Working Paper for the Penn Project on the Future of U.S.-China Relations

Updating Export Controls in US-China Competition: Countering China with Allies

Martin Chorzempa, Peterson Institute for International Economics

One of the most consequential policy choices the new Trump Administration and Congress will make is on the US approach to technology competition with China, encompassing measures to protect strategic technology and promote innovation at home. Export controls have been the main tool for the protect side, and President Trump has ordered agencies to "review the [US] export control system and advise on modifications" in one of his first executive orders. The first Trump Administration pioneered new uses of export controls against China with its controls on Huawei, and the Biden Administration built on this by restricting exports to hundreds more Chinese entities, imposing new controls aimed to cut all of China off from advanced chips for AI, and expanding authority beyond US borders to restrict exports from places like Taiwan. The stakes are even greater due to DeepSeek's recently demonstrated advances in China's development of advanced models for Artificial Intelligence (AI), which raise many questions about the US approach until this point.

The controls respond to real security concerns and foreign policy interests, and many have imposed major costs on their targets. Most aimed at China are targeted to slow its access to US technology that could be used for military modernization, development of AI, or human rights abuses in Xinjiang, as well as preventing diversion of US technology to adversaries like Russia and Iran. Yet other controls are less effective and some can be counterproductive, in part due to insufficient resources including outdated technical and data infrastructure. A relatively small investment in better technology would help achieve the new administration's objective of pushing for greater government efficiency. Modernizing export control systems would not only make controls more effective and efficient, e.g. by enabling more partially automated systems to detect loopholes and diversion by China and Russia, but also benefit US industry's competitiveness at no cost to security by reducing the administrative hassle of complying with export controls, such as getting faster responses from a more automated licensing system and updating clunky interfaces.

This paper distills lessons from history and today and provides actionable recommendations for export control policy. Historical experience should temper expectations for what controls can achieve due to the generally weak record of economic sanctions to achieve ambitious objectives, the difficulty of maintaining multilateral coalitions for export controls even when there is more of a security consensus than there is today on China, and the risk of relying on extraterritorial measures that require international buy in to enforce. Key recommendations include:

- Keeping control thresholds dynamic to follow changes in technology, drawing lines that are defensible and credible rather than trying to control technologies that are

becoming commodified far from cutting edge. This would concentrate limited resources on controls that are more likely to have an impact on adversaries.

- The US should also provide funding to expand technical and economic expertise at the bureau of the Commerce Department that is responsible for dual use export controls and modernize its currently extremely outdated technology that hampers its ability to head off circumvention, evaluate controls' effectiveness, and automate processes that waste valuable staff time.
- The US should spearhead an initiative to update how export controls are coordinated across countries to address new threats, a mechanism that would help the US build consensus and better implement more leakproof multilateral controls
- Washington needs to take into account increasing Chinese retaliation for export controls, including reassuring much more vulnerable allies that the US is taking seriously their concerns and the risks to their economies of going along with US controls on China that have or could expose them to retaliation.

Even during the Cold War, when the United States and its allies had a strong security consensus underpinning controls on the Soviet Union and its allies, it was challenging to maintain support for controls. Sanctions strategy needs to learn from the past, especially because evaluations of economic sanctions, including export controls, have found that they often fail to achieve their objectives.

The US has used export controls extensively since the first Trump Administration. More technologies and large firms are subject to restrictions, controls are more complex, and they apply also to sales outside the United States that the US cannot supervise directly. Yet, the implications of using this tool so extensively has been understudied due to the need to combine both analysis of the laws with technical knowledge of the controlled technologies/goods and understand how they affect globalized supply chains.

In addition, while Congress and two administrations have rightly elevated the importance of export controls, they have expanded as a largely unfunded mandate.[1] If the United States wants effective controls, it should invest in giving the Commerce Department's Bureau for Industry and Security (BIS) the technology and skilled experts it needs to quickly shut down Chinese efforts to circumvent controls and identify new chokepoints.

The United States, while strong in many areas of technology, cannot go it alone on controls. History shows that unilateral controls tend to be counterproductive in the long run, even if the US is the monopoly provider of the technology it is trying to keep from China. To get allies on board and set defensible lines, those lines may need to be less strict than US policymakers would prefer, but it is better than setting unrealistic goals that China can get around.

---

[1] Allen, Gregory C., Emily Benson, and William Allan Reinsch. 2022. "Improved Export Controls Enforcement Technology Needed for U.S. National Security." Center for Strategic and International Studies. November 30. https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security.

The US also needs to ensure that it is devoting not only time and resources to new controls but to decommissioning old ones, fitting with the new Trump Administration's avowed goals of cutting outdated regulations. The iPhone in our pockets contains technology that would have been strictly export controlled as a supercomputer not that long ago.[2] Cryptography, for example, used to be a highly secret military competency triggering strict controls, but now encrypted messaging apps are ubiquitous. As technology advances, goods that merited control in the past as advanced defense articles can become so widely available, including from foreign sources, that controlling them would be neither possible nor fruitful. Outdated controls that stay on the books are detrimental to security by wasting scarce enforcement and compliance resources away from the controls that make a difference, while burdening US firms with red tape that put them at a competitive disadvantage.

The new administration and lawmakers have space to make export control strategy more effective at achieving policy goals at manageable cost by ensuring controls are strategically targeted, sufficiently resourced for smart design and enforcement, and coordinated with allies.

What are Export Controls?

