Center for a New American Security

APRIL 13, 2023

TESTIMONY BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Hearing on "China's Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes"
Panel III: Policy Tools for the United States and Its Allies and Partners

The Role of Investment Security in Addressing China's Pursuit of Defense Technologies

BY

Emily Kilcrease

Senior Fellow and Director
Energy, Economics, and Security Program
Center for a New American Security

I. Summary of Testimony

Chairman Bartholomew, Vice Chairman Wong, and Commissioners, thank you for the opportunity to provide testimony before the Commission.[1] A summary of the recommendations included in this testimony is included below, followed by the supporting analysis.

In order to strengthen the ability of the U.S. government to mitigate national security risks associated with inbound and outbound investments that may contribute to China's military modernization efforts, including its efforts to obtain foreign defense and dual-use technologies, Congress should consider the following actions.

Committee on Foreign Investment in the United States (CFIUS)

- Establish new authorities to list emerging technologies as critical technologies for the purposes of investment screening, as a limited addition to the existing FIRRMA definition of "critical technology."
- Reduce CFIUS burden of addressing risks only indirectly related to foreign investment by passing data privacy and data security legislation.
- Strengthen the role of the Office of Legal Council to provide a check on possible CFIUS mission creep.
- Amend the Foreign Risk Review Modernization Act of 2018 (FIRRMA) to allow the Secretary of the Treasury to delegate approval authority for sharing transaction-specific information with key allies to strengthen cooperation.

Outbound investment controls

- Establish a set of outbound investment controls focused on addressing national security risks associated with China's indigenous development of critical technologies, including notification requirements, entity-based restrictions, bright-line prohibitions on investments involving certain high-risk indigenous technology capabilities, and ultimately a sector-based screening process.
    - Implement new controls through a phased approach that allows the government to build its knowledge base, expand institutional capacity, and coordinate with allies and partners.
    - Establish a broad notification requirement for U.S. investments in Chinese companies making technologies that would be controlled if made in the United States, as well as a select set of other technologies that have not yet been specified on U.S. control lists.

[1] This testimony reflects the personal views of the author alone. As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, the Center for a New American Security (CNAS) maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

The author would like to acknowledge Tim Fist, Martijn Rasser, and the CNAS artificial intelligence team for their collaboration during the preparation of this testimony, as well as Sarah Bauerle Danzman for her intellectual contributions to the recommendations related to outbound investment authorities, many of which were previously discussed in "Sand in the Silicon: Designing an Outbound Investment Controls Mechanism" jointly published by CNAS and the Atlantic Council.

- Establish bright-line prohibitions on U.S. investments in Chinese companies producing items that meet the technical specification of items listed on the U.S. Munitions List or for military or space purposes on the Commerce Control List.

- Expand the Chinese Military-Industrial Complex (NS-CMIC) sanctions program to include all types of investments into designated companies and to allow for designations of a broader range of entities engaged in China's indigenous development of critical technologies.

- Implement a sector-based outbound investment screening process, starting with the semiconductor sector.

- Incorporate strong transparency and due process requirements, taking lessons learned from the CFIUS context.

- Do not implement any new authorities until a robust public consultation is conducted, including through hearings and a public comment period.

- Establish a new office under the supervision of the Assistant Secretary of the Treasury for Investment Security to coordinate a new interagency process for outbound investment authorities.

International coordination on investment security

- Fully resource the international engagement functions of the Departments of the Treasury and State.

- Create new requirements for CFIUS to assess and report to Congress on the impact of the CFIUS process on foreign investment flows from allies and partners, including an assessment of the effectiveness of the exempted foreign state authorities and the frequency and impact of mitigation agreements on investors from allies and partners.

- Encourage full use of existing fora, such as the U.S.-EU Trade and Technology Council, to coordinate export controls and investment screening policies with allies and partners.

- Pursue a broad coordination mechanism with allies and partners that would identify technologies of shared strategic importance and align export controls and investment controls authorities to protect such technologies.

II. Overall Investment Climate

Chinese Investment in the United States

New foreign direct investment (FDI) flows into the United States by Chinese investors have fallen dramatically in recent years. Coming out of the 2007-2008 financial crisis, Chinese investment in the United States saw a sharp spike rising from a baseline of almost zero to $27 billion in 2016. However, 2016 was a distinct and unusual peak, as these investment flows have since fallen steadily, decreasing to $15 billion in 2017 and then declining to the level of $294 million by 2021, the most recent year for which data is available from the Bureau of Economic Analysis.[2] All FDI flows into the United States showed declines in the 2015 – 2020 period, including marked declines in the first year of the COVID pandemic. However, global FDI flows into the United States, including those from the Asia Pacific region, have rebounded well in 2021,

[2] Bureau of Economic Analysis, *China – International Trade and Investment Country Facts*, data on "Investment expenditures – first year expenditures." Data last published on July 21, 2022 and available at: https://apps.bea.gov/international/factsheet/factsheet.html#650.

making the continued drop in Chinese FDI a notable outlier. The declining trends held across merger and acquisition activities as well as greenfield investments. Mergers and acquisitions peaked at $26 billion in 2016 and have now fallen to $254 million. Greenfield investments peaked at $1 billion in 2015 and fell as low as $36 million in 2019.[3]

The direct investment position of China in the United States (*i.e.*, the FDI stock that has accumulated over the years) shows a near freeze in Chinese investments overall. The direct investment position was $13 billion in 2013, rising to a peak of $63 billion in 2017 and declining to a range of $52-54 billion in following years through 2021.[4] This logically flows from the sharp decline in new FDI flows, as the net position of China's FDI stock in the United States will not increase so long as new FDI flows have dried up.

Chinese venture capital investment in the United States follows the same general patterns, rising from near zero prior to 2010 and potentially peaking in 2018. In 2018, 249 funding rounds for U.S. startups included a Chinese venture investor, with these investors investing an estimated $3.2 billion.[5] Several factors likely dampened flows post-2018, including the passage of strengthened investment screening authorities in the United States and later the COVID pandemic. However, dealmaking has not completely disappeared. Since late 2018 through April 2023, there was a Chinese lead investor in funding rounds worth approximately $20 billion for U.S.-based businesses across all sectors, according to Crunchbase data.[6] The exact amount attributable to the lead Chinese investor for each round is not available.

U.S. Investment in China

The U.S. direct investment position in China has risen steadily in recent years, growing from $60 billion in 2013 to $118 billion in 2021.[7] FDI flows have varied over the same time period, with a high of $11 billion in 2014 and generally staying in the $6 billion to $9 billion range. In 2021, FDI flows dropped to under $3 billion, which was likely driven by China's Zero-Covid policies in place at the time. The total FDI flows into China in 2021 were $181 billion, and flows into the Hong Kong Special Administration Region accounted for an additional $141 billion, reflecting that China has access to a wide range of FDI sources other than the United States.[8] U.S. investment in China includes significant amounts of greenfield investment, in addition to merger and acquisition activity, in contrast to Chinese investment in the United States, which does not include large amounts of greenfield investment. U.S. investors have also been active in China's nascent venture capital space, investing upwards of $60 billion of venture capital since 2010.[9] In recent years, U.S. venture investments in China have appeared to slow.[10] Chinese investors have become increasingly active in venture capital, including in high profile sectors such as artificial intelligence (AI), indicating the availability of venture capital to Chinese start-ups from sources beyond the United States.[11]

