement contains a **"catch-all" provision** designed to control unlisted dual-use items destined for a country subject to an arms embargo and intended for "military end-use." As shown in Table 3, allied countries' end-use controls are thus confined to WMD and military applications, with the potential exception of the European Union.[2]

2 The EU Dual-Use Regulation contains an untested end-use authority related to **"cyber surveillance"** applications that is technically implemented outside of the multilateral export control regime structure.

Table 3: U.S., Allied, and Chinese End-Use Export Control Authorities

	Multilateral Regime-Based		Unilateral or Plurilateral	
	Country-Specific	Not Country-Specific	Country-Specific	Not Country-Specific
United States	☐	☑ (tied to WMDs)	☑	☑
European Union	☐	☑ (tied to WMDs)	☐	☐
Netherlands	☐	☑ (tied to WMDs)	☐	☐
Germany	☐	☑ (tied to WMDs)	☐	☐
Japan	☐	☑ (tied to WMDs)	☐	☐
South Korea	☐	☑ (tied to WMDs)	☐	☐
Taiwan*	☐	☑ (tied to WMDs)	☐	☐
China**	☐	☑ (tied to WMDs)	☑	☑

*Taiwan is not an official member of any of the traditional multilateral export control regimes, but it incorporates items listed in multilateral regimes into its control lists.

**China is a member of the Nuclear Suppliers Group, but not the Wassenaar Arrangement, Australia Group, and Missile Technology Control Regime.

Source: CSIS analysis of official government statements and documents.

In contrast, in October 2022, BIS **introduced** an end-use restriction related to the production of advanced node semiconductors in China. This move marked a major policy change, as U.S. end-use restrictions **had** previously been limited to situations involving WMDs. China also has the authority to implement end-use controls for reasons unrelated to WMDs. China's 2020 Export Control Law **provides** a catch-all for any end-use that likely would endanger "[China's] national security or national interests." These terms are left largely undefined, providing Beijing with the ability to require licenses for a very broad set of unlisted items on an end-use basis if it desires.

SERVICES CONTROLS

Allied countries surveyed in this paper only **apply** services controls for WMD end-uses. However, there is a key difference in how the United States interprets what is covered under WMDs compared to its allies. In October 2022, BIS **informed** all U.S. persons that the act of supporting the development or production of advanced node semiconductors and related equipment in China "could involve 'support' for . . . weapons of mass destruction-related end uses," and thus required a license. On the other hand, allied countries do not **consider** activities supporting the development or production of advanced node semiconductors to be related to WMDs and, as a result, do not imposes services controls on such activities. Table 4 summarizes the services controls landscape.

Table 4: U.S., Allied, and Chinese Services Export Control Authorities

	Multilateral Regime-Based		Unilateral or Plurilateral	
	Country-Specific	Not Country-Specific	Country-Specific	Not Country-Specific
United States	☐	☑ (tied to WMDs)	☑	☑
European Union	☐	☑ (tied to WMDs)	☐	☐
Netherlands	☐	☑ (tied to WMDs)	☐	☐
Germany	☐	☑ (tied to WMDs)	☐	☐
Japan	☐	☑ (tied to WMDs)	☐	☐
South Korea	☐	☑ (tied to WMDs)	☐	☐
Taiwan*	☐	☑ (tied to WMDs)	☐	☐
China**	☐	☑ (tied to WMDs)	☑	☑

*Taiwan is not an official member of any of the traditional multilateral export control regimes, but it incorporates items listed in multilateral regimes into its control lists.

**China is a member of the Nuclear Suppliers Group, but not the Wassenaar Arrangement, Australia Group, and Missile Technology Control Regime.

Source: CSIS analysis of official government statements and documents.

Despite holding a more limited view of WMD-based export control restrictions than BIS, certain allies do restrict their citizens' activities related to semiconductor manufacturing through other economic security tools. For example, according to a **report** by the Semiconductor Industry Association, South Korea has used its **Act on Prevention of Divulgence and Protection of Industrial Technology** "on numerous occasions to prevent firms transferring to mainland China technology deemed detrimental to the industrial competitive capabilities of Korean companies even in the absence of direct links to national security concerns associated with WMDs or conventional weapons." Taiwan also **restricts** its citizens and firms from supporting the Chinese semiconductor industry through a variety of regulations unrelated to its export control regime.

KEY GAPS BETWEEN U.S. AND ALLIED EXPORT CONTROL REGIMES

As demonstrated in the previous sections, allied countries possess far less expansive export control authorities than the United States. Although they are all capable of implementing list-based controls on advanced AI chips and SME, their export control tool kit is far narrower than what is available to BIS. For example, while the list-based controls announced by the Netherlands and Japan as part of a **reported trilateral deal** with the United States were a legitimate breakthrough in allied export control coordination, their controls were weaker than the U.S. regime in at least three important ways. Former Assistant Secretary of Commerce for Export Administration Kevin Wolf **summed up** these defects in his February 2023 testimony before the Senate Committee on Banking, Housing, and Urban Affairs, which is quoted below.

> [The trilateral deal does not impose] controls on activities of Dutch or Japanese citizens in support of advanced node manufacturing in China. (The new BIS rules prohibit U.S. persons from providing support, even involving uncontrolled foreign-made items, to the development or production of advanced node semiconductors in China.) It will not involve any ally imposing end-user controls such as those related to the EAR's Entity List. It will also not have controls specific to the . . . production of semiconductor production equipment in China. Thus, Japanese and Dutch companies will still be able to export to China items and services that U.S. competitor companies cannot.

It is worth adding to Wolf's point that license applications for sales of U.S.-controlled chips to China **generally face** "a presumption of denial." Thus, the U.S. policy imposes what is de jure a license requirement but de facto a ban. This is not always the case for U.S. allies. For example, in July 2023 Reuters reported that Japan's controls **would not be implemented** on a presumption of denial basis.

Only imposing simple list-based restrictions leaves allied countries vulnerable to the same failure modes that plagued earlier versions of the U.S. controls. For example, in July 2019, Japan issued an **update** to its export licensing policies, which removed South Korea from its "white countries" list of trusted trade partners and required individual export licenses for fluorinated polyimide, hydrogen fluoride, and related chemicals. A February 2023 World Bank analysis showed that in the absence of an FDPR equivalent, **Japanese firms simply relocated production** of the controlled chemicals from Japan to subsidiaries located in South Korea. While technically legal, these activities were in stark opposition to the intent of Japan's controls and greatly limited their strategic impact. Similarly, for years the United States blocked direct sales of cutting-edge chips to customers **explicitly affiliated** with the Chinese military, while allowing those same chips to flow freely to commercial entities in China. While this policy ended direct sales from U.S. companies to the Chinese military, it was mostly ineffective at stopping indirect sales to the shell companies that helped the **Chinese military** evade export controls. The October 2022 controls addressed this by implementing restrictions that applied on a China-wide basis. Without equivalent measures, there are good reasons to think that allied countries' controls will be susceptible to the same diversion risk.

The fact that the Netherlands and Japan used existing authorities to implement unilateral controls on advanced semiconductor technologies also illustrates that analysis of authorities alone yields an incomplete understanding of international semiconductor export control dynamics. Whether Japan and the Netherlands's reticence can be attributed to **poor diplomatic coordination** on behalf of the United States or a **lack of political will** on behalf of its allies is up for debate, but it cannot be entirely attributed to insufficient legal authorities. What is clear is that this delay harmed the U.S. strategic goals vis-à-vis China and its AI and semiconductor ecosystem.

The Dutch and Japanese governments announced their plans to impose controls in line with the October 2022 update in March 2023, but enforcement did not take place until July 2023 in the case of Japan and September 2023 in the case of the Netherlands. This delay allowed Chinese firms to engage in a massive stockpiling effort. According to a Financial Times analysis of Chinese customs data, the total value of Chinese imports of SME **increased from $2.9 billion** in June and July 2022 to $5 billion over the same two months in 2023. The analysis further found that "most of the imports came from the Netherlands and Japan."