Export controls regulate not only the export of goods from the United States but also their re-export once abroad; transfer of sensitive information; and even in some cases goods made abroad that are the "direct product" of US technology. Anyone who has left the United States with luggage has complied with export controls, which is easy thanks to the aptly named BAG license exemption[3] that excuses travelers from having to ask the government for a license to temporarily export toothpaste. Most trade is like this travel, falling under exemptions that allow exporters to make sales abroad without any compliance burden. Yet, firms in sensitive sectors like defense have always had to comply with strict export controls on munitions, chemical and biological weapons, and nuclear technology, and these firms generally know that China is off limits for sales because United States imposed an arms embargo on China after the Tiananmen Square Massacre in 1989.

However, stricter controls now apply to new types of goods, technology, and customers, especially related to China. Most relate to "dual use" goods that are neither purely defense nor purely civilian goods, which are the focus of this analysis. Dual use controls are the most interesting due to the rise of civilian technology like drones and artificial intelligence models trained on commercial chips with implications for national security. When goods for defense and consumers are clearly differentiated, the government can write regulations controlling the relatively small amount of defense goods without much impact on the consumer economy.

---

[2] Wolf, Kevin. 2022. "Remarks on Chad Bown Trade Talks Podcast 170: National security, semiconductors, and the US move to cut off China." November 2. https://tradetalkspodcast.com/wp-content/uploads/2022/11/Episode-170-Transcript-Complete.pdf.

[3] Code of Federal Regulations. 1996. "Title 15, Subtitle B, Chapter VII, Subchapter C, Part 740. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740/section-740.14.

However, controls become much more difficult and costly to design and implement when trying to control goods that are mass produced for consumer markets. The more of a good is floating around consumer markets in large volumes, versus tightly controlled military supply chains, the harder it is to stop China's military from obtaining it. But if the US shuts off civilian purchases for China as a result, it may block enormous volumes of harmless consumer sales for every military sale it prevents, resulting in an exorbitant cost per denial. Trying to deny it may also be fruitless, as China's military may be able to obtain its limited needs by smuggling the goods in from third countries.

The Commerce Department's Bureau of Industry and Security (BIS) is responsible for US dual use export controls, contained in the Export Administration Regulations (EAR). The EAR is a complex set of rules determining which goods, technology, or data can be exported or transferred to different countries, entities, or types of end use or user (military or civilian). Some exports, like consumer goods to a US ally, have low compliance burdens. Others, such as an advanced gaming chip that could be used for AI purposes, may require the exporter to notify BIS before export. Still others may require a license before export, which may be approved case by case (such as less advanced semiconductor equipment for China's leading chipmaker) or presumed denial (such as advanced semiconductor equipment to China). Presumption of denial generally tells an exporter not to bother wasting its and BIS' time even trying to get permission to export it.

Policymakers choose whether to apply controls to specific Chinese "entities" like individuals, firms or research centers or to apply them to the entirety of China. The first Trump Administration primarily focused on the former. It applied an existing export tool called the Entity List to cut off 384 new Chinese entities including Huawei, one of China's largest technology companies, from buying goods and technology from the US.[4] The Biden Administration added significantly more (Chorzempa, Lovely, and Wan 2024), but also added multiple rounds of controls that try to cut off all of China from the most advanced chips and chipmaking equipment. Firm-specific controls are more targeted with less collateral damage, but the trade-off is that a Chinese firm like Huawei may convince another Chinese firm to buy the goods for it, blunting their effectiveness.

Typical export controls restrict export from the United States of goods made in the United States. However, they also by necessity extend beyond US borders, where enforcement is more challenging and international cooperation is crucial. US controls also control re-exports to ensure that, for example, a banned export to China cannot become legal by first sending it to Kyrgyzstan and then re-exporting to China. There are also "de minimis" rules that control goods abroad containing a certain amount of US content. These ensure that a banned export, for

[4] Entities can be added to the list when they are deemed to have acted against the national security or foreign policy interest of the United States. The "End Use Review Committee" (ERC) that determines which entities are listed or de-listed is chaired by BIS with representatives from the Departments of State, Defense, and Energy.

example a machine tool to Russia, could not become legal by sending the good to China, bolting on another part, and then exporting that.

The most ambitious export controls invoke Foreign Direct Product Rules (FDPR), in which the US claims extraterritorial jurisdiction over goods made outside the United States if they are the "direct product" of certain US goods or software. For example, one FDPR makes it illegal for certain semiconductors made in Taiwan with US-origin software and chipmaking equipment to be exported to Huawei.

What Makes a Control "Effective"

Export control effectiveness and costs must be evaluated against their policy goals. The many types of goals, some of which are economic, some related to security, and others related to human rights, none of which are easy to quantify, make it difficult to evaluate China controls. Generally, export controls are designed to influence foreign behavior in support of US foreign policy and national security objectives. They can:

- Coerce policy change
- Deter additional aggressive acts
- Punish crimes and aggression
- Limit and erode the target's military and strategic capabilities
- Signal, at home and abroad, resolve to confront/oppose military and other actions

Deterrence can come if a Chinese actor, whether the state deciding whether to invade Taiwan or a technology firm weighing whether to work with its military, decides not to do so due to the risk that US export controls or other sanctions imposed in response will inflict pain.

Yet, no matter the goal, the most important question is whether a control has or could deprive the controlled party of a specific good or technology. For example, the deterrent effect of US export controls on a Chinese firm only has teeth if it relies on inputs from the United States. If China or Huawei, for example, can obtain the controlled technology from another supplier with minimal delay or cost, the control is generally worse than useless. China still obtains the technology it needs, but US firms are deprived of revenue and market share that benefits a competing firm in another country. This situation also has a negative security implication because it implies reduced Chinese dependence on the US and thus US deterrent power. It would also harm US intelligence, which would lose the knowledge of Chinese capabilities and vulnerabilities that comes from the US being its supplier.

