RAND

Research Report

WILL SHUMATE, DAVID LUCKEY, TIMOTHY MARLER, MONIKA COOPER,
CHRISTOPHER SCOTT ADAMS, JULIA ARNOLD,
CLAY STRICKLAND, JACQUELINE GARDNER BURNS

Export Controls on Artificial Intelligence and Uncrewed Aircraft Systems

Interagency Challenges

For more information on this publication, visit **www.rand.org/t/RRA3296-1**.

About RAND

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

Cover: Semiconductors—Grispb/Adobe Stock, ryanking999/Adobe Stock; Sgt. Charlie Duke/U.S. Army.

Limited Print and Electronic Distribution Rights

RR-A3296-1

About This Report

The People's Republic of China and the United States are in competition for the development of artificial intelligence (AI) technology and uncrewed aircraft systems (UASs). In this analysis, we examined the current and potential future states of export control regulations on AI and UAS technologies for military use. We also analyzed how existing regulations are effective, inadequate, or even detrimental. Finally, in this report, we provide insights on how AI and UAS export controls might be applicable to creating a system of export controls for AI-enabled UASs that balances competition with China and securely guided proliferation of AI-enabled UAS technologies.

Context and Time Frame of the Study

For this report, we analyzed U.S. export control policy for 2022 through 2024, tracing the competing forces and trade-offs that shaped key decisions during that period. The analysis concluded in February 2025 and therefore does not reflect subsequent developments—such as Executive Orders 14179 and 14307, the July 2025 America's AI Action Plan, U.S. Department of State revisions to UAS export rules, or Bureau of Industry and Security deregulation in early 2026—which, together, have significantly altered the global regulatory environment. By including our distillation of the benefits and drawbacks of different policy choices, however, this report serves not only as a historical record but also as a primer to inform future national-level decisionmaking in a rapidly evolving international landscape.

RAND National Security Research Division

This research was conducted within the Acquisition and Technology Policy Program of the RAND National Security Research Division (NSRD), which operates the RAND National Defense Research Institute (NDRI), a federally funded research and development center (FFRDC) sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise. This research was made possible by NDRI exploratory research funding that was provided through the FFRDC contract and approved by NDRI's primary sponsor.

This research began approximately 18 months ago, when regulatory data and case material for UASs were more readily available than comparable material for AI systems in these applications. Since then, AI has advanced rapidly, and the policy debate has expanded. The heavier UAS content in the descriptive chapters reflects available evidence at the time of drafting this report. Thus, there is more emphasis on AI in the findings and recommendations, and this reflects the urgent need to develop new approaches for emergent technologies.

Acknowledgments

We are grateful to our colleagues who led and contributed to the studies cited in this document, for generating insights on which much of this work is based. We appreciate the valuable contributions made by the participants in our discussions. Additionally, we appreciate the generous support and helpful guidance we received from NSRD and Acquisition and Technology Policy Program leadership.

Summary

The People's Republic of China (PRC) and the United States are developing technology for both artificial intelligence (AI) and uncrewed aircraft systems (UASs). In the United States, the Replicator initiative is one example of accelerating the development and fielding of UASs. International proliferation of UASs and its effects must be considered when implementing strategies that would accelerate development of these technologies because both the PRC and the United States will have the ability to fill the demand in other countries for these systems. The U.S. government regulates AI and UAS exports mostly separately from one another. How this situation will evolve must be considered, however, in the face of rapid and unpredictable evolution of both technologies and the agility required to regulate each. AI and UAS technologies, particularly those with dual uses, are advancing with increasing speed, but export controls lag. This deficiency in regulations can stifle appropriate national security, industry autonomy—and thus technological advances—and coordinated integration of the two technologies. The goal of this report is to review the current export control systems for AI and UASs, examine effectiveness, and consider how the United States could form a balanced system of export controls for AI and UASs. The report focuses on dual-use technologies, which are regulated by the Export Administration Regulations, which are administered by the Bureau of Industry and Security (BIS) in the U.S. Department of Commerce (DOC). However, the report also provides some insights on the International Traffic in Arms Regulations, which are administered by the Directorate of Defense Trade Controls in the U.S. Department of State (DOS). In the report, we also discuss the U.S. Department of Defense's (DoD's) Defense Technology Security Administration (DTSA), which provides technical expertise and risk assessment through the interagency process.[1]

Issue

For this report, we examined the current and potential future states of export control regulations on AI and UAS technologies; analyzed how current regulations are effective, inadequate, or even detrimental; and assessed how insights on AI and UAS export controls might be applicable to creating a system of export controls for AI and UASs that balances competition with China and securely guided proliferation of AI and UAS technologies.