III. Effectiveness of CFIUS

[3] The Bureau of Economic Analysis has suppressed data on greenfield investments in 2020 and 2021 following standard practice of statistical agencies to not publicly release data that may inadvertently disclose data of individual companies. In other words, levels of greenfield investment have dropped so far that it is difficult for statistical agencies to report them.
[4] Bureau of Economic Analysis, *China – International Trade and Investment Country Facts*, data on "Foreign direct investment position in the United States on a historical-cost basis by country of ultimate beneficial owner." Data last published on July 21, 2022 and available at: https://apps.bea.gov/international/factsheet/factsheet.html#650.
[5] Thilo Hanemann, Daniel H. Rosen, Mark Witzke, Steve Bennion, and Emma Smith, "Two-Way Street 2021 Update: U.S.-China Investment Trends" (U.S.-China Investment Project conducted by the Rhodium Group and the National Committee on U.S. China Relations, May 2021).
[6] Author calculations using Crunchbase data.
[7] Bureau of Economic Analysis, *China – International Trade and Investment Country Facts*, data on "U.S. direct investment position abroad on a historical-cost basis." Data last published on July 21, 2022 and available at: https://apps.bea.gov/international/factsheet/factsheet.html#650.
[8] United Nations Conference on Trade and Development, "Fact Sheet #9: Foreign direct investment" (UNCTAD Handbook of Statistics 2022). Available at: https://unctad.org/system/files/official-document/tdstat47_FS09_en.pdf
[9] Thilo Hanemann, Mark Witzke, Charlie Vest, Lauren Dudley, and Ryan Featherston, "An Outbound Investment Screening Regime for the United States?" (U.S.-China Investment Project conducted by the Rhodium Group and the National Committee on U.S. China Relations, January 2022).
[10] "A Daunting Arsenal," *The Economist*, April 1, 2023.
[11] Emily S. Weinstein and Ngor Luong, "U.S. Outbound Investment into Chinese AI Companies" (Georgetown University Center for Security and Emerging Technology, February 2023).

Overview of CFIUS

The United States has a well-established legal framework for screening certain foreign investments into U.S. businesses in order to address the national security risks that may arise from such transactions. These authorities are implemented by the CFIUS, an interagency body chaired by the Secretary of the Treasury.[12] CFIUS has broad authority to respond to risks arising from foreign investments covered by its jurisdiction (*i.e.*, covered transactions.)[13] It can do this through the negotiation – or in some cases, imposition – of terms on a transaction to mitigate identified national security risks. Where mitigation cannot overcome the national security concerns, CFIUS may recommend that the President suspend or prohibit the covered transaction. The CFIUS program, implemented on a day-to-day basis by hundreds of civil servants working across the executive branch and subject to high levels of political accountability, is functioning well. The analysis and recommendations offered in this testimony aim to further strengthen the CFIUS process, with the ultimate objective of ensuring that it focuses its limited resources on transactions of highest national security risk, including those that may aid China's military modernization efforts.

FIRRMA Reforms

In 2018, FIRRMA reformed CFIUS in several key respects, including through an expansion of its jurisdiction to review new types of investment transactions. Prior to FIRRMA, CFIUS had the authority to review controlling investments, in which a foreign person gained control of an existing U.S. business.[14] This jurisdiction generally covered traditional mergers and acquisitions activity and applied across the U.S. economy, regardless of what sector the U.S. business operated in. It did not, however, include venture capital investments, an area of growing concern due to rising levels of Chinese venture capital investment in the United States. To address this gap, FIRRMA provided CFIUS authority to review a defined class of non-controlling investments (*i.e.*, covered investments), defined on the basis of rights that the investor would obtain through the investment as well as the type of U.S. business that was the recipient of the investment.[15] The intent of Congress was to capture those investments in which the investor had an active, even if non-controlling, role in the U.S. business, while carving out from jurisdiction purely passive investment flows. This new jurisdiction did not apply across all sectors and was instead limited to covered investments into U.S. business involved in critical technology, critical infrastructure, or sensitive personal data, as defined in detail in the implementing regulations.[16]

FIRRMA also expanded the CFIUS jurisdiction to review greenfield real estate transactions, in response to concerns about foreign acquisitions of land in close proximity to sensitive military facilities. CFIUS agencies, led by the Department of Defense, undertook an extensive rulemaking process to scope this new jurisdiction to capture those areas of real estate that were determined to present proximity concerns, while scoping out real estate for which investment transactions were unlikely to present a national security risk.[17] CFIUS has the ability to refine or expand the real estate jurisdiction through future rulemakings, should the need arise.

FIRRMA also made productive updates to the CFIUS process, including related to streamlining filing requirements, strengthening mitigation agreements, and bolstering enforcement capabilities. Notably, CFIUS for the first time received authority to mandate notification of certain transactions involving foreign government investors or U.S. businesses working on critical technology.[18] The voluntary nature of the

[12] For an overview of the CFIUS interagency process, see the CFIUS website at: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.
[13] See 31 CFR § 800.213 (*covered transaction*).
[14] See 31 CFR § 800.224 (*foreign person*), 31 CFR § 800.208 (*control*), and 31 CFR § 800.252 (*U.S. business*).
[15] See 31 CFR § 800.211 (*covered investments*).
[16] See 31 CFR § 800.211 (*covered investments*), 31 CFR § 800.215 (*critical technology*), 31 CFR § 800.214 (*critical infrastructure*), and 31 CFR § 800.241 (*sensitive personal data*).
[17] See 31 CFR § 802 for the full regulations regarding CFIUS and real estate transactions.
[18] "Provisions Pertaining to Certain Investments in the United States by Foreign Persons," Department of the Treasury, Office of Investment Security (Federal Register Vol. 85, No. 179, September 15, 2020). Available at: https://www.govinfo.gov/content/pkg/FR-2020-09-15/pdf/2020-18454.pdf.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

CFIUS process has generally worked well, as investors are strongly incentivized to file with CFIUS in order to receive regulatory safe harbor from further government review. Mandatory notifications, however, provide a critical ability for CFIUS to have greater visibility into a subset of transactions that may be more likely to raise national security concerns, strengthening its overall enforcement posture. The mandatory notification requirements for critical technology transactions are linked to export control authorities, in that a notification is required if the U.S. business makes a critical technology that the foreign investor would require an export control license to access.

Recognizing the importance of partners and allies in addressing investment-related national security risks, FIRRMA provided new authorities to facilitate international cooperation. This includes the ability to share transaction-specific information, where appropriate, as well as more general direction to establish processes to share trends and threat information. FIRRMA also created the legal flexibility to exempt certain foreign persons from the expanded areas of CFIUS jurisdiction. CFIUS has implemented this flexibility through the excepted foreign state determinations that allow qualified investors from a small handful of close allies to bypass CFIUS review for covered real estate and covered investment transactions.[19]

In parallel to these changes to the legal framework, CFIUS undertook an extensive diplomatic effort to encourage allies and partners to establish their own investment screening regimes. Prior to this time, the United States had generally not prioritized investment screening in its diplomatic engagements, in part out of concern that new regimes could inadvertently create investment market access barriers for U.S. firms abroad. However, as the U.S. investment market became increasingly closed for Chinese firms, there was growing awareness that China could seek comparable access to sensitive technologies through investments in other countries. Strong U.S. investment screening would thus have weaker effect on the ultimate objective of denying China those technologies it needed to modernize its military, if the United States acted alone. The diplomatic effort to encourage investment screening regimes in key allies and partners was supported by intensive technical assistance work to share U.S. investment screening best practices. These efforts led to a wave of new investment screening mechanisms established or existing mechanisms strengthened.[20]

Assessing the Effectiveness of CFIUS in Addressing China's Technology Acquisition Efforts

Generally, CFIUS has been effective in addressing investment-related risks associated with technologies that can be used for military modernization in China or other adversary countries. Chinese companies have largely been shut out of the U.S. investment market for key technology areas, such as advanced semiconductors and aerospace. Technologies that have well-established relevance to military objectives present relatively easier cases for which CFIUS can assess national security risks. CFIUS has a harder time, however, articulating risks associated with emerging technologies whose full applications are not yet known. It must also increasingly assess national security concerns beyond just technology transfer and consider the implications of China gaining greater market share and capacity in certain technology areas – both emerging and legacy technologies - which presents a separate risk assessment challenge. These challenges, plus increasing caseloads and stress on the CFIUS process, are areas for Congress to address to ensure that CFIUS remains an effective tool for limiting China's access to U.S. technologies with potential military applications.