These factors need to be considered for controls on Chinese entities which have primarily non-economic value, such as demonstrating US concern for human rights. If a firm that does not rely on US inputs is entity listed, it may not suffer and instead wear the listing as a badge of honor in China. There is preliminary evidence that on average, listed Chinese firms in the IT

industry benefit from additional government contracts designed to offset the impact of sanctions.[5]

Denial is also a dynamic concept: refusal of US technology could be effective initially due to large costs of substituting non-US technology, but ineffective over time as alternative suppliers can be identified or developed. The long-term effectiveness of economic sanctions depends on the United States and US firms being so firmly in the lead that they are indispensable to global economic networks, providing leverage that can force other countries to cooperate. Even the toughest sanctions cannot work if China can evade them.

How and Why Export Controls Are Used Against China

China has become a primary target for US export controls as US-China relations have deteriorated and China has become more assertive, more technologically advanced, and more able to challenge the US strategically. Lines between the public and private sectors have blurred in the last decade, making it more difficult to tell whether a Chinese firm is ordering sensitive technology for its commercial reasons or for the government. President Xi exhorted China in 2022 to "coordinate strategies and plans, align policies and systems, and share resources and production factors between the military and civilian sectors"[6] This military-civil fusion (MCF) goal in China rings alarm bells in Washington, even if it has had limited success in enlisting Chinese private firms to help China's military so far.[7] Its ambitions to do so, nevertheless, complicate more tailored approaches to export controls. Export blacklists for companies linked to China's military are not useful if they end up being a whack-a-mole of new subsidiaries and firms obtaining technology that could be transferred to the military.

While the Obama Administration added 127 Chinese entities to the Entity List, only 21% of its additions from all countries, the first Trump Administration added 384, 58% of the total listings. Targets under Trump's first term were both more numerous and larger, newly targeting some of China's largest technology companies, including ZTE and Huawei. China's support of Russia has also made it a target. According to the Center for New American Security, 122

---

[5]Lu, Jualu. Sanction Busting via Industry Boosting: How China Strategically Counteracts US Sanctions on Chinese Firms. Working Paper. November 4, 2024. https://www.dropbox.com/scl/fi/k6edz5yo1jmfj0b475vs8/USsanctionChina.pdf?rlkey=no5eu3okuuzd5b8q7s3zu2tk8&e=3&st=7p4262o9&dl=0.

[6] Xi, Jinping. 2022. "Full text of the report to the 20th National Congress of the Communist Party of China." October 25. Available at: https://web.archive.org/web/20230316060946/https://www.fmprc.gov.cn/eng/zxxx_662805/202210/t20221025_10791908.html.

[7] Kania, Elsa B. and Lorand Laskai. 2021. "Myths and Realities of China's Military-Civil Fusion Strategy" Center for a New American Security. January 28. https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.

Chinese entities have been added to export control lists for assisting Russia in its war in Ukraine.[8]

Trump Pioneers Export Controls as Key Tool

The first Trump Administration stepped up use of these tools. starting with ZTE, a major Chinese telecommunications company caught violating US export controls and sanctions by selling equipment with US technology to Iran and North Korea. In early 2018, the US hit ZTE's with a denial order for US goods and technology. A deal between President Trump and Xi Jinping lifted the order only after ZTE agreed to pay fines and submit to US government supervision.[9] At least in this case, there were both carrots and sticks, removing restrictions once behavior changed.

In 2018, concerns about China's acquisition of US technology led Congress to update export control laws, which tasked BIS with identifying "emerging and foundational" technologies to control. The legislation required BIS to make controls multilateral or consider dropping them—recognizing unilateral controls were unlikely to work in the long term.

Semiconductors have always been a key theme of US controls. In October 2018, Chinese memory chipmaker Fujian Jinhua was put on the "entity list" after it was accused of stealing designs from US-based Micron and convincing a Chinese court to ban some of Micron's products from China.[10] The case argued that the intellectual property theft "threatens the long term economic viability of U.S. suppliers of these essential components of U.S. military systems." It marked a new use case for the entity list, which tended before to be used only in cases in which the US goods risked being diverted to destinations like Iran.

In May 2019, the US added Huawei, a globally important provider of devices like telecoms infrastructure and smartphones, to the entity list after it was indicted in US court for its dealings with Iran. The move caused immediate chaos. Firms across the US from chipmakers to software providers had to rapidly familiarize themselves with complex US export control laws and their supply chains. Then, the US government partially reversed course days later, issuing a "temporary general license" to allow some continued shipments to Huawei.

The Huawei controls illustrate the challenges of export control policymaking. Under the initial rules, foreign multinationals and even US firms who made their products outside the US could keep legally selling to Huawei. Firms using US parts were incentivized to move their

---

[8] Hume, Eleanor and Rowan Scarpino. 2024. "Sanctions by the Numbers: Comparing the Trump and Biden Administrations' Sanctions and Export Controls on China." Center for a New American Security. October 23. Available at: https://www.cnas.org/publications/reports/sanctions-by-the-numbers-comparing-the-trump-and-biden-administrations-sanctions-and-export-controls-on-china.

[9] Swanson, Ana. 2018. "Trump Strikes Deal to Save China's ZTE as North Korea Meeting Looms." New York Times. June 7. Available at: https://www.nytimes.com/2018/06/07/business/us-china-zte-deal.html.