For this report, we analyzed U.S. export control policy for 2022 through 2024, tracing the competing forces and trade-offs that shaped key decisions during that period. The analysis concluded in February 2025 and therefore does not reflect subsequent developments—such as Executive Orders 14179 and 14307, the July 2025 America's AI Action Plan, U.S. Department of State revisions to

[1] Executive Order 14347, signed September 5, 2025, authorized the use of Department of War as a secondary name for the Department of Defense. This publication was written before that order was released and thus refers to the secretary and department by their current statutory names under Public Law 81-216, National Security Act Amendments of 1949.

UAS export rules, or BIS deregulation in early 2026—which, together, have significantly altered the global regulatory environment. By including our distillation of the benefits and drawbacks of different policy choices, however, this report serves not only as a historical record but also as a primer to inform future national-level decisionmaking in a rapidly evolving international landscape.

Approach

Our approach utilized a literature review and framework analysis of interviews with subject-matter experts. We performed a literature review at three levels:

- primary sources, such as laws, regulations, and internal policy documents
- secondary sources, such as reports from the Congressional Research Service, the U.S. Government Accountability Office, and congressional testimony
- third-tier literature, including academic literature, reports from think tanks, and media sources.

We also conducted semistructured interviews with more than 20 subject-matter experts from government, the private sector, and academic institutions. The results of these interviews were analyzed using a doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTmLPF) framework.

Key Findings

- The U.S. defense industrial base lacks a significant technology edge over adversaries' industrial bases in AI and UASs. This shifts the risk–reward calculation on tightening or relaxing export controls in these areas.
- The United States still maintains some lead in AI and in some areas of military UASs, but it no longer acts from a monopolistic technology position like it did with AI and military UASs before 2018.
- Overregulation of AI and UASs poses the risk of dampening domestic competitiveness, accelerating advancements abroad, and creating security risks driven by China arming or making transfers to U.S. allies and partners. Foreign governments could also respond to U.S. export controls with retaliatory or punitive policies affecting access to critical resources.
- AI and UAS export control dynamics create feedback loops in which export controls can either strengthen the United States' lead in technologies or create a death spiral of regulation that depletes the U.S. technological lead in areas in which the United States maintains an advantage.
- Export controls for AI and UASs make up a dynamic and adaptive system that could be evaluated more efficiently and regularly and that requires analysis looking further in the future.
- Growth in technology competition, larger volumes of export control–related data, new methods of export control circumvention, and increasingly blurred lines between civilian and military uses of AI and UASs will increase the need for efficiency and adaptiveness.

- AI is newer than UASs in a military context, and DTSA could benefit from developing increased knowledge of the industry's infrastructure and ecosystem.
- DOC is understaffed and underfunded for meeting current needs for AI and UAS export controls. If trends in technology advancement and diversion efforts continue, the gap between capabilities and needs will likely grow. The evolution of AI-enabled UASs will likely add new dimensions to this problem.
- Data regulation—how to decide what data are, how to classify data, how to compartmentalize data, who gets access, how to store data to ensure proper access, how to monitor data transfer, and so on—is a critical consideration for AI-enabled UASs in the future and an area in which BIS could theoretically limit adversaries' access; however, imposing such limits would require identifying the differences between military training data and commercial data and require BIS to increase its expertise and further its engagement efforts (ideally in a joint forum) with stakeholders developing AI and UASs for the United States and its allies.
- There might be opportunities for limiting access to autonomous capabilities via limiting the spread of training data required to develop an autonomous UAS capable of performing on the battlefield.
- The U.S. government—the legislative and executive branches—would need to task DOC, DoD, and DOS with identifying criteria that make data military training data (which could originate from commercial sources) as opposed to other operational data, along with a means of identifying such data and the models that result from training on those data.
- Regulating training data for autonomous UASs would require expertise that BIS does not currently have, as well as repeated engagement with the stakeholder community that is developing autonomous UASs for use by DoD and U.S. allies. If, however, BIS could work around these hurdles, controls on data and models could be real means of limiting the proliferation of autonomous UASs to hostile countries.

Recommendations

DoD should find ways to further develop innovation leadership with research and development (R&D) for UASs and AI:

- In the past, military demands drove technological advancements, but commercial innovations have shifted the dynamic dramatically, and segmentation has increased.
- Although industry R&D funding might continue to surpass that of DoD, DoD could still play a leadership role in driving innovation and anticipating security and regulatory challenges.
- Deepening relationships with smaller, nontraditional defense industrial base firms at the forefront of innovation is critical to DoD's ability to inform export controls and mitigate risk.