The December 2024 export control update **showed** that while U.S. policymakers are providing incentives to allies to align themselves with the U.S. export control regime, they are willing to unilaterally restrict the activity of firms headquartered in unaligned countries. For example, South Korean SME and high-bandwidth memory will be restricted by the expanded FDPR even for sales from South Korea, with a possible future exemption if the country implements controls equivalent to those in the United States.

The following sections survey export control policies for the European Union, Netherlands, Germany, Japan, South Korea, Taiwan, and China.

European Union

OVERVIEW

The European Union lacks the export control authorities to compel its member states to follow U.S. restrictions on AI chips and related technologies. By the European Commission's own **admission**, the European Union "does not have the necessary legal provisions to adopt at EU level uniform export controls." Yet in the past 18 months, EU leadership has demonstrated a desire for greater involvement in the geopolitics of AI. In **November 2023**, the European Commission identified AI and semiconductors as "critical technology areas" that it would like to place restrictions on as it attempts to "de-risk" its relationship with China. Věra Jourová, one of the key proponents of the **European Chips Act**, **stated**, "Technology is currently at the heart of geopolitical competition and the EU wants to be a player, and not a playground." At the February 2025 AI Action Summit, President of the European Commission Ursula von der Leyen **reiterated** this sentiment, saying, "We want Europe to be one of the leading AI continents. . . . Too often, I hear that Europe is late to the race—while the U.S. and China have already gotten ahead. I disagree. . . . Global leadership is still up for grabs."

Russia's invasion of Ukraine sparked a major response in the form of what the EU Commission described as an "**unprecedented and rapid expansion**" of **sanctions** on military items and dual-use goods and technologies. The invasion also initiated a conversation about the role of Russia in obstructing the intended goals of the existing multilateral export control architecture. One European Commission export control strategy document **noted**, "Russia has blocked the adoption of important controls on emerging technologies in the Wassenaar Arrangement. . . . This raises serious questions on the capacity of multilateral export control regimes to deliver in times of serious geo-political tensions, and to ensure the security of the EU and the other members of the multilateral arrangements."

Russia's invasion of Ukraine also **began** a discussion among EU policymakers about what economic security tools should be used against China, especially in light of China's support for the Russian military. Furthermore, the 2021 U.S.-EU Trade and Technology Council Export Control Working Group joint statement **drew** specific attention to the "civil-military fusion policies of certain actors," a thinly veiled reference to China. For now, however, the European Union's export controls vis-à-vis Beijing remain decidedly weaker than those of the United States.

THE EUROPEAN UNION'S EXPORT CONTROL REGIME

The European Union set up its **export control regime** for dual-use items in the 1990s with a focus on preventing the proliferation of WMDs. In 2011, the European Commission **ordered** a review of its export control system to respond to demands from member states for a more flexible export control system. In 2021, **Regulation 2021/821**, often referred to as the EU Dual-Use Regulation, entered into law and governs the EU export control system as it exists today.

This regulation was **designed** to allow the European Union to better cope with "today's evolving and new security risks, rapid technological and scientific developments as well as transformations in trade and economic processes." Despite expanding the European Union's export control tool kit for dual-use

technologies, the final regulation was **significantly pared down** compared to the original draft text. The regulation allows for the following kinds of controls.

- **List-based controls:** Dual-use goods, software, and technology subject to license requirements are listed in Annex I of the EU Dual-Use Regulation. This list compiles items from multilateral export control agreements including the Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group, and Missile Technology Control Regime. Additionally, in **Annex IV of the regulation**, there is a list of high-sensitivity items that require licenses even to be transferred within the European Union. The European Union also maintains a **common list of military items**. However, this list is nonbinding, and member states are **responsible** for legislating and implementing their own controls on military items.
- **End-user controls:** N/A
- **End-use controls:** The EU Dual-Use Regulation also **includes** catch-all controls covering use cases related to WMDs, military applications, and cyber surveillance. Notably, the cyber surveillance catch-all **was** implemented outside of the multilateral regime structure.
- **Services controls:** The EU Dual-Use Regulation **imposes** license requirements on services related to three types of end-uses: "(i) weapons of mass destruction end use; (ii) military end-use in an arms embargoed country; or (iii) use as parts or components of military items exported without license or in violation thereof."

The European Union requires member states to impose authorization requirements for controlled items. These requirements are a weak tool, however. Though the European Union may require member states to impose authorization requirements, national governments may choose to approve every application they receive. The challenge posed by the European Union's narrow authorities is exacerbated by its **limited** enforcement capacity. The European Union's role in implementing its export control regime is limited to administrative support; it does not process applications, investigate noncompliance, or prosecute violators. The limitations to its export control regime are the **reason** the European Union turned to sanctions following Russia's invasion of Ukraine. While sanctions are a more agile tool than export controls (e.g., they allow for the targeting of a specific country), they require **unanimity** in the European Council to be implemented. The small set of countries and end-users **under EU sanctions** are also subject to export control restrictions.

Yet the European Union does empower its members to implement unilateral export controls on items not covered by multilateral export control regimes. Article 9 of the **EU Dual-Use Regulation** provides EU member states with a legal mechanism to implement unilateral controls on otherwise unlisted items for "reasons of public security, including the prevention of acts of terrorism," or for "human rights considerations." Member states have been exercising these authorities with **increasing frequency**, particularly for restrictions on emerging technologies. The **Netherlands**, **Spain**, **France**, **Germany**, and **Italy** have all implemented unilateral export controls in the last two years. In an attempt to preserve the single market principle, the European Union publishes national control lists which in theory allow for export control coordination at the EU level. In practice, however, potential coordination is **complicated** by insufficient consultation between states and inconsistent national-level legal frameworks.

RECENT DEVELOPMENTS

In January 2024, the European Commission **adopted** five initiatives to "strengthen the EU's economic security at a time of growing geopolitical tensions and profound technological shifts."

They include foreign direct investment (FDI) screening, improved member state export control coordination, and enhanced security around research and innovation sectors to avoid unwanted leakage. That same month, the European Commission **released** the final version of its white paper on export controls.

Despite the pivot to more aggressive economic security measures, EU leadership has expressed concern over recent U.S. export control action. For example, in response to the January 2025 AI Diffusion Framework, European Commission Executive Vice Presidents Henna Virkunen and Maroš Šefčovič **issued** a statement noting, "It is . . . in the U.S. economic and security interest that the EU buys advanced AI chips from the U.S. without limitations: we cooperate closely, in particular in the field of security, and represent an economic opportunity for the U.S., not a security risk."

Netherlands

OVERVIEW

Dutch company ASML is the world's **sole supplier** of the EUV lithography machines necessary to manufacture advanced semiconductor chips. As a result, the Netherlands occupies a key chokepoint in the AI chip value chain. Yet, for most of the 2010s, the Dutch government allowed these advanced semiconductor technologies to flow to China unimpeded. In 2019, the first Trump administration reportedly **persuaded** the Netherlands's leadership to impose limited controls on cutting-edge EUV machines by showing them classified intelligence reports about the dangers that China's acquisition of ASML's technology posed.

In October 2020, the Dutch Ministry of Defense published an **internal memo** which concluded that continued exports of advanced semiconductor technologies would increase the chance of a NATO member state having to defend itself against advanced weapons systems in the future. This document **highlighted** the key role U.S. diplomacy played in Dutch strategic thinking around semiconductors, noting, "Our most important strategic security partner, the United States, has made an emphatic appeal to the Netherlands not to export EUV technology to China."