[10] Lawder, David. 2018. "U.S. restricts exports to Chinese semiconductor firm Fujian Jinhua." Reuters. October 30. Available at : https://www.reuters.com/article/us-usa-trade-china-semiconductors/u-s-restricts-exports-to-chinese-semiconductor-firm-fujian-jinhua-idUSKCN1N328E.

production abroad to reduce US content so they could legally sell to Huawei despite the restrictions. Huawei continued to get the inputs it needed and was largely unscathed, while US firms took the brunt of the damage by losing out on sales to foreign rivals. To fix the loophole, the US escalated in August 2020 with a Foreign Direct Product Rule (FDPR) that barred certain chips like those for 5g made anywhere in the world from sale to Huawei if they were made with US equipment—which is ubiquitous in global semiconductor supply chains from Beijing to Seoul, Tokyo, and Taipei.[11] This time, the US dealt a serious blow to Huawei, but the company has continued to survive, and even is building out much of Germany's 5G networks.[12] The first Trump Administration's successful campaign to get the Dutch government to ban sales of ASML's most advanced chipmaking equipment in late 2019 were an exception to the rule that other countries have refused to go along with US controls.

Biden: Continuity with More Outreach

The Biden Administration built on the first Trump Administration's approach, adding more controls applying to all of China, more extraterritoriality, and more systematic attempts to convince others to adopt similar controls, which has had mixed results. The global response to Russia's invasion of Ukraine was a watershed for export controls, breaking taboos in countries, especially in Europe, that traditionally were loath to impose export controls beyond those adopted by the multilateral Wassenaar Arrangement. The US made a deal: countries that imposed similar controls to the US were exempt from an extraterritorial Russia FDPR.

The resulting coalition of over 30 countries including even Singapore and Switzerland went beyond the traditional focus on weapons to more economic controls aimed to hit the economy that fueled Russia's war machine, leading initially to a collapse of Russian imports.[13] Yet even this coalition of most producers of advanced technology failed to bring Russia's economy to its knees or force it to end the war—a stark lesson when considering the potential long-term effectiveness of more draconian controls on China.

Broader Chip Controls

On October 7th, 2022, the Biden Administration took aim yet again at China, but unlike with controls on Russia, it acted alone. The US supplies around 44% of semiconductor manufacturing equipment globally and most design tools, giving it unique chokepoints for at least temporarily effective unilateral controls. The controls are aimed to cut off the sale of super

[11] The Economist. 2023. "The history and limits of America's favourite new economic weapon." February 8. https://www.economist.com/united-states/2023/02/08/the-history-and-limits-of-americas-favourite-new-economic-weapon.

[12] Marsh, Sarah. 2022. "Germany ups reliance on Huawei for 5G despite security fears -survey." Reuters, December 16. Available at. https://www.reuters.com/technology/germany-ups-reliance-huawei-5g-despite-security-fears-survey-2022-12-16/.

[13] Chorzempa, Martin. 2022. Export controls against Russia are working—with the help of China. Peterson Institute for International Economics Realtime Economics Blog. June 27, Available at: https://www.piie.com/blogs/realtime-economic-issues-watch/export-controls-against-russia-are-working-help-china.

high end chips used for artificial intelligence and supercomputing applications with a new FDPR, and hobble China's attempt to produce more advanced chips itself—which could over the long term neuter US leverage, supplant chip producers abroad, and supply China's military. The US tried to tailor its controls to chips' used for "weapons of mass destruction, hypersonic missiles, autonomous systems, and mass surveillance."[14] They also avoided controls that would disrupt the supply chains for mature semiconductors, which China produces.

No other countries joined the controls initially, despite some shared threat perception around China and advanced semiconductors and that only two other countries, both US security allies, needed to join to cut China off from advanced semiconductor manufacturing equipment. The Netherlands and Japan did adopt similar controls eventually, but the Japanese controls did not take effect until July 2023 and Dutch controls in September, so China could stock up on non-US equipment for nearly a year after US controls took effect.[15] Their controls also lacked the strength of US controls, not including key provisions restricting their citizens from helping China advance its semiconductor manufacturing.[16]

In October 2023 the Biden Administration significantly ramped up its controls to address perceived leaks and ensure that larger quantities of less advanced chips could not help China reach the same AI/strategic goals. The new rules, outlined in hundreds of pages, applied controls not only to exports of advanced chips to China, but also exports to Chinese firms located anywhere in the world and to countries perceived as a risk of diversion to China. They also lowered the performance threshold for chips that would be restricted, widening the gap between what China could obtain from US sources and those on the cutting edge. The semiconductor controls are the most complex export controls ever created, running into hundreds of pages.

Whether the controls are working is hotly debated, and the record is mixed. Huawei's chip sourcing challenges due to controls have led its revenue to decline 18% in 2023 from 2019 levels, but it has become more profitable and is producing both 5g devices and advanced AI training chips.[17] SMIC, China's leading chipmaker, is producing 7 nanometer logic chips including for Huawei. While supply seems still constrained and the production may not be economical due to high failure rates, the controls had aimed to freeze China at the less advanced 14/16 nanometer level. Without extreme ultraviolet lithography equipment only produced in the

---

[14] Sullivan, Jake. 2022. "Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy" October 13. Available at: https://web.archive.org/web/20250117021326/https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy/.

[15] Haeck, Peter and Barbara Moens. 2023. "Dutch cozy up to US with controls on exporting microchip kit to China." Politico, September 1. Available at: https://www.politico.eu/article/the-netherlands-limits-chinese-access-to-chips-tools-asml/.

[16] Reuters. 2023. Japan, Netherlands to join U.S. in restricting chip equipment exports to China, Bloomberg reports. January 27. Available at: https://www.reuters.com/technology/japan-netherlands-join-us-china-chip-controls-bloomberg-2023-01-27/.

[17] Huawei Technologies Co., Ltd. 2025. "Financial Highlights." *Huawei Investor Relations*, accessed January 28, 2025. Available at: https://www.huawei.com/en/bond-investor-relations/financial-highlights.

Netherlands, which China cannot purchase, China may be unable to advance its logic chip production any further though.