CHALLENGES WITH EMERGING TECHNOLOGIES

[19] For information on CFIUS excepted foreign states, see the CFIUS website at: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-excepted-foreign-states.
[20] "Acquisition- and ownership-related policies to safeguard essential security interests: Current and emerging trends, observed designs, and policy practice in 62 economics," Research note by the Secretariat of the Organization for Economic Cooperation and Development (OECD) (OECD, May 2020).

Addressing risks associated with emerging technologies presents unique challenges for CFIUS. Risk assessments become inherently more speculative when considering applications that a technology could have rather than those it does have. U.S. companies may be making advances in pushing the emerging technology frontier forward as a general matter, but it may be difficult for CFIUS to articulate a credible risk scenario that ties such advances directly to contributions to China's military modernization. At the same time, U.S. national security leaders are increasingly recognizing that U.S. leadership in certain emerging technology areas will be foundational to America's future military preeminence, as well as its economic security. National Security Advisor Jake Sullivan has identified certain emerging technology areas that are "force multipliers" and in which U.S. leadership is a "national security imperative," including quantum information systems, artificial intelligence, and biotechnology, among others.[21] The CFIUS Executive Order issued on the day before Sullivan's remarks emphasized these same emerging technology areas, confirming that CFIUS will be used to protect U.S. advantage in these areas.[22]

The question remains, however, where CFIUS will draw a line between applications of emerging technologies that are commercial in nature and those that may make a meaningful contribution to China's military modernization. In fact, it appears plausible that no line will be drawn at all, and that U.S. policy is moving towards a more absolute approach in which access to any U.S. capabilities in key emerging technology areas will be seen as presenting a national security risk. Indeed, U.S. policy seems to be moving in this direction. Rather than seeking to control specific technologies of concern, the United States has shifted to attempting to halt the progress of entire technology ecosystems in China. Notably, the U.S. export controls issued in October 2022 related to chips, AI, and supercomputing are the first practical implementation of the strategic vision laid out by Sullivan, as they seek to cap China's advancement in these sectors.[23] While it is difficult to assess how far CFIUS specifically has moved in this direction, given the limited information available publicly on CFIUS determinations, U.S. export control policy has clearly moved to a broader ecosystem approach.

This broader ecosystem approach requires the government to rethink the longstanding links between its investment screening and export control authorities. CFIUS has traditionally defined "critical technology" through reference to the export control authorities, rather than developing its own lists of sensitive technologies. In order for a technology to be considered a critical technology for CFIUS purposes, the technology must have been identified and listed by the export controls agencies on one of the U.S. export control lists (*e.g.*, the U.S. Munitions List).[24] Prior to FIRRMA, this definitional issue had little practical impact. CFIUS had – and continues to have – full jurisdiction to review any covered control transaction, regardless of whether the U.S. business engaged in critical technology or not.[25] Under FIRRMA, however, the definition of critical technology took on heightened importance in two ways. First, the new CFIUS jurisdiction over covered investments was limited to only certain types of U.S. businesses, including those that engaged in critical technology. If, for example, a Chinese investor made a venture capital investment into a promising U.S. AI start-up, this investment would only be caught by CFIUS jurisdiction if the start-up's technology was export controlled. If it was not – any many emerging technologies may not be - the U.S. government has no legal jurisdiction to review the investment transaction. Second, the new FIRRMA authorities to mandate notifications of certain transactions to CFIUS also hinged on the definition of critical technology. These changes gave new importance to the legal links between export control authorities and CFIUS.

[21] Jake Sullivan, "Remarks at the Special Competitive Studies Project Global Emerging Technologies Summit" (Washington, DC, September 16, 2022). Available at: https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/.
[22] "Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States" (September 15, 2022). Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/.
[23] Emily Kilcrease, "How to Win Friends and Choke China's Chip Supply," *War on the Rocks*, January 6, 2023.
[24] See 50 USC § 4565(a)(6) and 31 CFR § 800.215.
[25] See 31 CFR § 800.210 (*covered control transaction*).

Tight linkages between export control and investment screening authorities generally make sense. If a technology is sensitive for national security reasons, then the government should protect it regardless of the form of commercial transaction that may expose it to foreign adversaries, whether that is an investment or an export. Alignment between the various authorities facilitate compliance efforts in the private sector, which is the first line of defense for any set of controls. It also makes more efficient use of limited bureaucratic resources, given the technical expertise and staff time required to assess the feasibility of any new controls. For these reasons, maintaining a strong alignment between export control technology classifications and investment screening authorities continues to be good policy.

However, there may be limited instances in which CFIUS has an interest in reviewing investment transactions involving uncontrolled technologies, particularly as the United States moves towards a broader ecosystem approach to the technology competition with China. Specifically, certain venture capital investments into U.S. companies developing emerging technologies may present national security concerns if such investments provide privileged access to expertise and capabilities that could be used to advance a foreign adversary's indigenous technology development. In emerging technology areas, this broader capabilities question may have national security relevance, even if the technology of the U.S. business itself is not controlled. International investment remains an important means of diffusing advanced technology expertise, and advances in emerging technologies areas may equally be made by start-ups receiving venture funding as they are from more established firms.[26] Certain transactions involving start-ups and emerging technologies may be falling outside of CFIUS jurisdiction, due to the limitations included in FIRRMA's definition of critical technology.

CASE STUDY: ARTIFICIAL INTELLIGENCE

The AI ecosystem provides a useful case study for where export controls and investment screening authorities may be differently positioned to address risks associated with emerging technologies. A country's capabilities in AI derive from its access to powerful computing power, the availability of large amounts of training data, and the ingenuity of its engineers to develop and train AI models. Export controls apply in different ways to these three categories of computing power, data, and talent. Computing power, or chips, are the easiest to address through export controls, as the export control authorities have a long practice of defining technical specifications of chips with national security relevance. For example, the United States imposed new controls on advanced AI chips as part of the October 2022 export controls package. Addressing concerns around access to data likely requires broader data privacy and data security legislation, as current AI models are built using publicly available data and thus export controls are unlikely to prevent access to that which is already available to the public. As AI systems exhaust publicly available data, controls on the export of private data sets may need consideration, as part of a broader U.S. push on data security.

More complicated questions arise when assessing risks that may arise from the development and training of AI models. General-purpose AI systems have recently broken into the headlines and sparked public curiosity with the release of large language models, such as ChatGPT. These general-purpose AI systems can approximate human cognitive abilities and learn new skills through analyzing data. These types of systems are trained through ingesting large amounts of data and learning how to produce accurate outputs from that data. For example, ChatGPT can draft a decent essay on U.S.-China strategic competition by ingesting think tank and other reports available online and synthesizing that information into a logical structure and argument.[27]

[26] "Managing Access to AI Advances to Safeguard Countries' Essential Security Interests" in *OECD Business and Finance Outlook 2021: AI in Business and Finance* (OECD Publishing, Paris, 2022).
[27] The workforce replacement effects of such developments on the think tank community, and the attendant risks to national security, have yet to be determined.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Today's general-purpose AI systems remain rudimentary, generating false facts or "hallucinations" and are not yet close to approximating the full range of human cognition.[28] But signs are already emerging of the dangers that these systems can present, and this risk will grow as the systems – and the underlying computing power – continue to grow. Existing large language models can be used, for example, to spread disinformation online, launch cyber attacks at a much faster scale than a human can alone, and generate disturbing pornographic images.[29] Large scale AI models, whether general-purpose systems or narrow AI systems focused on particular tasks, could be used for a range of military purposes, such as developing novel toxins, mapping the trajectory of hypersonic missiles, or simulating nuclear weapons testing.[30] The ability to achieve advances in the military AI domain can be supported through advances in general AI capabilities, and specifically the expertise, computing infrastructure, and institutional capacity to train and refine large scale models. Leading AI experts have called for a pause in the release of more powerful AI models until governments and industry develop more robust safety systems to mitigate this broad scope of risks and ensure that AI systems will have positive societal effects.[31]