This internal memo—along with continued discussions with the Trump and Biden administrations—prompted the Netherlands to **announce** that it would impose further license requirements for advanced SME in March 2023, bringing the government's policies in line with the U.S. October 2022 controls as part of the **reported trilateral deal** between the United States, Japan, and the Netherlands. Furthermore, the Dutch government allegedly **declined** to renew ASML's license to service and provide spare parts to its systems already in China. In September 2024, the Dutch government **announced** yet another update, this time on less advanced deep ultraviolet (DUV) lithography equipment.

Following the September 2024 controls, Dutch Minister for Foreign Trade and Development Reinette Klever **emphasized** that the Netherlands's leadership continues to view export controls on advanced SME as a significant national security priority: "I've made this decision for reasons of security. We see

that technological advances have given rise to increased security risks associated with the export of this specific manufacturing equipment, especially in the current geopolitical context."

THE NETHERLANDS'S EXPORT CONTROL REGIME

Dutch export controls on **dual-use items and technologies** are grounded in two pieces of legislation: the 2008 **Strategic Goods Decree** and the 2011 **Strategic Services Act.** Articles 2 and 3 of the **Strategic Goods Decree** refer to Annex I of the EU Dual-Use Regulation rather than maintaining a Netherlands-specific list of dual-use items subject to export controls. Article 4 of the decree refers to Article 9 of the EU Dual-Use Regulation, which permits member states to impose license requirements on items not listed in Annex I for reasons related to public security or human rights. The Strategic Services Act adopts the EU provisions on services controls. License applications are processed by the **Central Import and Export Office**.

The Dutch export control system allows for the following kinds of controls on dual-use items and technologies.

- **List-based controls:** Dual-use goods, software, and technology listed in Annex I of the EU Dual-Use Regulation or added by the Dutch government unilaterally are subject to license requirements.
- **End-user controls:** N/A
- **End-use controls:** The Dutch government enforces end-use controls through the catch-all authorities provided by the EU Dual-Use Regulation.
- **Services controls:** As an EU member state, the Netherlands implements services controls related to end-uses specified in the EU Dual-Use Regulation.

Like all EU member states, the Netherlands **primarily** controls dual-use items through Annex I of the EU Dual-Use Regulation. Similarly to a smaller subset of EU member states including **Spain**, **France**, **Germany**, and **Italy**, the Dutch government has made use of provisions in the EU Dual-Use Regulation (and its own legislation) that permit member states to implement controls outside of traditional multilateral agreements. As discussed in the previous section, the controls the Netherlands announced in March 2023 (and in **September 2024**, **October 2024**, and **January 2025**) were implemented on a unilateral basis. For example, the announcement accompanying the March 2023 export control updates **specifically referenced** the Article 9 provision of the EU Dual-Use Regulation which permits member states to "institute a ban on, or make the acquisition of a permit compulsory for exporting dual-use goods that are not specified in appendix I of the Regulation."

Unlike the U.S. restrictions, the Netherlands's controls do not specifically target China. In April 2023, then-Minister for Foreign Trade and Development Cooperation Liesje Schreinemacher **noted**, "The Dutch export control policy is country-neutral. When assessing an export permit application, considerations are made and tested against the additional strategic character for export control on a case-by-case basis, where among others the properties of the product to be exported, the use of the product, the end-user and destination country are taken into account."

However, there is increasing awareness in the Dutch policy community that China poses a significant danger. For example, in April 2023, the Dutch General Intelligence and Security Service **noted** in

its annual report that "[China] poses the greatest threat to the Netherlands' economic security . . . [through] legitimate investments, company takeovers, and academic cooperation, as well as illegitimate digital espionage, insiders, covert investments and illegal exports."

RECENT DEVELOPMENTS

On January 15, 2025, the Dutch government **announced** another export control update, due to enter into force on April 1, 2025, expanding **the types of SME subject to license requirements**. These additions are reflected in the annex to the **Regulation on Advanced Semiconductor Manufacturing Equipment** and include items such as measurement and testing equipment, as well as optimization software used in the production of advanced semiconductors. In an announcement accompanying the update, Dutch Minister for Foreign Trade and Development Reinette Klever noted, "We are observing increased security risks associated with the uncontrolled export of this specific equipment. For this reason an export authorization will henceforth be required." Consistent with previous controls, this measure did not specifically reference China. Nonetheless, this set of controls prompted an **outcry** from Beijing officials. The January 2025 controls followed unilateral measures announced in **October 2024** that covered items related to quantum technologies, semiconductors, and additive manufacturing.

The Netherlands has also recently demonstrated a desire to build a more robust economic security tool kit. For example, in June 2023 the government **announced** it was considering legislation that would require foreign doctoral students coming to the country to study in technical fields to undergo a screening process. While the announcement did not specifically mention protecting EUV and DUV lithography, these technology areas are likely the target of the proposed measure. Prior to that, in May 2023, the Dutch government **implemented** measures subjecting certain investments, mergers, and acquisitions in its semiconductor industry to review based on national security concerns.

Germany

OVERVIEW

For many years, Germany believed that robust economic relations with China would achieve ***Wandel durch Handel***, a German notion that roughly translates to "change through trade." A central tenet in German foreign policy since the 1970s, the idea **holds** that trade with authoritarian regimes can induce political change. Russia's invasion of Ukraine and China's subsequent support of the war effort **shook Germany's confidence** in the policy, as Germany's extensive trade with both countries failed to prevent violent authoritarianism from spilling into Europe. In April 2022, the European Commissioner for Economy summed up the prevailing view in Europe when he **stated** that the "notion of Wandel durch Handel, of bringing about change through trade, has shown its limitations" and that Europe needed to "rethink [its] relations with autocratic regimes."

In July 2023, Germany's Federal Foreign Office published its **Strategy on China**, further demonstrating an updated understanding of the Chinese threat. The document stated, "The Federal Government is committed to the adjustment of export control lists in international export control regimes as well as to reviewing national export control lists against the backdrop of new technological developments." It further noted that the government was "also taking China's Military-Civil Fusion policy into account in this regard." Germany also **pushed** the European Commission to adopt an EU-wide investment screening mechanism to better protect member states' economic security. This was widely **seen** as a

response to the Chinese acquisition of German robotics national champion Kuka in 2016. In its 2024 annual report, Germany's Federal Office for the Protection of the Constitution **described** China as Germany's "biggest economic and scientific espionage threat."

Despite its increasingly wary rhetoric about the threat of China to its economic security, Germany has not kept pace with the United States, at least not in terms of export controls on advanced semiconductors and related equipment. In March 2024, Bloomberg reported that senior U.S. officials **asked Germany** to block shipments of optical components produced by **Carl Zeiss**, which are needed for advanced chip production and are used in ASML's EUV machines, to China, but the German government was reluctant to act.

Germany's Export Control Regime

The legal authorities for Germany's modern export control regime come from the 2021 EU Dual-Use Regulation, as well as Germany's **Foreign Trade and Payments Act** and **Foreign Trade and Payments Ordinance**, both passed in 2013. Article 4 of the Foreign Trade and Payments Act gives the government authority to restrict foreign trade transactions in order to carry out EU controls or other member state obligations. It also stipulates that Germany can restrict exports unilaterally if doing so guarantees "essential security interests," prevents "disturbances to German foreign relations," or ensures the "public order or security" of Germany. The Foreign Trade and Payments Ordinance states that goods listed in Annex I of the EU Dual-Use Regulation are subject to export controls. License applications for listed items are processed by the **Federal Office for Economic Affairs and Export Control** (BAFA).

The German export control system allows for the following kinds of controls on dual-use items and technologies.