When it comes to AI, Chinese firms have put significant efforts into smuggling[18] in chips that are illegal to sell to China, and despite facing shortages of the best AI training chips due to controls, Chinese firms have produced large language models that are near the top of international rankings.[19] They can also rent access to chips outside China, which is happening at increasing scale.[20]

Resource Constraints Are Acute

Expanded export controls under the first Trump administration and Biden administration have put the system for administering and enforcing export controls under serious strain. BIS processed 40,765 license applications in its 2022 fiscal year, a 19% increase over Fiscal Year 2020.[21] The increase in licenses understates the workload increase. The effort required to counter well-resourced circumvention efforts by China and Russia on the wide swath of controlled exports and entities does not necessarily involve the controlled entities applying for licenses they know will be rejected. Yet, the budget for export control administration and enforcement has been flat for years, as figure 1 shows.[22] Export administration within BIS has only 216 full time equivalent staff and enforcement has 240.[23]

---

[18] Fist, Tim and Erich Grunewald. 2024. Preventing AI Chip Smuggling to China
A Working Paper. Center for a New American Security. October 24. Available at: https://www.cnas.org/publications/reports/preventing-ai-chip-smuggling-to-china.

[19] Ding Jeffrey and Jenny W. Xiao. 2023 ":Recent Trends in China's Large Language Model Landscape." Center for the Governance of AI. April. Available at: https://cdn.governance.ai/Trends_in_Chinas_LLMs.pdf.

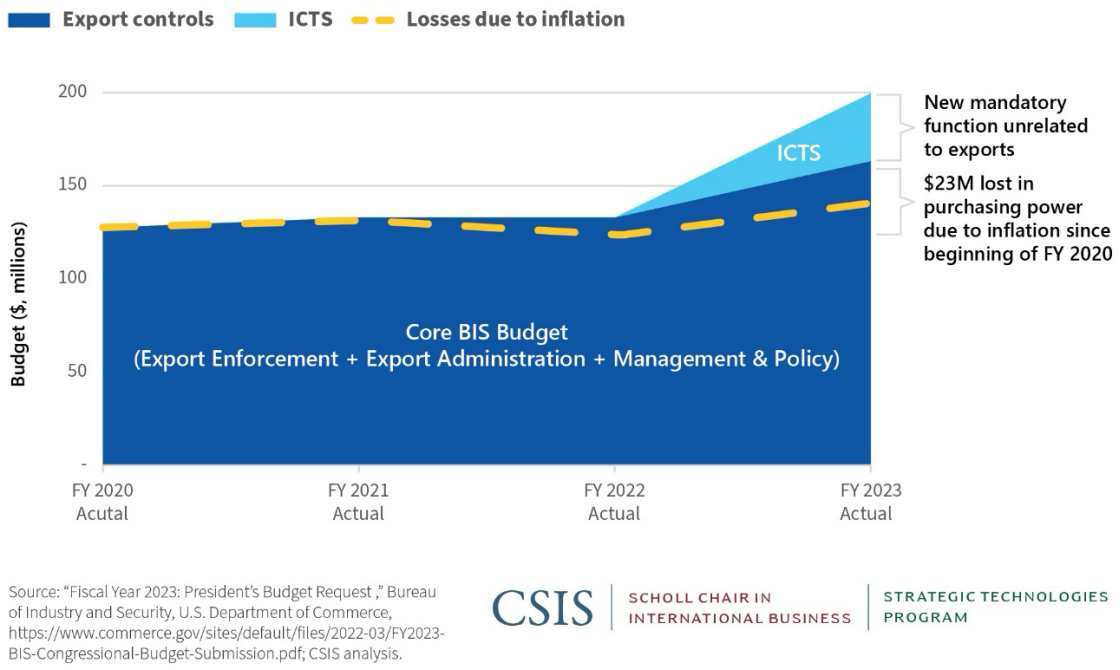
[20] Liu, Qianer and Juro Osawa. 2024. "ByteDance Planned to Spend $7 Billion on Nvidia Chips Next Year." *The Information*, December 30. Available at: https://www.theinformation.com/articles/bytedance-planned-to-spend-7-billion-on-nvidia-chips-next-year.

[21] Bureau of Industry and Security. 2023. "FY 2024 President's Budget Request." *U.S. Department of Commerce*, March. Available at: https://www.commerce.gov/sites/default/files/2023-03/BIS-FY2024-Congressional-Budget-Submission.pdf.

[22] The CSIS analysis from which this graph is sourced notes that a large increase in 2023 budget for BIS is mostly for a new program to secure the supply chain for information/communication technology, which is not related to export controls. https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security.

[23] [23] Bureau of Industry and Security (BIS). 2024. "FY 2025 President's Budget Request." *US Department of Commerce*, March. Available at: https://www.commerce.gov/sites/default/files/2024-03/BIS-FY2025-Congressional-Budget-Submission.pdf.

Figure 2: BIS Budget Annual Budget by Function



Source: Allen, Gregory C., Emily Benson, and William A. Reinsch. 2022. Improved Export Controls Enforcement Technology Needed for U.S. National Security. https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security

The technology systems required to derive data insights for smart enforcement, for example discovering networks of related entities or translating documentation that often would be in Chinese, is also antiquated. It currently takes 59 hours, more than two days, on current BIS systems to simply search for entities of interest and get data on shipments to those entities, the kind of daily activity for analysts wanting to disrupt Chinese smuggling efforts, for example.[24]

Lessons from the Past

The Cold War provided far different conditions for effective export controls than the situation with China today, but it yields rich lessons for the present. The United States was dominant in technology, industry, and the size of its economies, allies were aligned in their perception of the Soviet Union as a security threat, and the revenue foregone by prohibiting sales of strategic goods was limited due to the economic weakness and relative isolation of the Soviet

[24] Bureau of Industry and Security (BIS). 2024. "FY 2025 President's Budget Request." *US Department of Commerce*, March. Available at: https://www.commerce.gov/sites/default/files/2024-03/BIS-FY2025-Congressional-Budget-Submission.pdf.