DTSA should work more in depth with the AI industry to increase understanding of the infrastructure and ecosystem related to AI, mirroring BIS efforts:

- It should continue to increase interaction with industry and further capitalize on firms' desire to interact with DTSA early and often during the technology development process as they streamline their efforts to take technologies to global markets as military applications increase.
- Cooperation and learning from this process can enable DoD to better balance and manage increasingly segmented but overlapping technologies, such as AI and UASs, and can improve its ability to advise on export controls.

DTSA and DOC should conduct more-proactive analysis to identify and assess potential security risks associated with technological advancements:

- They should engage in additional analysis focused three to ten years in the future, outside the scope of current technology levels.
- They should perform technology forecasting to anticipate security challenges *before* they become critical issues.
- They should focus on the security implications of technological trends, highlighting potential dual uses.

The **U.S. government** needs to develop a more flexible and responsive regulatory framework for adaptive policymaking:

- It should improve DOC's, DoD's, and DOS's ability to quickly adjust export controls in response to new information or national security threats related to emerging technologies, thereby maintaining a balance between national security and technological advancement and decreasing the time from the identification of a national security threat to the drafting and implementation of export controls.
- The U.S. government needs to increase resources for BIS to engage more extensively with industry and to broaden emerging-technology expertise. BIS faces unique budgetary challenges, and DOC's focus on dual-use technology necessitates a great deal of complex interaction with industry.
- It should codify and publish the regulatory process and responsibilities in DoD, DOC, and DOS doctrine to address concerns about blurred lines and unclear responsibilities.

DOC should lead an effort with DOS and DoD to explore methods and procedures for more systematically tracking the effects and effectiveness of export regulations as perceived by each department.

DOC, DoD, and DOS should expand interagency efforts at technology assessments and forecasting to consider the *intersection* of emerging technologies, such as AI and UASs, and decrease stovepiping of relevant areas of expertise.

Contents

Table

Chapter 1

Introduction

Both China and the United States are working hard to develop artificial intelligence (AI) and uncrewed aircraft system (UAS) technologies. The Replicator initiative is accelerating the development and fielding of UASs.[2] International proliferation and its effects must be considered because both China and the United States will have the ability to fill other countries' demand for these systems. AI and UAS exports are regulated largely separately by the U.S. government. Policymakers and other stakeholders must consider how this situation will evolve in the face of the rapid and unpredictable evolution of both technologies and the agility required to regulate each. AI and UAS technologies are advancing with increasing speed, but export controls lag. This deficiency in regulations can stifle appropriate national security, industry autonomy—and thus technological advances—and coordinated integration of the two technologies. The goal of this report is to review the existing export control system for AI and UAS, examine its effectiveness, and consider how the United States could form an improved system of export controls for AI and UAS.

Scope

For this report, we examined the current and potential future state of export control regulations on AI and UAS technologies; analyzed how current regulations are effective, inadequate, or even detrimental; and assessed how insights on AI and UAS export controls might be applicable to creating a system of export controls for AI and UAS that balances competition with China and securely guided proliferation of AI and UAS technologies. Moreover, both AI and UASs are examined within the context of export controls. The analysis emphasizes dual-use and commercial technologies regulated under the Export Administration Regulations (EAR), which are administered by the Bureau of Industry and Security (BIS) in the U.S. Department of Commerce (DOC).[3] These include applications in logistics, communications, agriculture, and commercial drone services, as well as general-purpose AI software and computing infrastructure. Some systems, however, are designed, developed, or modified for military application. These are governed under the International Traffic in

[2] On August 28, 2023, Deputy Secretary of Defense Kathleen Hicks unveiled the Replicator initiative, a U.S. Department of Defense (DoD) strategy to counter the rapid buildup of the PRC's armed forces. The initiative's goal was to field thousands of multidomain (land, sea, air) autonomous systems over a period of 18 to 24 months. In particular, the initiative targets low-cost, less exquisite, "attritable" systems that have the ability to mass capabilities with volume and velocity. Such systems are intended to deter aggression or, in the case of conflict, ensure victory. See Joseph Clark, "Hicks Underscores U.S. Innovation in Unveiling Strategy to Counter China's Military Buildup," DoD, August 28, 2023.

Executive Order 14347, signed September 5, 2025, authorized the use of Department of War as a secondary name for the Department of Defense. This publication was written before that order was released and thus refers to the secretary and department by their current statutory names under Public Law 81-216, National Security Act Amendments of 1949.