- **List-based controls:** Dual-use goods, software, and technology listed in Annex I of the EU Dual-Use Regulation are subject to license requirements. Items found in Part I, Section B of the German Foreign Trade and Payments Ordinance, often referred to as its national control list, are also subject to license requirements. Importantly, the national control list contains 20 dual-use items not included in multilateral agreements. In other words, it contains items Germany has put in place unilaterally. In theory, restrictions on these items apply to all countries, but German export control officials told CSIS that EU members and other allies are effectively exempt from these unilateral restrictions.
- **End-user controls:** N/A
- **End-use controls:** The German government enforces end-use controls through the catch-all authorities provided by the EU Dual-Use Regulation.
- **Services controls:** As an EU member state, Germany implements services controls related to end-uses specified in the EU Dual-Use Regulation.

Despite U.S. **pressure**, Germany has not publicly implemented China-specific export controls on advanced semiconductors. In fact, German export control officials told CSIS that they view their export control system as in principle applying to all countries. They noted that for restrictions to apply on a country-specific basis, they have to be implemented through a sanctions regime.

RECENT DEVELOPMENTS

On July 17, 2024, Germany used its **Foreign Trade and Payments Ordinance** to unilaterally add a set of items related to semiconductor manufacturing, including equipment for wafer inspection and dry etching, to its national control list. German government officials told CSIS this measure was undertaken to align Germany with the existing U.S. export control regime, and that additional unilateral controls could arrive by mid-2025.

BAFA has also undertaken a major effort to streamline its export control processing. In March 2024, the office **announced** its third tranche of policy changes in three years related to this effort. Sven Giegold, state secretary in the Federal Ministry for Economic Affairs and Climate Action, noted, "Procedural simplifications are contributing to significantly faster authorizations without compromising the scrutiny standards." German export control officials told CSIS a fourth tranche went into effect in January 2025.

Japan

OVERVIEW

In March 2023, Japan announced **plans** to **restrict exports** of 23 types of advanced SME not controlled by multilateral agreements. This measure came after a **reported deal** earlier that year between Japan, the Netherlands, and the United States. However, Japanese officials insisted these controls were not targeted toward China. Japanese Minister for Economy, Trade and Industry Yasutoshi Nishimura **stated** in a March 2023 press conference following the announcement, "We do not have one particular country in mind with these measures."

These controls underline the emerging consensus in Japan's national security community that export controls and advanced semiconductor technologies play a significant role in securing Japan's economic security. In 2021, Japan's Ministry of Economy, Trade and Industry (METI) **stated** that the goal of its semiconductor industry was "to ensure Japan remains strategically essential and strategically independent amid the conflict for technological hegemony between the U.S. and China." Meanwhile, Japan's 2022 National Security Strategy **recommended** measures to "enhance investment screening and export control as well as response [sic] to forced technology transfer, and further advancing research integrity and measures against talent drain." The 2023 Camp David pact, a trilateral agreement between Japan, South Korea, and the United States, **demonstrated** Japan's desire to work more closely with the United States on economic security issues.

Despite the March 2023 controls, Japan remains a significant supplier of SME to China. For example, in the first three quarters of 2024, **around 50 percent** of Japan's SME sales went to the country. As a result, over the past year, both the **Biden administration** and **Congress** called for Japan to further limit SME sales to China. In January 2025, Japan **issued** another export control update covering advanced semiconductor technologies, demonstrating the country's continued willingness to implement controls on strategic technologies outside of multilateral export control regimes.

JAPAN'S EXPORT CONTROL REGIME

The foundation of Japan's present-day export control system dates back to 1987 in the aftermath of the **Toshiba Machine incident**. In 1987, the U.S. intelligence community discovered that the Japanese Toshiba Machine Company was providing the Soviet Union with nine-axis propeller milling machines and related software to support the Soviet submarine program, in clear violation of the COCOM

regime. In response to pressure from the United States and allied countries, the Japanese government **implemented** significant changes to its export control regime including major amendments to the **Foreign Exchange and Foreign Trade Act** (FEFTA), first passed in 1949, and the creation of the **Center for Information on Security Trade Control** (CISTEC), a nongovernmental body dedicated to **supporting** Japan's export control system and economic security objectives.

FEFTA remains the bedrock of Japan's export control regime today and was the basis for its March 2023 and January 2025 controls on advanced semiconductor technologies. FEFTA contains two key provisions—Article 25 and Article 48—which provide the legal framework for its export control system. Article 25 states that the export of specific controlled technologies to a foreign person or country requires a license, and Article 48 states that the export of specific controlled goods requires a license. Japan enforces the following kinds of export controls.[3]

- **List-based controls:** Items specified in Attachment List No. 1 of FEFTA are subject to license requirements. Items on this list are based on multilateral agreements like the Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group, and Missile Technology Control Regime, or are added unilaterally.
- **End-user controls:** METI maintains an **end-user list** that contains people and firms potentially involved in the development, production, manufacturing, or storage of WMDs. Japanese officials told CSIS that METI also plans to create a military end-user list focused on entities that pose a military end-use diversion risk.
- **End-use controls:** METI requires exporters to **obtain a license** for any item that may "be used for the development, manufacture, use, or storage of WMD[s]."
- **Services controls:** As a member of the four traditional multilateral export control regimes, Japan has the authority to **implement** services controls related to WMD end-uses.

While Japanese export controls are largely grounded in multilateral regimes, Article 48 of FEFTA allows for **unilateral action** when the export of an item "is deemed to obstruct the maintenance of international peace and security." The Japanese government specifically **referenced** these authorities when it announced its March 2023 controls on SME.

Within METI, **three specific offices** deal with export controls and are housed in the Trade and Economic Cooperation Bureau under the Trade Control Department.

The first of these divisions, the Security Export Control Policy Division, administers export control policy and legislation and engages with international export control regimes. The second, the Security Export Licensing Division, is responsible for examining license applications and issuing licenses. The final division is the Security Export Control Administration Division containing the Security Export Inspection Office, which conducts company inspections and provides guidance for exporters, and the International Affairs Office, which engages with international export control regimes.

3 METI **divides** Japan's export control authorities into "list controls" and "catch-all controls." However, in this paper, the authorities are divided into four categories to facilitate comparison with other countries.

RECENT DEVELOPMENTS

In April 2024, METI issued an **interim report** containing recommendations for significant changes to its export control regime. According to an **English language overview** of the document published by METI, the traditional framework for export controls is at a "turning point." The report made the following four policy recommendations.

1. Review the complementary approach to the list control;
2. Establish a new dialogue framework on technology transfer between public and private sectors;
3. Explore multilayered international collaboration for agile and effective export control;
4. Streamline and prioritize export control systems and implementations in accordance with the respective levels of security concerns, etc.[4]

In September 2024, Japan **imposed** restrictions on several AI and semiconductor technologies to its control list. These included scanning-type electron microscopes and technologies used to design or manufacture gate-all-around field-effect transistor (GAAFET) structures.

Despite these actions, U.S. lawmakers have continued to **pressure** Japan to increase restrictions on chip-making equipment destined for China. In October 2024, the ranking members of the House China Select Committee, Congressman John Moolenaar (R-MI) and Congressman Raja Krishnamoorthi (D-IL), sent Japanese Ambassador to the United States Yamada Shigeo a letter requesting "urgent action to address the flow of Japanese semiconductor manufacturing equipment (SME) to the People's Republic of China (PRC)."

On January 17, 2025, METI **announced** its intention to **add 21 items to its control list** including previously uncontrolled advanced SME, further aligning its export control policy with the United States. This proposed measure prompted the Chinese Ministry of Commerce (MOFCOM) to release a statement **noting,** "For some time, certain countries have generalized the concept of national security and abused export control measures to suppress China's semiconductor industry. . . . China reserves the right to take necessary measures and will firmly safeguard its legitimate interests."

Despite this criticism, the United States-Japan Joint Leaders' Statement following the February 2025 meeting between President Trump and Prime Minister Shigeru Ishiba **noted** the two countries would resolve "to continue discussions on aligning policies to further promote and protect critical and sensitive technologies, including through export controls," showing the country's intention to continue export control coordination with the United States.