AI governance will implicate a wide range of legal, ethical, and societal factors, and export controls will be only one of many governance tools needed to ensure the safety and stability of AI systems. While one could envision the establishment of export controls based on the overall computational power of an AI model, many if not all of the most powerful models are intended to be made open source. An open-source model is inherently impractical to control, as it is available to anyone with an online connection. It may also fall under the publications exception to U.S. export controls, which carve out unclassified software or technology that has been made available to the public without restriction.[32] Additionally, the development of AI models will be based on the value-laden judgements of the developers and institutions that build them, in some ways similar to – but more powerful than – how social media platforms have evolved. Export controls, which govern the transfer of technology out of a U.S. firm, cannot tell an AI company which values to have. While policymakers should continue assessing which parts of the AI ecosystem may be amenable to export controls, there are likely to remain significant areas in which export controls should not be the first line of defense to protect against risks.

Investment controls are differently situated, in that they can address a broader range of concerns that can arise institutionally within a firm and by virtue of the firm's governance or investment structure. For example, certain foreign investment interests could negatively impact an AI start-up's willingness to abide by emerging AI governance standards or to implement voluntary safety and stability standards. These types of corporate decisions cannot be caught via export controls but could nonetheless have significant impacts on U.S. national security. Large scale AI models are currently run by a small handful of large technology firms that can fund the massive expense of building the models, including the need for large numbers of expensive computing chips. However, start-ups can access comparable capabilities by, for example, buying an AI model developed by another firm and fine-tuning it for their own purposes. Chinese venture investors remain active in the U.S. AI start-up ecosystem, involved in over $2 billion worth of funding rounds for U.S. AI companies since the passage of FIRRMA, though the sensitivity of the invested companies is unclear based on existing data.[33] More broadly, the United States retains a lead over China in developing both general purpose and narrow AI systems, indicating that the United States will remain an attractive target for Chinese investors absent U.S. policies to regulate their engagement.

AI provides one case study for why the CFIUS process would benefit from additional authorities, but other emerging technology areas may present similar concerns. To provide flexibility to capture venture

[28] GPT-4 System Card, OpenAI, March 23, 2003. Available at: https://cdn.openai.com/papers/gpt-4-system-card.pdf.
[29] "Opwnai: Cybercriminals starting to use ChatGPT," Check Point Research, January 6, 2023. Available at: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt; "Eshoo Urges NSA and OSTP to Address Unsafe AI Practices," Office of U.S. Representative Anna G. Eshoo (D-CA), press release, September 22, 2022.
[30] Fabio Urbina, Filippa Lentzos, Cédric Invernizzi, and Sean Ekins, "Dual use of artificial-intelligence-powered drug discovery," *Nature Machine Intelligence*, 4, March 2022.
[31] Cade Metz and Gregory Schmidt, "Elon Musk and Others Call for Pause on A.I., Citing 'Profound Risks to Society,'" *The New York Times*, March 29, 2023.
[32] 15 CFR § 734.7.
[33] Author calculations based on Crunchbase data.

capital transactions involving these emerging technologies, Congress should authorize a limited expansion of the definition of *critical technology*. This could be accomplished through a targeted amendment to the Export Control Reform Act of 2018, authorizing Commerce to create a new export control classification number (ECCN) for investment purposes, complemented by a conforming amendment in FIRRMA to include this new category in the definition of *critical technology*. The investment ECCN would be additive to existing ECCNs and allow for the listing of emerging technologies that the government has an interest in reviewing in the investment context but that may not be suitable for an export control. The investment ECCN should be seen as a backstop tool used in limited, ad hoc circumstances, rather than a new requirement for CFIUS or Commerce to populate a new list of technologies. It should also only apply to a small handful of countries which present the highest risk with respect to emerging technologies, such as those countries listed under the EAR's military end user authorities or in the EAR's country group D5, which lists countries under an arms embargo.[34] In most cases, if CFIUS identifies a technology of interest, it will also be appropriate for Commerce to list it under traditional export controls, and the current legal framework already provides channels for this sort of coordination. The investment ECCN approach allows CFIUS to maintain consistency and alignment with export controls while providing flexibility to address a broader range of emerging technology risks.

BANDWIDTH CONSTRAINTS OF CFIUS

In 2021, the most recent year for which Treasury has reported data, CFIUS reviewed 164 short-form declarations and 272 notices.[35] For context, in 2018 (the year of FIRRMA's passage), CFIUS reviewed 229 notices, meaning that the number of transactions that CFIUS is reviewing has nearly doubled.[36] The number of difficult reviews also remains high, and it is important to note that it is the difficult reviews that consume most of the time of CFIUS. In 2021, 63 transactions were withdrawn and refiled, indicating that either the transacting parties or CFIUS required further time to assess risks or negotiate a mitigation agreement.[37] In contrast, in 2015 (a year in which Chinese investment in the United States was rapidly increasing), only 8 transactions were withdrawn and refiled.[38]

The numbers show that CFIUS has been under strain since before FIRRMA and that the additional transactions brought in post-FIRRMA continue to exacerbate challenges with processing transactions in a timely fashion. Importantly, these trends impact investment from friendly countries as well as that from adversary countries. While transactions involving investors from China regularly rank in the top three filing countries, so do those involving investors from Japan and Canada.[39] It is critical that investments from friendly countries get in and out of the CFIUS process expeditiously. Doing so means that a robust CFIUS process remains consistent with the long-standing open investment policy of the United States and that the U.S. economy continues to benefit from these types of investments. It also frees up resources for CFIUS to focus on transactions that present genuine national security risks, including ramping up its efforts to find transactions that have not been notified to CFIUS. Certain adjustments that FIRRMA made to the CFIUS process, such as the creation of a short-form declaration process to expedite certain reviews, are helpful but the numbers show that there is still a long way to go. Ensuring adequate staffing, not just in Treasury but across the CFIUS agencies and supporting intelligence community components, is critical.

DATA SECURITY AND DATA PRIVACY

[34] See 15 CFR § 744.21 and 15 CFR § 738 supplement no. 1.
[35] "Committee on Foreign Investment in the United States Annual Report to Congress" (Report period: CY 2018, public/unclassified version). Short-form declarations are subject to a 30-day review period and involve fewer informational requirements. Notices involve more extensive submission of information, and an initial 30-day review period can be extended to a 45-day investigation period or further.
[36] "Committee on Foreign Investment in the United States Annual Report to Congress" (Report period: CY 2021, public/unclassified version).
[37] 2018 CFIUS Annual Report.
[38] "Committee on Foreign Investment in the United States Annual Report to Congress" (Report period: CY 2015, public/unclassified version).
[39] 2021 CFIUS Annual Report.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Part of the solution to CFIUS's bandwidth issues should come from easing the burden on CFIUS to address risks that are only partially or indirectly related to foreign investment, and here data security is a prime example. CFIUS spends significant time assessing risks related to the potential exposure of sensitive personal data, or other forms of sensitive data, to foreign adversaries. CFIUS is required to assess whether existing authorities are adequate and appropriate to resolve any national security concerns arising from the covered transaction. Indeed, CFIUS is intended to be a tool of last resort, serving as a backstop when foreign investments present particular risks that cannot be addressed by other authorities available to the U.S. government. Too often, however, CFIUS is forced into the uncomfortable position of being the first line of defense when it comes to protecting sensitive data, since no comprehensive authority for data privacy or data security yet exists. It has become a tool of convenience to impose a patchwork of protections for sensitive data held by companies that just so happen to be receiving a foreign investment.