[3] Code of Federal Regulations, Title 15, Subtitle B, Chapter VII, Subchapter C, Part 730, General Information; 15 C.F.R. Part 732, Steps for Using the EAR; 15 C.F.R. Part 734, Scope of the Export Administration Regulations.

Arms Regulations (ITAR), which is administered by the U.S. Department of State (DOS).[4] The ITAR governs defense articles, defense services, and related technical data, including software. Although the primary focus of this report is on dual-use and commercial regulation under the EAR, certain issues necessarily involve ITAR jurisdiction. Furthermore, although both AI and UASs are addressed in this report, much of the descriptive security analysis focuses on UASs because export controls for these systems have a longer regulatory history and provide established examples. Therefore, many of the findings and recommendations focus on AI because the technology is emergent, less tested in regulatory frameworks, and advancing rapidly. This difference in emphasis reflects the maturity of UAS regulation and the need to develop approaches for AI.

Engagements with subject-matter experts concluded in late 2024, and the majority of analytic work was finalized by February 2025. Since that time, several significant policy developments have occurred in the realm of export controls for AI and UASs, including both the implementation and subsequent rescission of the AI diffusion rule,[5] as well as executive actions by President Donald Trump's administration aimed at promoting the export of U.S. AI technologies.[6] These developments fall outside the scope of this report and are not incorporated into the present analysis. Nevertheless, the report addresses the broader structural and policy dynamics that have shaped export controls for AI and UAS technologies to date. For the purposes of this analysis, AI and UASs are treated primarily as dual-use and commercial technologies under the jurisdiction of DOC under the EAR.[7] Certain AI and UASs, however, were designed, developed, or modified for military application. These systems fall under the ITAR and are administered by DOS.[8]

The ITAR governs defense articles, defense services, and related technical data. Although the emphasis of this report is on dual-use and commercial regulation under the EAR, some discussion necessarily implicates technologies that cross into ITAR jurisdiction.

Objectives and Research Questions

This research has two objectives: (1) to serve as a primer for export controls in the current conversation around AI and UASs and (2) to provide insight into the nuance and challenges related to these export controls and how that could translate into regulation of AI-enabled UASs. In pursuit of those objectives, we addressed the following research questions:

- What is the current state of U.S. regulations on the export of dual-use AI and UAS technologies?
- In what ways are current AI and UAS export controls effective? In what ways are they inadequate?

[4] Code of Federal Regulations, Title 22, Chapter I, Subchapter M, International Traffic in Arms Regulations.

[5] BIS, DOC, "Framework for Artificial Intelligence Diffusion," *Federal Register*, Vol. 90, No. 9, January 15, 2025b (interim final rule and request for comments).

[6] Office of Congressional and Public Affairs, BIS, DOC, "Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Chip-Related Export Controls," press release, May 13, 2025.

[7] 15 C.F.R. Subchapter C.

[8] 22 C.F.R. Subchapter M.

- Could AI and UAS export controls have an effect on private-sector development of AI and UASs?
- In what ways could the relaxation or tightening of export controls affect U.S. security interests?
- How could export control regulations be modified to balance competition with China and securely guided proliferation of AI and UASs?

Methodology

We used two approaches in our methodology: a literature review and interviews of subject-matter experts from the U.S. government, the private sector, and academia. The literature review was performed across three levels: primary sources, such as laws, regulations, and internal policy documents; secondary sources, such as reports from the Congressional Research Service, the U.S. Government Accountability Office, and congressional testimony; and other literature, including academic literature, reports from think tanks, and media sources. Our interviews with federal officials focused on subject-matter experts in DoD, DOC, and DOS, and private-sector interviews were conducted with subject-matter experts in the defense industrial base whose work focused on UAS and AI technologies. In total, we interviewed more than 25 participants; discussions were spread evenly between DoD, DOC, DOS, and industry. We then used a doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTmLPF) framework to organize thematic analysis on the outputs of the literature review and subject-matter expert interviews to develop insights and recommendations on how AI and UAS export controls could be improved to balance competition with China and the securely guided proliferation of AI-enabled UAS technologies.

Overview of the Report

The report is structured as follows: Chapter 2 provides an overview of the major export control updates that have dictated AI and UAS export control regulation from 2022 to 2024. We based this discussion on export controls that were discussed in depth during our subject-matter expert interviews. Chapter 3 presents insights from those interviews on the effectiveness of, challenges with, and opportunities for the export control process. Chapter 4 presents the AI and UAS export controls' potential impact on the private sector. Chapter 5 discusses the national security impact of controls and of AI and UAS technologies. Chapter 6 closes with overall insights, challenges, opportunities, and recommendations.