South Korea

OVERVIEW

For most of the twenty-first century, China was South Korea's biggest trading partner. During this time, South Korean AI and semiconductor companies made significant investments in China. For example, **SK Hynix** and **Samsung** invested more than $20 billion to buy or build facilities in the Chinese cities of Dalian and Xi'an in 2020 and 2021, respectively. As recently as 2022, roughly **60 percent** ($66 billion) of South Korea's chip exports went to Chinese customers, though this includes companies such as

4 The review of the complementary approach to the list control was completed in January 2025 and **added** 42 entities to Japan's end-user list.

Apple that do final assembly in China. South Korea is also the world's **largest** supplier of memory chips and holds roughly half of global DRAM capacity, according to analysis by the **Center for Security and Emerging Technology** (CSET). That same analysis found that South Korea ranks third behind China and the United States in AI patent applications and granted patents. The country has also played an important role in AI diplomacy, hosting the **AI Seoul Summit** in May 2024.

Despite its status as a global leader in strategic technologies, South Korea has been hesitant to implement strict export control measures due to its **export-led** economy and fear of retaliation from China. For example, South Korea originally **refrained** from joining the **sanctions regime** against Russia in 2014 after its illegal annexation of Crimea. However, South Korea **aligned** itself with international export controls and sanctions against Russia in March 2022, which many saw as a watershed moment for South Korea's export control approach.

The 2023 Camp David pact, a trilateral agreement between South Korea, Japan, and the United States, further **committed** South Korea to cooperation on technology and economic security issues. That same year, the United States **overtook** China as South Korea's biggest export market. On September 10, 2024, Minister for Trade Dr. Inkyo Cheong stated, "Economic security requires more than unilateral action," highlighting the government's newfound openness to implementing export control outside of traditional multilateral frameworks.

However, South Korea has yet to match its strategic thinking to concrete export control action, at least not to the same degree as the United States, Japan, or the Netherlands. In fact, the U.S. December 2024 export control update applied the FDPR to South Korean SME and high-bandwidth memory, as U.S. policymakers **determined** South Korea did not have "equivalent controls" for items specified in U.S. restrictions.

SOUTH KOREA'S EXPORT CONTROL REGIME

During the Cold War, the United States and South Korea signed a **Memorandum of Understanding on the Protection of Strategic Commodities and Technical Data** to bring South Korea in line with guidance prohibiting the export of COCOM-controlled items to communist-bloc destinations. South Korea's current export control authorities for dual-use technologies are grounded in its **Foreign Trade Act, originally passed in 1987**. In 2007, the Foreign Trade Act underwent a significant revision, establishing the Korea Strategic Trade Institute (KOSTI), which **supports** the implementation of export controls. South Korea enforces the following kinds of export controls.

- **List-based controls:** Dual-use goods and technologies **subject** to license requirements are listed in Annexes 2 and 3 of South Korea's Public Notice on Trade of Strategic Goods and Technologies. These annexes reflect control lists in multilateral agreements including the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australia Group, and the Missile Technology Control Regime.
- **End-user controls:** South Korea also maintains a **denial list**, which includes people, companies, and institutions subject to restrictions **based** on UN Security Council sanctions.
- **End-use controls:** South Korea **implements** catch-all controls on items not included in multilateral control lists but which may be intended for use in the creation of WMDs.

- **Services controls:** As a member of the four traditional multilateral export control regimes, South Korea has the authority to **implement** services controls related to WMD end-uses.

South Korea's export control system **divides** export control administration by item type across **three bodies**.

- The Ministry of Trade, Industry, and Energy (MOTIE) oversees dual-use items.
- The Defense Acquisition Program Administration (DAPA) of the Ministry of National Defense (MND) oversees military items.
- The Nuclear Safety and Security Commission (NSSC) oversees nuclear items.

In September 2024, South Korean police **arrested** two former Samsung employees for attempting to steal trade secrets reportedly worth $3.2 billion on behalf of a Chinese chip manufacturer. Industrial espionage has proven to be a major issue for Korean AI and semiconductor firms. According to the **South Korean government**, "The majority of the [industrial espionage] incidents [in 2023] involved cutting-edge semiconductor technologies, an area in which South Korean firms are among the world leaders."

South Korea has partly addressed this challenge through its national core technology list, authorized by the **Act on Prevention of Divulgence and Protection of Industrial Technology**. This act requires companies who work with one of the **76 listed technologies** to adhere to stringent facility security requirements. Furthermore, if a company intends to export a listed technology, it must obtain approval from MOTIE. Any foreign investment (including mergers, acquisitions, or joint ventures) in a company that holds a listed technology is also subject to MOTIE review. The South Korean legislature significantly **expanded the scope** of the Act on Prevention of Divulgence and Protection of Industrial Technology in January 2023. The act was **amended** yet again in December 2024 to increase protections around national core technologies.

RECENT DEVELOPMENTS

On August 21, 2024, South Korea made several important changes to its export control laws by amending the Foreign Trade Act. First, South Korea **renamed** KOSTI to the Korea Trade Security Administration. While its English acronym KOSTI remains unchanged, the new Korean title reflects the agency's expanded responsibilities including broader trade and technology security functions, and support for policymaking and industry analysis. Second, Article 19 of the Foreign Trade Act—which authorizes MOTIE to designate which goods require export licenses—added the phrase "or the equivalent multilateral export control cooperation" to the original text, which read, "in accordance with international export control regimes"

This revision was significant because previously the law only allowed compliance with control lists established by consensus among member countries of the four international export control regimes. With the revision, the Foreign Trade Act potentially allows for the addition of items that have not reached a consensus in traditional multilateral fora but are controlled by an ad hoc set of countries (such as the reported deal between Japan, the Netherlands, and the United States or a **Wassenaar minus one arrangement**). Despite these authorities, South Korea has not yet joined the Netherlands and Japan in imposing restrictions on advanced semiconductor technologies not controlled by multilateral regimes.

Taiwan

OVERVIEW

Taiwan occupies a unique position in the semiconductor manufacturing landscape. The Taiwan Semiconductor Manufacturing Company (TSMC) produces **over** 90 percent of the world's advanced semiconductor chips. Beyond TSMC, Nanya Technology Corporation (NTC), Winbond Electronics Corporation, and Macronix International are **among** the top 10 memory manufacturers in the world. MediaTek, ASE Group, and Unimicron also play important roles in other parts of the semiconductor supply chain.

The semiconductor manufacturing industry is of such strategic importance to Taiwan's national security, it is **known** as the huguo shenshan, which roughly translates to the "sacred mountain that protects the nation." In 2021, Taiwan's trade minister Wang Mei-hua **stated**, "This isn't just about our economic safety. . . . It appears to be connected to our national security, too." That same year, then - President of Taiwan Tsai Ing-wen **noted**, "Our semiconductor industry is especially significant: a 'silicon shield' that allows Taiwan to protect itself and others from aggressive attempts by authoritarian regimes to disrupt global supply chains." Morris Chang, the founder of TSMC, made this point more bluntly in a **2022 interview on 60 Minutes**, saying, "because our company provides a lot of chips to the world, maybe somebody will refrain from attacking [Taiwan]."

In addition to manufacturing cutting-edge chips for U.S. chip design companies like Nvidia, TSMC was also the linchpin of the Chinese AI and advanced technologies ecosystem in the 2010s. For example, in 2019 Huawei's first-generation Ascend 910A chip was **manufactured** by TSMC. This, at least in theory, changed in 2020 when the company officially halted its business with Huawei to comply with the first Trump administration's export controls, **causing** Huawei to temporarily "exit whole lines of business," such as its consumer smartphone operation. This action also had a **significant impact** on Huawei's revenue, which dropped 23 percent between 2019 and 2021.