CFIUS is fundamentally unsuited to address broader concerns over data privacy and data security. The ongoing TikTok saga highlights this dilemma. The Chinese ownership of TikTok undoubtedly presents national security concerns, including with respect to sensitive personal data.[40] However, there is no law on the books preventing any of TikTok's U.S. competitors from selling very similar data sets to an overseas partner, and the data broker market is unfortunately robust.[41] Congress can help by passing comprehensive data privacy and data security legislation. Data privacy objectives should include giving individuals greater control over what data is collected about them online and how that information is sold or used. Data security objectives should address the national security concerns that can arise from the bulk transfer of sensitive data to a foreign adversary. Data privacy and data security have overlapping objectives and stronger data privacy will inherently reduce data security risks through minimization of the personal data on the open market. Data privacy and data security legislation is important in its own right but will also help return CFIUS to its intended purposes of addressing foreign investment risks rather than dealing with data risks writ large.

THIRD-PARTY RISKS AND THE NEED FOR INTERNATIONAL COLLABORATION

CFIUS expends significant energy in addressing third-party risks, in which national security risks arise not from the foreign investor directly but from the foreign investor's relationships with adversary countries. For example, if a European company is seeking to buy a U.S. business engaged in critical technology and the European company also has substantial operations in China, CFIUS may assess that the transaction presents national security concerns arising from diffusion of technology to China via the European investor. As foreign investment risks directly from China have declined with the overall drop in Chinese investment in the United States, third party risks have gained more prominence in the CFIUS assessment process. Third-party risks present a dilemma for CFIUS. On the one hand, these risks can be genuine and severe. On the other hand, CFIUS ideally would not be addressing these risks, if the export control and investment screening process of allies and partners were more closely aligned with those of the United States. With stronger alignment, the United States could have greater comfort that transfers of technology, expertise, and capabilities to allies and partners – including those that occur as part of an investment – would not lead to the diffusion of these assets to China. Instead, the United States could rely on the economic security authorities of partners and allies to effectively address these risks, reducing the pressure on CFIUS to do so.

Strengthening coordination with allies and partners can take different forms, depending on the maturity of the allies and partners' screening mechanisms. For partners like the Five Eyes countries and the European Union, cooperation can take more advanced form, such as coordinating specific transaction reviews or sharing classified risk assessments. For these partners, the Secretary of the Treasury has the ability to authorize the sharing of transaction-specific information as needed, though in practice this does not

[40] Committee on Energy and Commerce, U.S. House of Representatives, "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms," March 23, 2023.
[41] Captain Steven J. Arango, U.S. Marine Corps, "Data Brokers are a Threat to National Security" (U.S. Naval Institute *Proceedings*, December 2022, vol. 148/21/1,438).

happen regularly. Congress could encourage further information sharing by permitting the delegation of the information-sharing authorization to the Deputy Secretary level, as this official is deeply engaged already on most complex transaction reviews. More broadly, Congress should ensure that the Departments of Treasury and State have sufficient resources to regularly conduct technical outreach and engage in sustained cooperation on investment screening with key allies and partners. Ultimately, the United States should pursue a broad coordination mechanism that provides a forum for allies and partners to identify technologies of shared strategic interest and to align both export control and investment screening authorities to strengthen joint protection of these technologies.[42]

Strengthening coordination with allies and partners should also include intentional efforts to ensure that the CFIUS process is not impeding friendly investment flows into the United States. Congress can strengthen its oversight role here by instituting a new requirement for CFIUS to assess and report to Congress on the impact of the CFIUS process on foreign investment flows from allies and partners. This should include assessment of whether these flows have been negatively impacted by FIRRMA's expansion of CFIUS jurisdiction and whether FIRRMA's tool to address this, including the exempted foreign state program and the declaration process, are being effectively utilized. The reporting requirement should also address the impact of mitigation agreements on the investments of allies and partners, with the aim of ensuring that these mitigation agreements are genuinely focused on risks arising from the transaction and attributable to the foreign investor, rather than broader systemic risks.

Congress may also want to consider strengthening the role of the Office of Legal Counsel (OLC) within the CFIUS process, in order to ensure that CFIUS remains tightly focused on risks arising from covered transactions. When dealing with risks such as data security and third-party exposure to China, CFIUS risks straying from its core mission (*i.e.*, risks arising from foreign investment in the United States) and being used as a tool of convenience to address broader systemic risks. CFIUS already has certain mechanisms to ensure that its actions are consistent with its legal mandate, including the strenuous interagency consensus process and the requirement for all transactions to be signed off on by high-level political appointees. OLC provides guidance on the most complex transactions as well as those that will be recommended to the President for action. Moreover, the Department of Justice, in which OLC resides, is a voting member of CFIUS and actively engaged in all CFIUS functions. Strengthening OLC's role would thus be an intensification of existing practice, rather than an entirely new process. Involving OLC in a broader range of transaction reviews involving mitigation agreements can provide an independent check on possible mission creep and lessen the chance that mitigation is chilling benign foreign investment flows.

IV. Risks Associated with U.S. Investments in China[43]

While the United States has a robust process for addressing risks associated with foreign investment into the United States, it is less well positioned to address national security risks associated with U.S. investments into China. U.S. investments in China can present a range of foreign policy challenges, including support for companies implicated in systemic human rights abuses, offshoring of critical supply chains, and furtherance of China's indigenous technology development aims.

Each of these policy concerns requires a different response, and a broad-based set of outbound investment controls may not be appropriate in all cases. Human rights concerns, for example, may be addressed in a more targeted manner through the continued use of financial sanctions and Entity List designations, both of which have been used increasingly in recent years for human rights related reasons.[44]

[42] Emily Kilcrease, Senior Fellow and Director of the Energy, Economics, and Security Program at the Center for a New American Security, "Challenging China's Trade Practices," testimony before the U.S.-China Economic and Security Review Commission, April 14, 2022.
[43] Commentary and analysis in this section draws heavily from the author's paper with Dr. Sarah Bauerle Danzman, "Sand in the silicon: Designing an outbound investment controls mechanism" jointly published by CNAS and the Atlantic Council. Further detail is available in that paper.
[44] Emily Kilcrease and Michael Frazer, "Sanctions by the Numbers: SDN, CMIC, and Entity List Designations on China" (Center for a New American Security, March 2, 2023).

Tools such as the Uyghur Forced Labor Prevention Act will be critical to reduce global demand for goods made with forced labor. Offshoring of critical supply chains is most effectively addressed through policies that address the underlying economic drivers leading to offshoring. Blocking offshoring transactions is a blunt instrument that does nothing to make it commercially viable for firms to produce critical goods in the United States. A disciplined industrial policy is a more durable policy to encourage the development of secure, resilient supply chains. The passage of the CHIPS and Science Act and the Inflation Reduction Act to spur the development of chips and clean energy sectors in the United States are examples of how the United States might bolster supply chains by addressing the economics of why firms have in the past chosen not to manufacture in the United States. Enhanced government capacity to analyze supply chains and innovative financing mechanisms to support the expansion of critical manufacturing capacity domestically are also critical.[45]

Designing Outbound Investment Controls

Risks arising from capital flows that support China's indigenous development of critical technologies can and should be addressed through outbound investment controls. In prior work, my co-author Dr. Sarah Bauerle Danzman and I outline five principles that should guide the development of a new outbound investment mechanism. We recommend that new outbound investment tools be:

- targeted at transactions that present the highest national security risk;
- clearly defined and understandable to private-sector participants, who will be responsible for the first line of compliance;
- non-duplicative of existing tools that address national security risks associated with global economic activities, including inbound investment screening conducted CFIUS, export controls, list-based export sanctions programs, and the CHIPS and Science Act of 2022;
- scoped proportionately to the administrative capacity available to effectively administer a new mechanism; and
- designed to enable meaningful conversations with allies about adopting similar regimes.