Chapter 2

The Current State of Export Controls on Artificial Intelligence and Uncrewed Aircraft Systems

Historical Context for Controls on Artificial Intelligence

In this chapter, we review three sets of export controls most relevant to our examination of AI export controls: the October 2022 restrictions, the October 2023 updates, and the December 2024 updates. We start with the October 2022 controls as they represent a significant change in the U.S. strategy to address AI by more robustly targeting the Chinese commercial sector's intertwined relationship with the Chinese military. The October 2023 and December 2024 updates to export controls represent attempts to build on the previous export control strategy by widening the scope and strictness of the October 2022 controls and plugging various loopholes.

This provides context for our observations derived from interviews with subject-matter experts, described in Chapter 3, and our discussions of private-sector and national security impacts, described in Chapters 4 and 5. Notably, another important round of export controls was released in January 2025; it is mentioned briefly at points, but the export controls were released too late for our team to perform a full review for this report.

In addition, Chapter 4 highlights the economic impact of export controls on AI and UAS technology. Economic security is integral to national security. Control over advanced technologies, sustainable and resilient supply chains, and, ultimately, industrial capacity enables the United States to sustain military superiority. Near-peer competitors, particularly the People's Republic of China (PRC), are integrating economic policy with military modernization, making economic security a critical success factor in strategic competition. Semiconductors, AI, and, to a lesser extent, UASs are foundational to both U.S. economic strength and U.S. defense capabilities. Accordingly, U.S. policy has elevated security to the same level of priority as traditional defense domains.[9]

To underscore this point, in February 2025, President Trump issued a memorandum, "America First Investment Policy," that states, "Economic security is national security." The memorandum directs exhaustive review of foreign direct investment from adversary nations in sensitive sectors.[10] In

[9] Chris Clement and Sidney Traynham, *Economic Security Is National Security*, Global Economic Hub, U.S. Global Leadership Coalition, June 2025; Marco Macchiavelli Navin Girishankar, and Matthew S. Borman, "Do Export Controls Erode the United States' Lead—or Protect It?" Center for Strategic and International Studies (CSIS), Back and Forth 5, August 13, 2025.

[10] Donald J. Trump, "America First Investment Policy," memorandum for the Secretaries of the Treasury, Defense, Commerce, Labor, Energy, and Homeland Security; U.S. Attorney General; administrator of the U.S. Environmental Protection Agency; directors of the Office of Management and Budget, National Intelligence, the Office of Science and Technology Policy, and the Federal Bureau of Investigation; the U.S. Trade Representative; the chair of the Council of Economic Advisers; and the assistant to the President for national security affairs, White House, February 21, 2025.

April 2025, a national emergency declaration cited foreign trade practices as risks to U.S. economic sovereignty and security.[11]

These initiatives reinforce the October 2022, October 2023, and the December 2024 export controls, which were implemented to restrict transfers of advanced chips, AI systems, UASs, and related dual-use technologies to China. The objective of these policies is to facilitate U.S. technological leadership by denying adversaries access to critical capabilities and aligning economic policy with defense strategy.[12]

October 2022 Restrictions

On October 7, 2022, BIS released rules to limit the PRC's ability to acquire and use advanced U.S. semiconductor technologies to support the modernization of the PRC's military. These rules were intended to establish a more direct connection between AI technologies and Chinese military applications involving supercomputing and quantum computing to reduce diversion tactics used by the PRC to enable civil–military fusion. The export controls limit the PRC's access to advanced integrated circuits (ICs) that enable military modernization and human rights violations. The rules also limit the PRC's ability to leverage U.S. technologies supporting a PRC supercomputer program used to support efforts related to weapons of mass destruction (WMD) and military modernization. Furthermore, the rules aim to deny the PRC access to U.S. semiconductor manufacturing equipment (SME) for indigenous development or production of IC chips for the PRC's civil–military fusion program.[13] These controls represented a shift from previous U.S. efforts to regulate PRC development of advanced chips by broadly targeting the supply chain via end-use and item-specific export controls, as well as U.S.-person controls. This shift was driven by the ineffectiveness of previous export controls caused by those controls' inability to separate Chinese commercial and military interests.[14]

The controls were intended to limit access to AI chips, design capability, the ability to manufacture advanced chips, and access and ability to develop advanced chip manufacturing equipment.[15] The United States pursued what was termed a *small-yard, high-fence strategy*, in which a small number of technologies and entities are targeted with very strict export controls.[16] The rules stated that high-end AI chips could be sold to entities operating in China, including the Chinese military, Chinese tech companies, and companies from other countries. This strategy is a response to a PRC civil–military fusion policy in which all companies can be connected to and operate with the

[11] White House, "President Donald J. Trump Declares National Emergency to Increase Our Competitive Edge, Protect Our Sovereignty, and Strengthen Our National and Economic Security," fact sheet, April 2, 2025.