Union and *its* allies, and it was still challenging to have effective controls. However, reviews of the export control system and other sanctions imposed at the time reveal patterns that can guide policymakers to controls that are more likely to be effective.

Literature on Export Controls

Comprehensive analyses on the effectiveness of economic sanctions, including export controls, show they generally fail to achieve their stated objectives. Hufbauer et al. (2009) have found that sanctions episodes contributed at least modestly to the achievement of publicly stated foreign policy goals or reduced target military capacity in about one-third of the cases they analyze. Success was more likely for sanctions with modest ambitions to change minor policies of the target regime. Sanctions have not tended to impose large costs on countries imposing the sanctions because their targets have tended to be small, less advanced countries, but such costs would be more salient for large targets like China. The same analysis found that autocracies are better at withstanding sanctions pressure than democracies, recommended that coalitions of sanction-imposing nations be kept small to minimize coordination challenges, and that extraterritorial sanctions (as the United States is applying against both China and Russia through the Foreign Direct Product Rule) rarely work.[25] Many of their findings suggest that success for ambitious sanctions on a target like China will be an uphill battle.

Golden Age of Export Control Coordination

After World War II, the Coordinating Committee for Multilateral Export Controls (COCOM) limited the flow of advanced technology to the Soviet Union and its allies, including China. COCOM members coordinated on the types and levels of technology to control, but for the most sensitive goods, other members could veto an export to ensure that firms in one country could not undermine collective security by making sales other countries refused. Allowing another country such power over one's exports, typically the decision of sovereign nations, was only possible with a great deal of trust that this power would be used fairly and judiciously.

However, even under these ideal conditions for controls, effectiveness was spotty and relationships strained. In the Toshiba-Kongsberg incident, for example, a Japanese and Norwegian firm violated controls to help the Soviet Union develop advanced propellers for submarines that US sonars had more difficulty detecting.[26] The United States was more hawkish than other members in restricting exports, which led to mounting frustration with the system that reduced other members' willingness to comply with it.[27] Other countries and firms undermined

---

[25] Hufbauer, Gary, Jeffrey J. Schott, Kimberly Ann Elliot, and Barbara Oegg, *Economic Sanctions Reconsidered*, 3d ed. (paper) (Washington: Peterson Institute for International Economics, June 2009).
[26] Bown, Chad P. 2020. "Export Controls: America's Other National Security Threat." **Working Paper 20-8**, Peterson Institute for International Economics, May. Available at : https://www.piie.com/sites/default/files/documents/wp20-8.pdf
[27] Mastanduno, Michael. "Economic Containment: Cocom and the Politics of East-West Trade." Cornell Studies in Political Economy. 1992.

the system's purpose by, for example, reclassifying some sales as less sensitive ones so the US could not veto them.

As the cold war faded with the Soviet Union's dissolution, the security consensus required to sustain COCOM fell apart. European countries were eager to take advantage of newly opened markets in countries that no longer appeared to be security threats, including China. COCOM was dissolved in 1994 and replaced by the Wassenaar Arrangement in 1996, which only coordinates on lists of what items/technology are controlled that members can implement as they choose. The other countries this time would not agree to a US veto power. Rather than shared goals of holding back specific countries or blocs of countries with a shared strategy of economic containment, the regime is based on a narrower goal of avoiding proliferation of dual use goods and arms. Cooperation may be shallower, but Wassenaar's breadth of membership is wider, even including Russia to ensure coverage of major arms exporters. Russia's membership creates serious complications for Wassenaar today, as Russia has become one of the main targets for export controls and thus has been stonewalling updates to control lists.

Policy debates in the 1990s centered on tradeoffs relevant to today. While "control hawks" wanted stricter controls on China, a "run faster" coalition believed that tighter controls in many cases would be counterproductive, depriving US firms, including those in the defense industrial base selling their best products to the Pentagon, of revenue they needed to invest in R&D and stay at the cutting edge.[28] In that period, the Defense Department as a result favored *looser* controls on China so its contractors could use those sales to fuel their own advances.[29] According to a US risk assessment, stricter controls in one now famous case caused the US global share of satellite exports to decline "while doing nothing to protect" the technology."

The COCOM era and its aftermath suggests that controls are never airtight even under the best of circumstances, extraterritorial use of US authority too far beyond what other countries can accept erode the legitimacy and effectiveness of cooperation, and that multilateral controls cannot be sustained without a strong security consensus.

Controls are More Challenging Today

The geopolitical and economic world today makes it more difficult to impose effective export controls on China than it was for COCOM-era controls on the Soviet Union. The United States has less weight in the world economy and technology; BIS has suffered from insufficient investment, skills, and outdated technology; increased innovative capacity in China in part designed to insulate against US export controls makes controls less durable; and limited consensus to take action on China in allies makes agreement on multilateral controls harder.

---

[28] Meijer, Hugo. 2016. *Trading with the Enemy: The Making of US Export Control Policy toward the People's Republic of China.* Oxford University Press.
[29] Ibid.