However, TSMC-manufactured products continue to find their way to Chinese firms in an apparent violation of U.S. export controls. In October 2024, an **analysis** by prominent semiconductor research firm TechInsights found that Huawei's Ascend 910B chip contained TSMC-made components. In response, the U.S. Department of Commerce launched an investigation of the relationship between TSMC and Huawei. The U.S. Foundry Due Diligence Rule—which went into effect in January 2025 and imposed stricter restrictions on chip manufacturers—was **widely understood** as targeting TSMC and its illicit support of Huawei.

TAIWAN'S EXPORT CONTROL REGIME

Taiwan's current export control regime for dual-use items is governed by Article 13 of its Foreign Trade Act, originally passed in 1993. This legislation establishes Taiwan's export control program for strategic high-tech commodities (SHTC). The Foreign Trade Act allows for the following kinds of controls.

- List-based controls: Taiwan enforces **five** separate dual-use export control lists:
  - **High-Tech Commodities List for Exportation to Russia and Belarus**;
  - **Sensitive Commodities List for Exportation to North Korea**;
  - **Sensitive Commodities List for Exportation to Iran**;

    - **Export Control List for Dual-Use Items and Technology (based on the EU Dual-Use Regulation);** and
    - **Common Military List (also based on the EU Dual-Use Regulation)**.

    Taiwan also **maintains** a list of "restricted regions" subject to license requirements. These "regions" include Iran, Iraq, North Korea, China, Sudan, and Syria. China only **qualifies** as a restricted region for "12 categories of semiconductor wafer fabricating equipment for SHTC."

- **End-user controls:** The Taiwanese International Trade Administration (TITA) maintains the **Strategic High-Tech Commodities Entity List**, which inventories people and companies subject to restrictions.
- **End-use controls:** Taiwan **implements** "catch-all" controls on end-uses for which there is a risk of WMD proliferation.
- **Services controls:** N/A

TITA, housed within the Ministry of Economic Affairs (MOEA), is the **principal government organization** charged with implementing the country's export control regime. However, TITA coordinates with the Ministry of National Defense, the Ministry of Finance, and other agencies with subject-matter-specific mandates on export control enforcement matters.

Taiwan has also restricted the flow of sensitive AI and semiconductor technologies through economic security tools beyond export controls. In June 2022, Taiwan **announced** amendments to its **National Security Act** that created a national core technology list **covering** a wide range of SME including "manufacturing technology for chips (ICs) with processes of 14nm and below" and other packaging and chip security technologies. These amendments added increased protection for intellectual property related to listed technologies. In June 2022, the Taiwanese government also **announced** changes to the Cross-Strait Relations Act and the National Security Act that required employees of corporations and research institutions who work in national core technology areas or receive significant government funding to go through a strenuous review process to travel to China. Taiwan has also used its **Trade Secrets Act** to protect its semiconductor industry. For example, in May 2017, a former TSMC engineer who **shared** sensitive information with the Shanghai Huali Microelectronics Corporation was charged under the act.

Additionally, Taiwan has a robust and long-standing outbound investment screening process for transactions related to the production of advanced node semiconductors. For example, in 2002 MOEA **issued** the Operational Guidelines for Key Technology Review and Supervision of Investment in Foundry, Integrated Circuit Design, Integrated Circuit Packing, Integrated Circuit Testing, and LCD Panel Plants in Mainland China, which limit the ability of Taiwanese semiconductor manufacturers to invest in China.

To incentivize Taiwanese semiconductor firms to remain in Taiwan, the country also **amended** Article 10-2 of the Statute for Industrial Innovation, informally known as Taiwan's CHIPS Act, in March 2023 to provide tax credits to semiconductor companies to pursue research and development efforts in Taiwan. While this tax incentive scheme was not in and of itself new, the amendment to the statute tightened the eligibility requirement such that only semiconductor manufacturing firms were able to apply.

Recent Developments

Despite the robust economic security measures Taiwan has implemented, a series of incidents over the past year demonstrated that Chinese firms continue to exploit loopholes in Taiwan's export controls to gain access to sensitive semiconductor technologies. In October 2024, reporting in The Wire China found that TSMC was **manufacturing chips** for Chinese chip design company Xiamen Sophgo Technologies, which was then transferring chips to Huawei. A January 2025 teardown by TechInsights **revealed** that 5 nm chips in Huawei's L540 series of laptops were **manufactured by TSMC**, further demonstrating TSMC's far-from-perfect record of following U.S. export controls.

Other gaps in Taiwan's export control regime have also appeared. For example, an August 2024 report from the Taiwanese government-funded Research Institute for Democracy, Society and Emerging Technology (DSET) found that Chinese company Bitmain **acquired** access to controlled AI chips and related technology through a "remote poaching model." In other words, Taiwanese engineers were teleworking for Bitmain. The study determined that Chinese company Bitmain leveraged Taiwanese engineers' expertise, TSMC manufacturing, and ASE packaging to design and build controlled AI chips, without relocating any Taiwanese nationals to China.

China

OVERVIEW

In December 2024, China employed a variety of economic security tools against the United States including **banning** the export of certain critical minerals to the country, **announcing** an investigation into Nvidia on anti-trust grounds, and **adding** major U.S. defense companies to a Chinese equivalent of the U.S. Entity List. While these measures arrived in rapid succession, they were the product of more than five years of China's export control and economic security **capacity building**.

The **strategic turning point** for China's domestic semiconductor strategy came in April 2018, following the comprehensive export controls the United States imposed on Chinese telecommunications company ZTE. These controls prompted a series of Chinese government actions designed to make China less vulnerable to future U.S. export controls and sanctions, which included an **assessment** of China's most vulnerable technology chokepoints, the **stockpiling** of chips and chip-making equipment, and massive **domestic semiconductor subsidies**. While these were primarily defensive measures, China also laid the groundwork for more offensive economic security tools in this period.

In February 2019, Chinese Communist Party (CCP) General Secretary Xi Jinping **called** for the acceleration of "the construction of our country's legal system for extraterritorial application" in a speech at the second meeting of the Central Committee for Comprehensive Law-Based Governance. A little more than a year later, at the seventh meeting of the Central Financial and Economic Affairs Commission, he **stated**, "We must tighten international production chains' dependence on China, forming powerful countermeasures and deterrent capabilities based on artificially cutting off supply to foreigners." China has passed a series of laws and regulations with these two goals in mind. These **include** the **2020 Regulation on Unreliable Entity List**, the **2020 Export Control Law**, the **2021 Anti-Foreign Sanctions Law**, and most recently the **2024 Regulation on Export Control of Dual-Use Items**.

CHINA'S EXPORT CONTROL REGIME

China's modern export control regime can be traced back to the 1990s with the passage of the **Foreign Trade Law** in 1994, which focused on WMD proliferation. However, China's export control system for dual-use technologies has undergone a significant reorganization in the last six months. On September 30, 2024, China announced its **Regulation on Export Control of Dual-Use Items**. Using authorities granted in **China's 2020 Export Control Law**, this move consolidated previous rules and regulations, including

- **the 2007 Regulation on Export Control of Nuclear Dual-Use Items and Related Technologies;**
- **the 2002 Regulation on Export Control of Missiles and Missile-Related Items and Technologies; and**
- **the 2002 Regulation on Export Control of Dual-Use Biological Agents and Related Equipment and Technologies**.

Under this new regulation and previous laws, China has the following export control tools.