[12] Nury Turkel "AI, National Security, and the Global Technology Race: How US Export Controls Define the Future of Innovation," policy memo, Hudson Institute, March 24, 2025.

[13] Matthew S. Axelrod, "Remarks as Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod to the Society for International Affairs 2022 Fall Advanced Conference," BIS, DOC, November 14, 2022.

[14] Ansgar Baums, "The 'Chokepoint' Fallacy of Tech Export Controls," Henry L. Stimson Center, February 6, 2024.

[15] Sujai Shivakumar, Charles Wessner, and Thomas Howell, "A Seismic Shift: The New U.S. Semiconductor Export Controls and the Implications for U.S. Firms, Allies, and the Innovation Ecosystem," CSIS, November 14, 2022.

[16] Sujai Shivakumar, Charles Wessner, and Thomas Howell, "Balancing the Ledger: Export Controls on U.S. Chip Technology to China," CSIS, February 21, 2024.

military.[17] The export control regime uses tools similar to those used in previous regimes but layers these tools to target specific, interconnected sections of the semiconductor supply chain. The controls also prohibit access to U.S. nationals' expertise, strengthen licensing requirements, make a presumption of denial (the initial assumption that any request for license to export will be denied), increase the number of entities on the unverified list, expand the foreign direct product (FDP) rule, and increase scrutinization of investments.[18]

Specifically, to achieve these objectives, BIS took several paths:

- First, BIS placed specific limitations on chips and items used in AI and advanced computing applications, with the thresholds designed to restrict chipset measuring 14 nanometers (nm) or less.[19] Furthermore, a new FDP rule extended these restrictions to chips manufactured in other countries using certain U.S. technologies or tools, including chips made with PRC chip designs if those chips fell within the parameters of restrictions set by BIS technical experts.
- Second, controls were implemented for chips and other items to be used in PRC supercomputers or supercomputers being exported to the PRC. A second FDP rule was implemented that applies to select foreign-made products being sent to the PRC for use in supercomputers, including foreign-made semiconductors.[20]
- Third, 28 PRC entities were added to the BIS Entity List (a compilation of foreign entities deemed a national security risk) as a response to their involvement in advanced IC-related activities or supercomputer-related activities.[21] These entities are subject to the Entity List FDP rule, which restricts the ability to procure foreign-produced chips and related items. The Entity List was further expanded in December 2022.[22]
- Fourth, countrywide controls were put in place for the PRC on exports of some SME tools critical to high-end chip production. Furthermore, controls were put in place to restrict the export of any item intended to go to PRC semiconductor fabrication facilities engaged in either the development or production of either advanced logic or memory chips. License requirements were also put in place for U.S. persons involved in providing support to such entities.
- Last, controls were imposed on items to be used for the development or production of indigenous SME within the PRC.[23]

To accomplish the halt of development, production, or procurement transfer of advanced chips, the 2022 rules defined a performance threshold for what sorts of chips could be sold to China, and any

[17] Gregory C. Allen, "Blocking China's Access to AI Chips Matters to U.S. National Security," commentary, CSIS, July 31, 2023b.

[18] Shivakumar, Wessner, and Howell, 2022.

[19] Thea D. Rozman Kendler, "Statement of Thea D. Rozman Kendler, Assistant Secretary of Commerce for Export Administration, Before the Senate Banking, Housing, and Urban Affairs Committee Hearing Entitled, 'Countering China: Advancing U.S. National Security, Economic Security, and Foreign Policy,'" May 31, 2023.

[20] Kendler, 2023.

[21] Kendler, 2023.

[22] Kendler, 2023.

[23] Kendler, 2023.

activity related to any chip above the performance threshold required the seller to seek an export license with a presumption of denial for companies operating in China. Essentially, this license requirement is a de facto ban on the sale of chips above the performance threshold: (1) any chip that is a powerful parallel processor (300 tera operations per second or higher) and (2) any chip that has an interconnect speed of 600 gigabytes (GB) per second or higher.[24] The interconnect performance threshold targets chips designed for networking in data centers and supercomputer facilities necessary for training and running large AI models. Notably, this still provides China with access to powerful parallel computer chips used for individual computers and video game consoles.[25]

Licensing requirements and presumption of denial apply to all field-effect transistor logic manufacturing equipment, which affects most 16-nm or lower technology nodes. The United States is also blocking less-advanced legacy chip manufacturing equipment, including restrictions on the sale of 18-nm process node and smaller dynamic random-access memory (DRAM) memory chips, and long-term not-and (NAND) flash memory is restricted at 128 layers or higher.[26]