To achieve these objectives, outbound investment controls should be crafted to serve as a complement to existing export control authorities. Export controls can be thought of as a three-legged stool, comprised of list-based controls (*e.g.*, the Commerce Control List), end user controls (*e.g.*, the Entity List), and end use controls (*e.g.*, military end use). Each of these legs of the stool are intended to capture different types of technology flows and will work best when used in tandem. In this context, investment controls can be thought of as the fourth leg in the stool, regulating the flow of capital that can support the indigenous development of technologies that would be controlled if they were developed in the United States. For example, a U.S. exporter may be prohibited from exporting an advanced semiconductor to China, but there would be no legal prohibition on a U.S. investor investing in a Chinese company to produce a comparable chip. Designing an outbound mechanism in this way provides an important scoping parameter for the types of technologies and sectors that will be covered.

In addition to the types of technologies covered, an outbound investment mechanism will need to define the types of investment transactions covered. Outbound investment controls should focus on "smart money" or investment flows that are accompanied by managerial expertise or other intangible benefits that may advance China's indigenous technology capabilities. For example, an advanced manufacturing operation requires not just technology, but also management that knows how to orchestrate complex supply chains, attract and retain skilled workers, and operate efficiently in a cost-competitive environment. These skills, which can be broadly characterized as "management expertise," are critical to the success of a sector but are not possible to capture through export controls. At the same, allowing U.S. investments that have these associated benefits to support the advancement of critical technology sectors in China is not in the U.S.

[45] Emily Kilcrease and Emily Jin, "Rebuild: Toolkit for a New American Industrial Policy" (Center for a New American Security, September 8, 2022).

interest. Is it this precise gap that an outbound investment mechanism can address. Passive capital flows that do not include management expertise should not be included in any outbound investment mechanism, as China's economy has sufficient capital or could easily obtain capital from other global sources. A focus on smart money echoes prior testimony before the Commission given by Adam Lysenko, who noted that regulation to target investments that involve contribution of "proprietary technical knowhow, valuable networking ties, or other forms of differentiated support" is more likely to have a "tangible impact."[46]

Focusing on indigenous technology development, complementarity to export controls, and smart money can provide an overarching framework for designing an outbound investment mechanism. To fill in this framework, the government should implement new controls through a phased approach that allows time to build institutional capacity and coordinate policies with allies and partners. This should include a mixture of notification requirements, entity-based restrictions, bright-line prohibitions on investments involving certain high-risk indigenous technology capabilities, and ultimately a sector-based screening process.

A first phase would include the establishment of a mandatory notification regime. Gaining visibility into the full scope of investments occurring remains difficult. Existing data sources provide only incomplete information on the investment transaction types and volumes, as well as the flow of information, technology, and expertise that may occur as part of the investment transaction. It is also difficult to ascertain from existing data sources what the technical capabilities are of the Chinese business receiving the investment. These data issues are exacerbated with private deal flows, including venture capital flows, which face fewer public disclosure requirements than publicly listed companies. A notification regime can fill these gaps but would need to be subject to strict confidentiality requirements (*e.g.*, exemption from Freedom of Information Act disclosures) in order to build public confidence that the confidential information collected would appropriately protected.

A notification regime must specify what types of investment transactions are covered, as well as what kinds of Chinese businesses. A broad capture of investment transaction types is appropriate for this information-gathering phase. While ultimately, any controls should be implemented on the basis of the smart money principle noted above, the government may not have sufficient visibility into investment flows at present to determine where to draw the line between smart money and passive investments. Alternatively, investment transaction types could be scoped down using concepts drawn from the CFIUS context, such as *controlling transaction* or *covered investment*. That is, if the U.S. investor gains a controlling share, or specified governance rights that fall short of control but indicate an active role for the investor, in a Chinese company, then the notification requirement would be triggered.

Notifications should not be required for all U.S. investments in China, but only for those investments into a Chinese firm that produces, designs, tests, manufactures, fabricates, or develops any item or items that would be controlled under U.S. export controls if originating in the United States. This captures those technologies that the U.S. government has already determined may present national security risks. In addition, there may be justification for adding technologies beyond those already controlled, particularly in the emerging technologies space. For example, the concerns noted in the above section on CFIUS about general purpose AI models could equally apply in the outbound investment context, even if it is difficult to capture these concerns via export controls. The White House's Critical and Emerging Technologies List may provide a starting point for the identification of other technologies that merit inclusion in the notification requirements, though that list does not provide sufficient technical detail to be used in its current form.[47] Any technologies that the government seeks to cover that go beyond those already listed under export control authorities should be outlined in detail through a rulemaking process.

[46] Adam Lysenko, "U.S. Investment in China's Capital Markets and Military-Industrial Complex," testimony before the U.S.-China Economic and Security Review Commission, March 19, 2021.
[47] National Science and Technology Council, Fast Track Action Subcommittee on Critical and Emerging Technologies, "Critical and Emerging Technologies List Update," February 2022. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

Beyond notifications, there are further steps that the government could take in the near term to address obvious inconsistencies in existing law or policy and that do not require additional information gathering. The administration could establish a prohibition on U.S. investments in any Chinese firm that produces, designs, tests, manufactures, fabricates, or develops any technology that meets the technical specification of a technology that is subject to a U.S. arms embargo with respect to China. This would capture Chinese companies making items listed on the U.S. Munitions List, as well as space and military items listed on the Commerce Control List. This can be accomplished through regulatory changes to the International Trafficking in Arms Regulations (ITAR) and the Export Administration Regulations (EAR).

The administration or Congress could authorize the expansion of the Chinese Military-Industrial Complex (NS-CMIC) sanctions program. This program currently restricts U.S. persons from buying or selling publicly traded securities of the designated entities and is limited to entities operating in the defense and related materiel or cyber surveillance sectors in China. This program could be expanded to include all investment categories, beyond just publicly traded securities. A broader range of sectors critical to China's military modernization, such as chips, could be included in the program. It could be further strengthened by establishing an internal policy process within the administration to automatically consider cross-listings between entities designated under the NS-CMIC program and those on the Entity List. An expanded NS-CMIC program could serve as a useful option between the current NS-CMIC authorities, which have had limited impact on the designated entities, and more severe financial sanction, such as a full blocking sanction or specially designated national designation, which would be a highly escalatory step. To maximize the effect of an expanded NS-CMIC program, the administration should issue public guidance on what types of entities may ultimately be listed, in order to shape private sector incentives when making future investment decisions.

Over time, as institutional capacity is built to implement outbound investment controls, the mechanism should be expanded to implement sector-based screening. Sector-based screening should be additional to the expansion of the NS-CMIC sanctions program and bright-line prohibitions related to arms-embargoed technologies but should be significantly narrower than the notifications requirements. A core part of a screening process would be to permit the government to negotiate mitigation terms to address national security risks that may arise from an outbound investment, or to recommend that the President prohibit transactions where warranted. These reviews will therefore be inherently more time intensive and consequential that a notification regime and the jurisdiction should be scoped accordingly to permit effective administration of a screening process. Given the criticality of the semiconductor sector to U.S. national security, this sector should be prioritized in a sector-based screening mechanism, including design, fabrication, manufacturing equipment, design software, and packaging.