- **List-based controls:** The Regulation on Export Control of Dual-Use Items created a **unified** control list **combining** items on lists such as the 2023 Catalogue of Dual-Use Items and Technologies Subject to Import and Export Licenses Administration, the 2017 Export Control List of Nuclear Dual-Use Items and Related Technologies, and the 2002 Export Control List of Missiles and Missile-Related Items and Technologies. Items on this unified list are subject to license requirements.
- **End-user controls:** The new regulation also **introduced** the Control List. Similar to the U.S. Entity List, the Control List comprises people and firms that are judged to pose some kind of national security risk and are thus subject to authorization requirements and other restrictions.
- **End-use controls:** China's 2020 Export Control Law **provides** a catch-all for any end-use that could endanger "[China's] national security or national interests." These terms are left largely undefined, providing MOFCOM with the ability to require licenses for a very broad set of unlisted items on an end-use basis if it desires.
- **Services controls:** China's 2020 Export Control Law **provides** the authority to impose controls on services for any end-use that could endanger "[China's] national security or national interests."

The regulation announced on September 30 also **allows** for controls based on the destination country of a given export. In fact, MOFCOM issued a blanket ban on the export of certain critical minerals to the United States two days after the new regulation went into effect. Furthermore, Article 49 of the new regulation **gives** China the ability to impose controls on foreign-produced items located outside China if they are a direct product of Chinese technology or software. According to a **January 2025 report** by the National Bureau of Asian Research, this authority is analogous to the U.S. FDPR.

MOFCOM, in coordination with the Chinese Customs Bureau, the State Council, and the Central Military Commission, is responsible for export control coordination and enforcement functions.

Recent Developments

Since the Regulation on Export Control of Dual-Use Items entered into force, China has put its new (and previously existing) authorities to work in what is **widely seen** as a response to recent U.S. AI and semiconductor export controls. On December 3, 2024, MOFCOM **issued** a notice banning the export of gallium, germanium, antimony, and other critical minerals to the United States. The December 3 controls were particularly significant as they **marked** the first time China had imposed critical mineral export control on the United States on a country-wide basis. Two days later, MOFCOM followed these controls up by **sanctioning** U.S. defense contractors including General Dynamics, Lockheed Martin, and RTX's Raytheon under its Anti-Foreign Sanctions Law.

On January 2, 2025, MOFCOM continued its slew of restrictions against U.S. defense contractors, **adding** 28 companies to the Control List in order to "safeguard national security and interests," **including** Anduril, Raytheon Missiles & Defense, and L3Harris. This action banned the export of any dual-use items to listed companies. That same day, MOFCOM **placed** an additional 10 companies on the Unreliable Entity List, **preventing** them from doing business in China and prohibiting their executives from entering or living in the country.

The same week as the U.S. December 2, 2024, export control update, the Anti-Monopoly Bureau of the State Administration for Market Regulation (SAMR) **announced** it would investigate Nvidia for "suspected violations of Chinese anti-monopoly laws." More specifically, China's competition regulator **said** it would revisit Nvidia's 2020 acquisition of Mellanox Technologies. This is hardly surprising. China has a robust record of employing anti-trust measures in technology competition. A December 2022 **analysis** by the law firm Skadden finds that "of the thousands of deals that China has reviewed, only three (less than 0.01%) have been prohibited. . . . Nearly all of the prohibitions, conditional approvals, and abandonments over the past 10 years have occurred in the technology sectors that are important to China's national growth, such as semiconductors."

Chinese officials **have** also indicated that further retaliatory measures are coming following the Biden administration's AI Diffusion Framework and Foundry Due Diligence Rule.

Recommendations to U.S. and Allied Policymakers

There are three elements, shown in Figure 1, that must be combined for the successful implementation of export controls: authority, capacity, and will. This paper focuses on the first of these elements, authority. However, capacity and will are also crucial to the success of U.S. and allied technology competition with China. Accordingly, the recommendations in this section address all three elements.

Figure 1: The Three Elements of Effective Export Controls

For example, former U.S government officials have **said that** allied governments do "not really understand why the US Government is imposing its new China-specific controls," and "do not see the national or common security justification of the controls." Even if allied countries possessed the same export control authorities as the United States, they would also need to be convinced that using those authorities is in the best interests of their countries and international security. This clearly cannot be taken for granted.

The same is true of capacity. If an allied country has the political will and authority to unilaterally control advanced node semiconductors and related SME, ensuring compliance with the restrictions that it imposes would also require significant enforcement capacity. The United States invests considerably more resources into export control administration than allied countries, but even the United States faces significant concerns about enforcement capacity, particularly in the new administration. In fact, on February 5, 2025, U.S. Attorney General Pam Bondi signed a Department of Justice (DOJ) **memorandum** that disbanded the National Security Division's Corporate Enforcement Unit, which was "created with the goal of investigating and prosecuting corporate actors involved in sanctions evasion, export control violations, and other national security-related economic crimes." At the time of writing, the DOJ has not explained how any other part of the DOJ will perform this function or take over these critical responsibilities. Similarly, on March 2, 2025, the Treasury Department **announced** the suspension of the enforcement of the corporate transparency act which was "aimed at curbing the use of anonymous shell companies to conduct illegal financial activity."

As this report has detailed, U.S. allies have most or all of the legal authorities they would need to strengthen restrictions on export of technologies and services related to cutting-edge AI. To address the shortfall in political will, the key for the United States therefore is persuading these countries of the need for these controls and the viability of implementing them using their existing authorities. To address the shortfall in capacity, the U.S. government must persuade allies of the national security return on investment in effectively denying adversaries access to strategic technologies.

U.S. and allied policymakers should consider the following policy actions for more effective AI and semiconductor export controls.

Recommendation 1: Allied policymakers should restrict citizens' support of advanced node semiconductor production in China using existing authorities.

The Chinese semiconductor industry has been the beneficiary of technical assistance and consulting services provided by U.S. and allied individuals and corporations. For example, as noted in a **previous CSIS paper**, the Semiconductor Manufacturing International Corporation (SMIC) 7 nm chip found in the Huawei Mate60 Pro was supported by significant foreign technical advice.

In October 2022, BIS used the U.S. Persons Rule to impose controls on the activities of U.S. persons if they were in support of the development or production of advanced node semiconductors in China. This move restricted China's access to technical assistance provided by U.S. citizens and companies. To address such assistance provided by the non-U.S. persons, U.S. allies should implement equivalent controls. Imposing such controls would not require legislative changes to the export control framework of most allied countries. For example, the European Union and its member states already have the **authority** to impose controls on services related to WMD end-uses and military applications. However, EU member states have not traditionally considered the development or production of advanced node semiconductors to fall under their existing WMD restrictions. But this is a political choice rather than a

result of insufficient legal authorities. It is up to the Trump administration's national security officials to make the case to allies that a different interpretation is in their best interests. There is a clear precedent for allies changing their tune when it comes to assessing the bounds of their own economic security tool kit. Allied government officials told CSIS that following Russia's invasion of Ukraine, they used existing authorities to impose restriction on Moscow that they had previously thought would require new statutory authorities. In other words, they said they could not do something and then they did it.

Recommendation 2: Allied policymakers should create China-specific restrictions for AI chips and related technologies.

In February 2015, the U.S. Department of Commerce **blocked** Intel from selling its Xeon and Xeon Phi chips to four Chinese firms working on China's Tianhe-2 supercomputer, which was being used for military research related to nuclear weapons. The logic was straightforward. As these firms were working on Chinese military projects, they were "acting contrary to the national security or foreign policy interests of the United States." From this point forward, the Department of Commerce generally restricted U.S. firms from selling advanced node chips to customers working with the Chinese military. However, China's policy of **civil-military fusion** meant that shell companies designed to help the Chinese military evade export controls were able to access advanced chips easily. A 2022 CSET study **found** that the majority of advanced chips procured by the Chinese military **were designed by U.S. firms**, despite U.S. restrictions on military end-users. The October 2022 control **addressed** this, at least in theory, by introducing a blanket prohibition on the export of AI chips to all of China.