Furthermore, licensing restrictions block exports of components and items on the Commerce Control List (CCL) that could enable China to develop its own advanced SME. These restrictions were intended to keep Chinese companies' advanced NAND production facilities from staying in business. The restrictions are reinforced by blocking access to support that U.S. equipment companies supply, such as support team availability and access to spare parts, thereby slowing or halting production.[27]

The use of export controls on chip manufacturing equipment combined with the FDP tool ensures that, if Chinese entities have access to U.S.-designed software, they will not be able to use design-out strategies and have other countries manufacture the chips for them. This means there can be no Chinese outsourcing of the manufacture of advanced chips.[28]

The 2022 export controls placed significant burden on the PRC's ability to manufacture its own chips. They mark the start of the recent round of efforts to regulate the transfer of advanced chips and chip-making capabilities to China. Chinese firms still face foreign competition with both low-performance and high-performance technologies.[29] Thus, China has been reproducing the value chain of SME in order to produce its first chip.[30] To block China from making Chinese alternatives to U.S. AI chips, the export controls continue to allow sales of chips below certain technological performance thresholds (which prevents Chinese companies from filling the gap in the market and gaining the

[24] Kendler, 2023.

[25] Gregory C. Allen, "Choking Off China's Access to the Future of AI," CSIS, October 11, 2022; Office of Congressional and Public Affairs, BIS, DOC, "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)," press release, October 7, 2022.

[26] Allen, 2022; Office of Congressional and Public Affairs, 2022.

[27] Allen, 2022; Office of Congressional and Public Affairs, 2022.

[28] Allen, 2022; Office of Congressional and Public Affairs, 2022.

[29] *Low performance* and *high performance* denote technologies both above and below the performance thresholds set forth in the October 2022 and October 2023 export controls.

[30] Allen, 2023b.

revenue and scale to fund their own advanced chip development) and restrict the sale of advanced chip-making equipment.[31]

October 2023 Updates to the October 2022 Semiconductor Export Control Rules

The October 2023 updates bolstered the initial export control measures set on October 7, 2022. These updated rules further restrict the PRC's ability to acquire and manufacture advanced high-end chips that are crucial for military applications. By expanding the Entity List and refining previous regulations, the United States sought to enhance the effectiveness of previous measures, ensuring robustness and responsiveness to technological and strategic shifts while minimizing unintended repercussions for international trade. Where the initial 2022 controls used a small-fence, high-yard strategy, the 2023 rules increased the number of technologies and entities targeted, as well as the strictness of the rules.[32] U.S. Secretary of Commerce Gina Raimondo acknowledged an increased impact on commercial interests and the need to balance potential societal benefits and harms.[33]

The October 2023 controls extended restrictions to less advanced chips and expanded controls to new types of SME. Furthermore, they required manufacturers to notify BIS if a chip from a list of even less advanced chips were to be sold to restricted countries, such as China.[34]

New rules were created for logic chips that had either nonplanar transistor architecture chips or production nodes below 16 nm. Additionally, they were created for DRAM chips of 18 nm or less and NAND memory chips with layers of 128 or more. These were organized into two tiers.[35]

The advanced computing chip rule enhances the previously established licensing requirements with two primary categories of modifications: refinements to the parameters that characterize a restricted chip and additional measures to thwart efforts to bypass these controls.[36] The first adjustment to parameters was the elimination of the interconnect bandwidth parameter for classifying restricted chips. The rule established restrictions based on the violation of either the existing performance threshold from the October 2022 rule or a performance density threshold intended to preempt work-arounds used against the October 2022 rule parameters. At the same time, exports of chips for certain consumer applications were exempted in an attempt to provide flexibility with the more stringent framework. Furthermore, the October 2023 rule requires notification of intended export of certain chips that are near but below the restriction parameters.[37]

---

[31] Allen, 2023b; Office of Congressional and Public Affairs, 2022.

[32] Office of Congressional and Public Affairs, BIS, DOC, "Commerce Strengthens Restrictions on Advanced Computing Semiconductors, Semiconductor Manufacturing Equipment, and Supercomputing Items to Countries of Concern," press release, October 17, 2023a.

[33] Eva Dou, "Commerce Department Moves to Cut Key Supply Lines to China's AI Industry," *Washington Post*, October 17, 2023.

[34] Will Henshall, "What to Know About the U.S. Curbs on AI Chip Exports to China," *Time*, October 17, 2023.