Designing an effective outbound investment screening process would include:

- Borrowing the concepts of *covered controlling transactions* and *covered investments* as defined in CFIUS to scope jurisdiction for the types of transactions covered, adjusting as needed based on information learned during the notification regime;
- Mandating screening for investments across the chips sector,
- Establishing prospective authorities only and not applying jurisdiction retroactively;
- Granting regulatory "safe harbor" from further review once the government concludes action on a transaction; and
- Clarifying how the outbound investment authorities will relate to the guardrail provisions under the CHIPS and Science Act that prohibit the recipients of federal subsidies from expanding their chips operations in China.[48]

[48] "Commerce Department Outlines Proposed National Security Guardrails for CHIPS for America Incentives Program," Department of the Commerce, press release, March 21, 2023. Available at: https://www.commerce.gov/news/press-releases/2023/03/commerce-department-outlines-proposed-national-security-guardrails.

A core element of an effective screening mechanism will be a rigorous risk assessment process. Generally, the analytic process for assessing national security risk under CFIUS will be a good guide for an outbound investment mechanism, including the requirements to analyze the component parts of threat, vulnerabilities, and consequences. An outbound investment risk assessment should consider relevant national security factors, such as

- contribution of the U.S. investment to China's indigenous technology development;
- relevance of the technology to U.S. national security interests;
- availability of alternative foreign sources of capital for the proposed investment;
- capability of U.S. investors to offshore key capabilities to circumvent U.S. outbound investment controls; and
- willingness of key allies to implement similar controls.

While CFIUS conducts its transaction risk assessment anew each time, there may be benefits to setting more clear policies around how risk will be assessed in an outbound investment context. An outbound investment mechanism could implement a policy of a "presumption of denial" for any investment that is made into a Chinese company making chips that a U.S. company would not be able to export to China. For example, a presumption of denial policy would be logical for investments into any companies fabricating chips at the technical threshold laid out in the October 2022 export controls (*e.g.*, 14 nanometers for logic chips.)

An outbound investment mechanism can draw important lessons from existing CFIUS procedures, particularly around transparency and due process, to ensure that the process is implemented in a manner consistent with an open investment environment. The administration should issue guidance on the types of national security risks that it will consider when reviewing outbound investment transactions. The recent CFIUS Executive Order provides an excellent template, as it identifies a range of technologies and risk factors that CFIUS considers. Risk assessments for specific transactions would be necessarily classified, but public guidance such as the CFIUS Executive Order are important steps to provide clarity and transparency into an otherwise opaque process. Like CFIUS, an outbound mechanism should have mandated timelines for the government to complete review of a transaction. Strict timelines allow transacting parties to make commercial decisions based on a more predictable regulatory process. In the event that the government identifies risks with a particular outbound investment transaction and seeks to take adverse action (*e.g.*, to prohibit the deal), it should provide due process to the transacting parties, including providing them with the unclassified basis for the determination as well as an opportunity to respond. Finally, Congress will have an important oversight role to play, including to ensure that the outbound investment function is fully resourced. Like the current CFIUS process, Congress should have the ability to request briefings on specific transactions once the administration has concluded its review. This process has served CFIUS well in providing accountability to Congress while avoiding particular transaction reviews from becoming politicized (as a general matter, though there are a handful of notable exceptions).

Organizationally, the Department of the Treasury is best situated to lead a new outbound investment process. The Treasury experience chairing CFIUS, as well as its lead role in implementing U.S. sanctions, give it unique strengths and insights when it comes to tracking international investments and global financial flows. Congress should create a new office to lead an interagency outbound investment process and place it under the leadership of the Senate-confirmed Assistant Secretary for Investment Security. The outbound investment authorities should not be located within the CFIUS process. As noted earlier, the CFIUS process is already under significant strain and Congress should seek to reduce rather than increase the burdens on CFIUS. The Department of Commerce should also be given a leading role, given the recommended structure of designing the outbound mechanism as a complement to existing export control authorities. An interagency process to support the outbound investment process should be established, including the same set of agencies that currently participate in the CFIUS process (*i.e.*, the Departments of Defense, Energy, Homeland Security, Justice, State, and the White House Offices of Science and Technology

Policy and of the U.S. Trade Representative). This group of agencies provides deep expertise on risks associated with economic ties to China and represents the range of diplomatic, economic, and national security equities that should be considered when implementing an outbound investment mechanism. The Office of the Director of National Intelligence should be tasked to provide threat assessments in support of the outbound investment process.

Legislative or Executive in the Lead

An unresolved question in the debate remains whether new outbound investment authorities will be implemented via executive order or through legislation. Some of the recommendations in this testimony, such as expansion of the NS-CMIC program or updates to the EAR and ITAR, can easily be accomplished via executive action and do not require Congressional action. The International Economic Emergency Powers Act (IEEPA) likely provides sufficient authority for the President to establish the full scope of recommended actions, including a sector-based screening mechanism. A legislative solution would ultimately provide a more durable policy response, as executive orders can be rescinded by subsequent administrations. Legislation also avoids the mission creep that has been associated with recent use of IEEPA for a range of China-related threats, many of which present serious national security and foreign policy concerns but may not strictly speaking constitute "emergencies" as originally envisioned in IEEPA. Brennan Center research has noted that the President's use of IEEPA is "virtually unchecked," calling in to question whether the extensive use of IEEPA as a routine foreign policy measure erodes the checks and balances between the executive and legislative branches.[49] For these reasons, legislation would be more appropriate from a procedural perspective, though the current legislative proposals do not align with the substantive recommendations in this testimony.

Under either a legislative or an executive approach, no new authorities should be established prior to a rigorous public debate. At a minimum, legislation, executive orders, and regulations should be released in proposed form and should not be made effective until after an adequate public comment period. Commission and Congressional hearings on outbound investment screening should be continued, to advance the public debate on the need for and appropriate design of these new authorities.

Anticipating the Unintended Consequences of Outbound Investment Controls

If designed or implemented without careful consideration, new outbound investment controls can present serious risks to U.S. competitiveness. An overly broad mechanism could stifle the ability of U.S. firms to engage in FDI. Firms engage in FDI for a variety of reasons, including to serve customers in the domestic market in which they are making the investment. For example, a fast-food restaurant will need to invest in a foreign market in order to sell its burgers there. Similarly, for a wide range of non-sensitive goods, FDI can allow U.S. firms to produce in a cost competitive manner closer to the end customer, enabling them to more effectively reach the 96 percent of the world's consumers that live outside the borders of the United States, including those in China.[50] Many FDI flows do not present national security concerns and can benefit U.S. economic growth, and care should be taken to ensure that beneficial flows can continue unimpeded. Research from the Rhodium Group estimated that certain outbound investment proposals could capture 43 percent of U.S. investment flows into China.[51] Such a broad scope trends towards decoupling in a blunt way that may not be connected to genuine national security risks and that may ultimately disadvantage U.S. commercial interests by closing off an important global market.

[49] Andrew Boyle, "Checking the President's Sanctions Powers" (Brennan Center for Justice, June 10, 2021).
[50] Small Business Administration, Export Products Business Guide, available at https://www.sba.gov/business-guide/grow-your-business/export-products#:~:text=Nearly%2096%25%20of%20consumers%20live,power%20is%20in%20foreign%20countries.
[51] Hanemann et al., 2022.

Further, outbound investment risks are highly concentrated in a small handful of countries and do not present on a global basis. An outbound investment mechanism should focus on countries of high risk, to avoid a chilling effect on U.S. investment ties with the rest of the world. The U.S. FDI position worldwide is $6.5 trillion, of which only $118 billion is in China.[52] U.S. outbound investment tools should reflect these basic facts and be designed to avoid disrupting the large amount of FDI flows that do not involve China. Specifically, in contrast to the CFIUS process that provides authority to screen all foreign investments into the United States, an outbound investment process should be limited to a defined list of foreign adversaries, such as those countries subject to the EAR's military end use and end user restrictions (*i.e.*, Burma, Cambodia, PRC, Venezuela, Belarus, and Russia).[53]

A tailored outbound investment mechanism that is squarely focused on transactions of high national security risk can avoid these pitfalls. A disciplined design can also avoid another potential unintended consequence, which is that other countries mimic a broad U.S. mechanism and the proliferation of such mechanisms create new barriers to U.S. investors abroad. The United States has been a recognized leader in developing an inbound investment screening process that builds confidence in the open investment climate by developing a well-tailored regime to guard against genuine national security risks. This has allowed the United States to credibly engage with other countries and encourage them to develop similarly targeted inbound investment regimes, limiting the risk that such regimes would be used to block U.S. investors abroad. A similar approach for outbound investment would ensure that the United States can continue to attract beneficial foreign investment in the United States and that other countries will not block their investors from seeking such investments.