With the partial exception of Taiwan, U.S. allies do not have China-specific controls, or at least have not publicly stated that they have such controls. In the case of the Netherlands, their export controls on advanced SME are **explicitly** "country-neutral." There are at least two good reasons that allies might pursue this approach. First, restrictions that apply on a China-wide basis mean that allied firms miss out on valuable revenue from sales to commercial firms in the Chinese market. For example, **between 2016 and 2024**, ASML saw growth in sales of equipment to China that exceeded growth in the rest of the world. Secondly, as **demonstrated** by the recent anti-trust action against Nvidia, there are legitimate concerns about Chinese retaliation against countries who implement controls perceived to target Beijing. However, there is no reason to believe allied controls will be any less susceptible to the kinds of evasive tactics that rendered the United States' pre-October 2022 controls, which did not apply on a China-wide basis, ineffective. If allied countries are serious about restricting Chinese military end-users' access to advanced node semiconductors and related technologies, they will have to do so on a China-wide basis.

Recommendation 3: Allied policymakers should develop FDPR equivalents.

Another significant loophole in the pre-October 2022 controls was the fact that Chinese firms were accessing controlled SME, components, and spare parts from U.S. companies without a license via foreign-headquartered partners. The October 2022 controls addressed this in part through an expansion of FDPR, which prohibited foreign-headquartered firms from exporting SME made using U.S. technology to China.

While the United States made these changes over two years ago, allies are still lagging behind. In fact, all allies surveyed in this paper lack meaningful equivalents to the FDPR, limiting the effectiveness of

their restrictions on AI chips and related technologies. As previously mentioned, China added these capabilities to its export control tool kit in its new regulation. If allies must pass new legislation to create these capabilities, then they should do so.

Recommendation 4: U.S. and allied policymakers should ensure penalties for export control violations are significant enough to deter violations.

U.S. and allied semiconductor firms are among the most valuable in the world. For example, as of January 2025, TSMC had a **market capitalization** of $899 billion. Given their financial prospects, these companies have significant capacity to weather fines. As a result, there is increasing awareness in the policy community that more significant fines are needed to deter export control violations. In October 2024, Chris Miller, author of Chip War, **noted** that "governments—including the U.S. and Taiwan—need to couple stricter enforcement with larger financial penalties for violations."

This logic has also found increasing support in the U.S. government. In January 2024, then-Assistant Secretary for Export Enforcement Matthew Axelrod **described** a $300 million fine on Seagate Technology Holding as a mere "down payment," and highlighted the need for heightened penalties, saying, "You can expect to see more big-ticket corporate resolutions going forward." While acknowledgment of the gap in deterrence is an important step, more concrete action is needed. Other companies have gotten off relatively lightly for export control violations, at least compared to the revenue and profits of the illicit sale. For example, on November 1, 2024, BIS **imposed** a $500,000 fine on GlobalFoundries for shipments of semiconductor wafers to **SJ Semiconductor**, a company on the BIS Entity List. This fine only amounted to around 3 percent of the value of GlobalFoundries' shipment. Given semiconductor firms' massive financial resources, U.S. and allied policymakers should also consider jail time or personal fines for the perpetrators rather than just corporate fines.

Recommendation 5: U.S. and allied policymakers should increase spending on export control processing and enforcement functions.

Since the United States implemented its October 2022 export controls, the administration of the export licensing process and enforcement of controls has become significantly **more difficult**. BIS's licensing workload has **roughly doubled** since 2012. Yet, the BIS budget for these activities has remained **relatively flat** in inflation-adjusted terms. Furthermore, BIS's data analysis tools and other enabling digital technologies are inadequate for its broad set of responsibilities. In March 2024, in response to a question about whether BIS's data analysis tools and infrastructure were sufficient, Alan Estevez, then-Under Secretary of Commerce for Industry and Security, **responded**, "The answer to that is an emphatic no." He went on to say BIS personnel are "relying on antiquated systems for both license adjudication and enforcement work that were put in service in 2006 and 2008, respectively."

As a result, BIS must rely on private sector companies' compliance programs and due diligence efforts. In fact, the **majority** of investment in export control compliance is in commercial firms, rather than BIS. But, as noted in a **previous CSIS report,** "The primary goals of U.S. companies are generally legal compliance and maximizing profits, not determining and advancing U.S. national security interests beyond what is stated in law and policy."

Even though U.S. export license processing and enforcement capabilities are clearly not adequate for the task at hand, U.S. investment in these areas dwarfs that of its allies. For example, in fiscal year 2024, the United States **allocated** $222.4 million for BIS, almost twice the amount Germany plans to allocate to its export control office, **BAFA**, in fiscal year 2025. Export control administration and enforcement functions are at the forefront of technology competition with China. The United States and its allies must treat them as such.

Conclusion

Following the October 2022 export control update, then-Secretary of State Antony Blinken gave a speech in which **he said**, "We are at an inflection point. The post-Cold War world has come to an end, and there is an intense competition underway to shape what comes next. And at the heart of that competition is technology." This reference to the Cold War was more than a rhetorical trick. Over the last four years, the United States has repeatedly used Cold War–era economic security tools against China, such as restricting commercially developed technologies via export controls. But there is also wisdom in how the U.S. national security community thought about the role of allies in technology competition during the Cold War period relevant to policymakers today.

In 1955, the **Council on Foreign Economic Policy**, a now-defunct body created by President Eisenhower to coordinate economic policy across federal agencies, **conducted** a study titled "NATO, SEATO, and the Economic Defense Program." This study recommended merging two nascent military and economic security organizations: NATO, the transatlantic military alliance, and COCOM, the export control coordination forum. The authors concluded that the "tie in of the organizations . . . will increase the mutual understanding of the overall security effort of the free world." While this proposal was never implemented, the study contained a key insight relevant to the contemporary debate about restricting the flow of AI and advanced semiconductor technologies to China. The study notes,

> Even in the U.S., with its tremendous economic, scientific, and technological power, there was an increasing awareness that we need allies as much as allies need us. . . . More and more we look to other areas of the free world for many of the raw materials needed to supply our industry.

This is equally true for U.S. leadership in AI today. State-of-the-art semiconductors designed by U.S. firms rely on technical partners located in countries like Germany, the Netherlands, and Taiwan to be manufactured. As shown in this paper, U.S. efforts to limit China's access to the most advanced AI technology also require allied cooperation to be successful. While certain countries have made steps in the right direction, the reality is that allied cooperation on export controls has been either too slow (in the case of Japan and the Netherlands) or largely absent (in the case of South Korea).

The America First Trade Policy released on the first day of Trump's second term **called** for the "The Secretary of State and the Secretary of Commerce . . . to identify and eliminate loopholes in existing export controls—especially those that enable the transfer of strategic goods, software, services, and technology to . . . strategic rivals and their proxies." To achieve this goal and maintain the U.S. advantage in cutting-edge AI technology, the Trump administration will require both a thorough understanding of what export control authorities allied countries possess and the willingness to ask hard questions when it comes to their alignment with U.S. strategic goals. ■

Gregory C. Allen *is the director of the Wadhwani AI Center at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Isaac Goldston*** *is a research associate with the Wadhwani AI Center.*

The authors would like to thank former interns Irena Petryk, Samantha Gonzalez, and Teddy Foley for their research assistance. The authors would also like to thank Sadie McCullough, William Reinsch, Jack Chang, Jack Hung, Wonho Yeon, Jeremy Chih-Cheng Chang, Sebastian Bennick, Kevin Wolf, and Chae Soohong, as well as a variety of government officials who wish to remain anonymous for their helpful feedback on earlier drafts of this paper.

This report is made possible by generous support from the RAND Corporation.

The views expressed in this document are those of the authors and do not necessarily reflect RAND opinion.

Cover Photo: liangpv via GettyImages