The US share of global economic output declined from nearly 40 percent in 1960 to 25 percent in 2022, while China's share rose from 4 percent to 18 percent in the same period. Companies, including US companies, are increasingly doing R&D not only outside the US, but outside traditional US security allies (Branstetter, Jensen, and Glennon 2019). In this world of globalized supply chains with innovation coming from commercial firms instead of the Pentagon, it is much harder to effectively control technology with unilateral controls, or even those from multiple countries. US firms have also been able to work around sanctions—that is, more able to maintain exports to export-controlled countries by employing supply chains through other countries.[30]

China has strong and growing domestic capacities for innovation and diversified supply networks for many goods that often run through countries that would not readily sign on to US export controls on China. If China responds to controls by sourcing the technology the US means to deprive it of either from another country or develops homegrown capacity to produce it, the result would be lost revenue for US firms, less understanding of China's capabilities, and ultimately lost leverage to impose costs on targets via sanctions. Without US firms in a leading role in key chokepoint areas, even the most ambitious extraterritorial measures that cut off access to US finance, technology, or markets would fail.

Current coordination among sanctioning countries on Russia has been suboptimal and ad hoc, and prospects for future export controls in general and related to China are uncertain, despite progress in working with Japan and the Netherlands.[31] As mentioned above, target countries can shift to other currencies or suppliers of goods and services. But multilateral controls take longer to impose and may need to be diluted to achieve consensus within a coalition.[32] Multilateral support for controls on China is currently limited at best. The European Union and many countries who have imposed sanctions on Russia have generally not agreed to impose controls on China like those of the United States.

Recommendations

Dynamic Controls to Keep Pace with Technology

The Obama administration's export control reform initiative focused on reducing both outdated and unfocused controls that "strained government resources by attempting to protect all

---

[30] Richardson, J. David, and Asha Sundaram. 2013. "Sizing Up US Export Disincentives for a New Generation of National-Security Export Controls." **Policy Brief 13-13**, Peterson Institute for International Economics, May. Available at https://www.piie.com/publications/policy-briefs/sizing-us-export-disincentives-new-generation-national-security-export.

[31] Wolf, Kevin, and Emily S. Weinstein. 2022. "COCOM's Daughter: Why a New Multilateral Export Control Regime Is Needed to Address Contemporary National Security and Human Rights Issues." *WorldECR*, May. Available at: https://www.worldecr.com/archive/cocoms-daughter/.

[32] Gregory C. Allen, Emily Benson, and Margot Putnam. 2023. "Japan and the Netherlands Announce Plans for New Export Controls on Semiconductor Equipment," CSIS Commentary, April 10, 2023. Available at: https://www.csis.org/analysis/japan-and-netherlands-announce-plans-new-export-controls-semiconductor-equipment

items" in wide categories, which led many buyers to source non-sensitive components from outside the US and "harmed the U.S. defense industrial base."[33] Frederick the Great famously said "he who defends everything, defends nothing," because spreading one's forces too thin to protect everything actually makes it easy to break through at any point.[34] This is why former Secretary of Defense Robert Gates advocated for export controls to be a "small yard, high fence" that focused limited defensive resources like export controls only on key technologies for security. President Biden's National Security Advisor Jake Sullivan also advocated for a small yard, high fence strategy. Trying to control too much means export control enforcement resources are spread too thin, undermining their ability to effectively deny China access to controlled technology.

Therefore, just as the new administration has promised to cut outdated regulations to boost US business and eliminate waste in government, it should also cut outdated export controls by doing what it always has done historically: adjusting the thresholds for control with technological progress. While Sullivan's goal of creating "as large a lead as possible" between the US and its adversaries in key technologies is sensible, the emphasis needs to be on the possible. It may be possible in 2022 to impose a control on Chinese chipmaking that corresponds to the state of the art a decade earlier, but China will not be stuck at that level falling one year further from the cutting edge every year. Technologies further from the cutting edge are easier to master or source from others, so if our controls are not adjusted with increases in Chinese capabilities, they will become easier every year to circumvent.

For example, if Huawei can produce at scale AI chips that are better than what Nvidia and other firms under US controls can sell in China, then the ultimate effect of the controls could be to hand that market to Huawei, giving it the revenue it needs to innovate further and reach scale for its software for AI training. A smart US control strategy could, subject to Chinese supply constraints, undermine Chinese domestic AI training chipmakers by updating export controls to ensure what US firms can sell in China are equivalent or just a bit better than Chinese domestic alternatives, incentivizing AI firms in China to avoid buying domestic.[35]

Eliminating outdated controls and adjusting thresholds for control with technological advances would also allow BIS to free up resources spent on implementing those controls to focus on more advanced, impactful controls.

---

[33] The White House. 2013. "Fact Sheet: Announcing the Revised U.S. Export Control System." *Press Release*, October 15. Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/10/15/fact-sheet-announcing-revised-us-export-control-system.

[34] Friedrich II of Prussia. 1746. "Die Generalprinzipien des Krieges und ihre Anwendung auf die Taktik und Disziplin der preußischen Truppen." Available at https://www.projekt-gutenberg.org/friedri2/preusstr/preusstr.html.

[35] This strategy would also need to consider supply constraints and the security trade-offs of additional computing resources available to Chinese AI firms. If Huawei was, for example as it seems to be the case now, not able to produce its Ascend AI GPUs at scale, then tighter controls on US chips than China's domestic capabilities could constrain Chinese compute available for AI. But if Chinese supply was not constrained, tougher controls on US exports would just hand revenue to Huawei instead of a US firm.

Give Export Controls Resources to Match New Tasks

Increase importance of export controls in competition with China, the top strategic challenge for the United States, merits commensurate resources. The first order of business should be to fund a technology upgrade that enables BIS to integrate these data with data from other government agencies and open sources and leverage internal data to discover attempts to circumvent controls. Second, it should have resources and authority to hire more industry expertise to identify critical technologies and better evaluate claims of "foreign availability." Firms will often claim that they should be allowed to ship an export controlled good if it is available from a country that does not impose controls, because blocking the sale would have no effect on the target while depriving them of revenue. However, BIS needs the technical expertise to evaluate these claims.