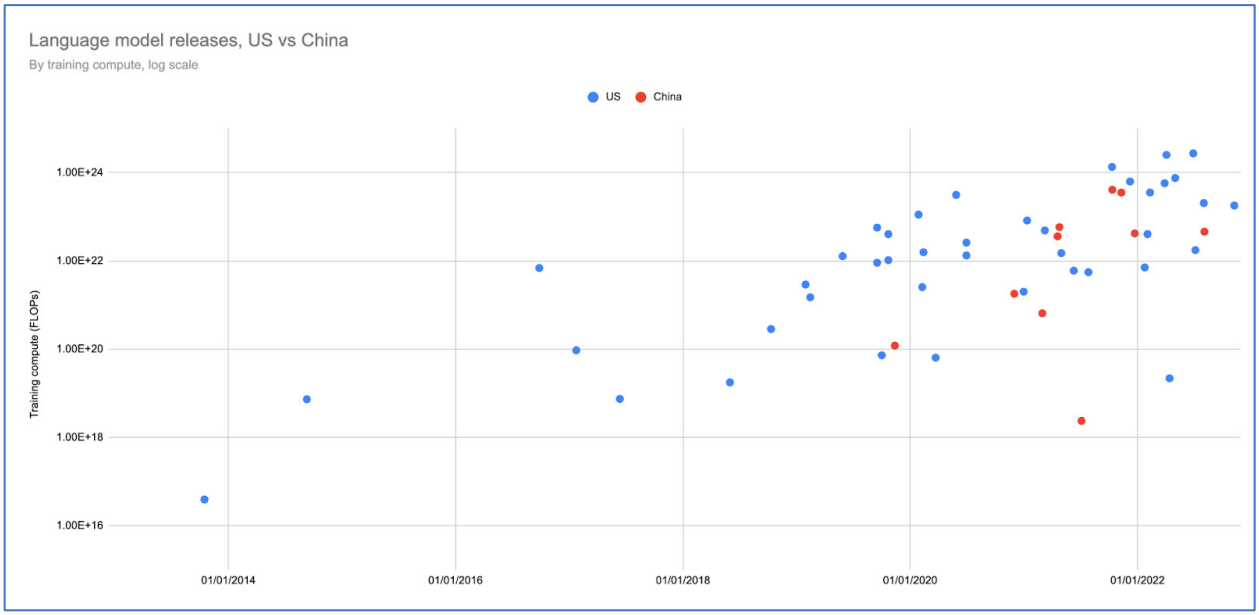
U.S. commercial interests will be damaged if the United States acts unilaterally in implementing an outbound investment regime. Capital and expertise can flow easily across borders and non-U.S. investors can quickly step in to backfill any space left by U.S. investors in the China market. Just as export controls are most effective when implemented by all key producer nations, investment controls will work best if done with allies and partners that are also critical sources of capital and expertise. Certain allies and partners have established or are moving towards developing an outbound investment screening regime, including South Korea, Taiwan, and the European Union.[54] The United States must work closely with these and other partners to align outbound investment screening mechanisms, as well as to ensure consistency between these mechanisms and existing export control and inbound investing screening tools. Congress can support these efforts by fully resourcing the international engagement functions of a new outbound investment office or offices. Doing so will be critical for ensuring U.S. national security, as well as preventing the further fragmentation of the open global trading system.

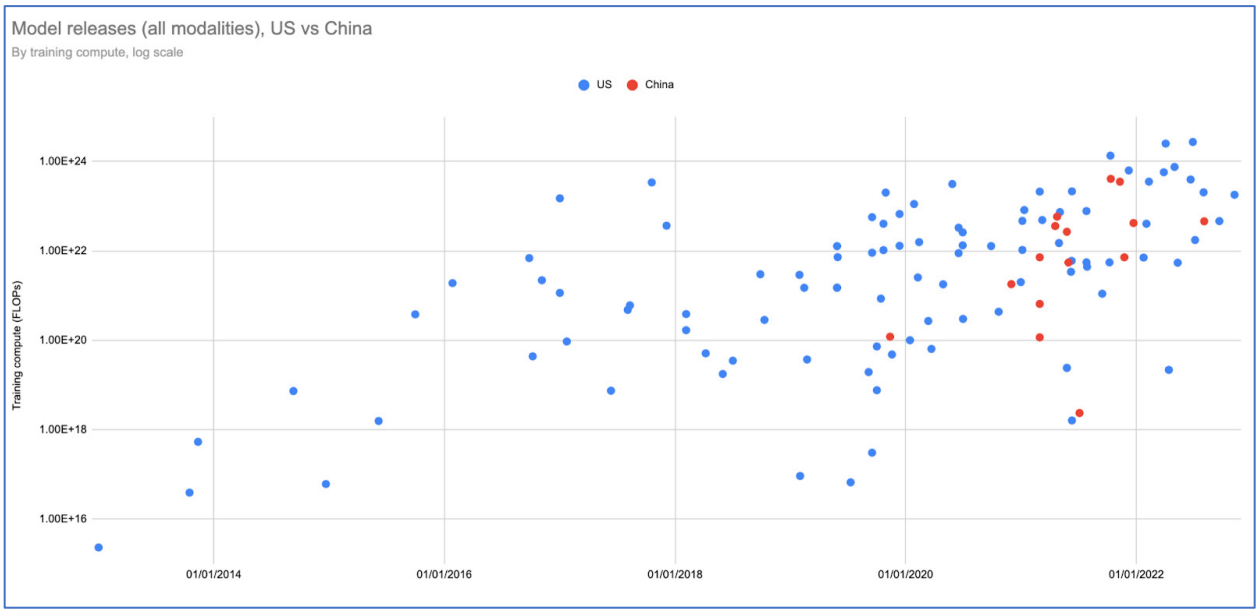
###

Appendix: U.S. and China AI Model Releases[55]

[52] Bureau of Economic Analysis, *China – International Trade and Investment Country Facts*, data on "U.S. direct investment position abroad on a historical-cost basis." Data last published on July 21, 2022 and available at: https://apps.bea.gov/international/factsheet/factsheet.html#650.
[53] 14 CFR § 744.21.
[54] Chad Bown and Yilin Wang, "Taiwan's Outbound Foreign Investment, Particularly in Tech, Continues to Go to Mainland China Despite Strict Controls," Peterson Institute for International Economics, February 27, 2023. Available at: https://www.piie.com/research/piie-charts/taiwans-outbound-foreign-investment-particularly-tech-continues-go-mainland. Ursula von der Leyen, President of the European Commission, "EU-China Relations" (Mercator Institute for China Studies and the European Policy Centre, March 30, 2023). Hanemann et al., 2022.
[55] Data compiled from publicly available information by Tim Fist, Fellow, Center for a New American Security.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc


Language model releases, US vs China
By training compute, log scale
US
China
Training compute (FLOPs)
1.00E+24
1.00E+22
1.00E+20
1.00E+18
1.00E+16
01/01/2014
01/01/2016
01/01/2018
01/01/2020
01/01/2022


Model releases (all modalities), US vs China
By training compute, log scale
US
China
Training compute (FLOPs)
1.00E+24
1.00E+22
1.00E+20
1.00E+18
1.00E+16
01/01/2014
01/01/2016
01/01/2018
01/01/2020
01/01/2022