Third, BIS needs more economic expertise to project the impact and measure the effectiveness of past controls. As export controls affect more consumer goods, and global supply chains beyond defense, the economic effects of controls have become more important, and their ultimate impact on security hinges on questions of economics as much as defense, such as: how have past controls affected US industry competitiveness and thus the durability of chokepoints that give our controls teeth? Are firms routing R&D or sourcing outside the United States to avoid controls? What has been the financial impact on Chinese firms we have put on control lists? Having the answers to these questions would arm the new administration and Congress with the information they would need to figure out what controls are working and double down, while dropping ineffective or counterproductive controls.

Upgrade Multilateral Coordination

Unlike during the Cold War, there are very few areas in which not only US firms, but production in the United States is so much better than alternatives that the United States has a monopoly. Therefore, if it wants export controls to work outside of the few semiconductor chokepoints relied on today, it needs cooperation of other countries to either impose their own controls and help the US enforce its extraterritorial rules. The 10 or so export control officers around the world cannot hope to police diversion of US goods once abroad without local assistance. Yet few countries have imposed the kind of export controls the US wants on China.

So far, the US has taken a plurilateral approach including with the Netherlands and Japan on semiconductor manufacturing equipment. It has also worked with its allies to at least partially overcome the most acute coordination challenge of Russia's blocking behavior in the Wassenaar Arrangement, allowing countries to update their export control lists with agreement among "Wassenaar minus 1" that uses much of what exists today under Wassenaar but without requiring consent of Russia to update control lists.

The US needs to work with allies to not only keep the Wassenaar mechanism active, but also build a new multilateral system for export controls, designed to work with plurilateral

agreements but make them less ad hoc. The new regime should address shared security concerns on China balancing two dimensions. First, the need to include enough countries to cover key producers of technologies for control without making the coalition too broad to achieve consensus. Second, the new regime would require checks and balances on US power because allies are concerned about US overreach and will not agree to a cold-war style COCOM 2.0.

Recognize Risks of Chinese Retaliation

When the first Trump Administration imposed tariffs on China, the PRC retaliated with tit-for-tat tariffs on US goods, but six years of US technology controls on China did not led to any serious retaliation. China has been building out its own export control system along with a counter sanctions toolkit that includes a counterpart to the US Entity List called the "unreliable entities list" largely made up of US military contractors it sees as infringing on its interests in Taiwan. However, for many years it did not invoke this toolkit.

China decided retaliation was either infeasible or against its interests. Imposing its own export controls or targeting US firms would discourage US and other foreign firms from investing in production in China and could give fuel to the fire of voices in the United States and elsewhere advocating for either decoupling or derisking from China. China may have also perceived that it lacked the chokepoints needed for leverage.

This, however, is changing. China has long used economic coercion against US allies, but these tended to use the size of China's market rather than its control of unique technology as the point of leverage, refusing to for example import Norwegian Salmon after the Nobel Prize was awarded to a Chinese human rights activist. Recently, however, China imposed export controls with its dominant position in critical minerals like graphite used particularly in battery components, as well as gallium and germanium used in semiconductor production. These initially were aimed at US allies like Japan as a threat to cripple its automotive industry by shutting down graphite exports if it imposed further export controls on semiconductor equipment, but in December 2024 expanded to ban export to the United States.[36]

Allies often bemoan that the United States has not taken the threat of retaliation seriously, in part because China did not retaliate against the US. But that is now beginning too. China recently cut off a US drone company from batteries, a shot across the bow.[37] New export control laws entered into force in December 2024 that create extraterritorial authority similar to the foreign direct product rule (FDPR), allowing it to assert control over dual use goods made outside of China with Chinese technology, which if invoked could wreak havoc on many US

[36] Kurtenbach, Elaine. 2024. "China Bans Exports to US of Gallium, Germanium, Antimony in Response to Chip Sanctions." AP News, December 3. Available at: https://apnews.com/article/china-us-tech-semiconductor-chip-gallium-6b4216551e200fb719caa6a6cc67e2a4.

[37] Hille, Kathrin, Demetri Sevastopulo, and James Politi. 2023. "Chinese Sanctions Hit US Drone Maker Supplying Ukraine." Financial Times, July 4. Available at: https://www.ft.com/content/b1104594-5da7-4b9a-b635-e7a80ab68fad.

supply chains including in the defense industry. More recognition of the risks and costs of retaliation would also help the United States show it is taking its allies concerns seriously, which should help in building a broader coalition for controls.

References

Branstetter, Lee, Britta Glennon, and J. Bradford Jensen. 2019. "The Rise of Global Innovation by US Multinationals Poses Risks and Opportunities." **Policy Brief 19-9**, Peterson Institute for International Economics. Available at: https://www.piie.com/publications/policy-briefs/rise-global-innovation-us-multinationals-poses-risks-and-opportunities.

Chorzempa, Martin, Mary Lovely, and Christine Wan. 2024. "Rise of Economic Sanctions on China: Analysis of a New PIIE Dataset." **Event Publication**, Peterson Institute for International Economics. Available at: https://www.piie.com/events/2024/publication-launch-rise-us-economic-sanctions-china-analysis-new-piie-dataset.

Hufbauer, Gary, Jeffrey J. Schott, Kimberly Ann Elliott, and Barbara Oegg. *Economic Sanctions Reconsidered, 3rd Edition*. Peterson Institute for International Economics. Available at: https://www.piie.com/bookstore/economic-sanctions-reconsidered-3rd-edition-paper.