[35] William Alan Reinsch, Matthew Schleich, and Thibault Denamiel, "Insight into the U.S. Semiconductor Export Controls Update," *Critical Questions*, CSIS, October 20, 2023.

[36] Office of Congressional and Public Affairs, 2023a.

[37] Office of Congressional and Public Affairs, 2023a.

Four new Export Control Classification Numbers (ECCNs) were added to the CCL:[38]

- 3A090 addresses advanced ICs with transfer rates equal to or greater than 600 GB.
- 3B090 addresses certain SME and related items.
- 4A090 addresses computers, assemblies, and components that contain ICs that surpass the limit outlined in 3A090.
- 4D090 addresses software specific to developing items under the control of 4A090.[39]

Furthermore, BIS revised chip software and technology rules and restricted license exceptions for exports, reexports, and in-country transfers of certain items related to the PRC. In addition, BIS introduced three new FDP rules, created end-use licensing requirements for both SME and supercomputers, and placed restrictions on U.S. persons' participation in PRC production of advanced ICs.[40]

Several measures were put in place to prevent circumvention of controls. The October 2023 rule mandated licensing requirements for exports of controlled chips to any company headquartered in an arms-embargoed country (including the PRC), or any company with a parent company in an embargoed country. Additionally, new red flags and due-diligence protocols and indicators were put in place to facilitate foundries' identification of restricted chip designs and prevent illicit fabrication of chips.[41]

Presumption-of-denial licensing requirements were tightened to include all 22 of the countries that were under U.S. arms embargo at the time. There are circumstances, however, in which exports destined for an embargoed country would have a presumption of approval to allow enhanced monitoring and control of potential diversion and unauthorized access.[42]

2024 Updates to October 2022 Semiconductor Export Control Rules

Additional export controls were published in December 2024. These export controls address primarily six issues:

- The controls expanded restrictions to high-bandwidth memory (HBM), which is a crucial type of memory for AI applications.
- Additionally, the controls expand the list of SME to include equipment used to produce HBM, DRAM, and advanced packaging, as well as expanding equipment covered by end-use and end-user controls to protect additional technology chokepoints.
- Furthermore, the new controls expanded the FDP rule's applicability to additional types of chips and SME.[43]

[38] Reinsch, Schleich, and Denamiel, 2023.

[39] Reinsch, Schleich, and Denamiel, 2023.

[40] Reinsch, Schleich, and Denamiel, 2023.

[41] Office of Congressional and Public Affairs, 2023a.

[42] Office of Congressional and Public Affairs, 2023a.

[43] Gregory C. Allen, "Understanding the Biden Administration's Updated Export Controls," CSIS, December 11, 2024b.

- The new policy also addresses the need for buy-in from countries involved in semiconductor manufacturing by offering certain countries, such as Japan and the Netherlands, exemptions and incentives to adjust their domestic export controls to align with the goals of the U.S. AI export control regime.
- The new rules implemented further create new red-flag guidance, increasing the stringency of due diligence for exports.
- They also added 140 new entities to BIS Entity List and created a restricted–fabrication facility exception.

These policies align with the rationale behind the 2022 and 2023 controls.[44]

The HBM rule specifically targets Chinese companies that already design advanced AI chips—both those that already design such chips (e.g., Huawei) and those that have the capability (e.g., mainly, international semiconductor manufacturing corporations). HBM enables more-efficient use of memory, which cuts down on time and costs by allowing chips to run near full utilization. Companies that aim to design, manufacture, and sell advanced chips need HBMs. The HBM rule prohibits the sale of HBMs to countries headquartered in China and companies headquartered in the 24 countries in group D:5 (U.S. arms-embargoed countries, which include Russia, North Korea, and Iran).[45] The rule does this by requiring a license for all exports with a presumption of denial for companies in these countries. The United States and the Republic of Korea (ROK) dominate the HBM market, making the ROK's cooperation on this rule critical. The rules do allow the sale of older, lower-performing HBMs to China, with the requirements that HBMs be sold directly to end users and that those end users not use HBMs for AI applications or to produce advanced chips. The metric for advanced HBM is memory bandwidth density, which is a threshold set at 3.3 GB per second per square millimeter. Any HBMs more advanced than second-generation HBM (HBM2) will not be allowed to be sold to China. These HBMs were introduced in 2016.[46]

Updating the list of restricted SME was an attempt to address loopholes that were allowing China to manufacture equipment, including equipment used to create through-silicon vias (TSVs),[47] which are critical for the production of HBM, with the goal of allowing TSV equipment needed for legacy chip production.[48]

Equipment that is used specifically to manufacture advanced semiconductors, which CSIS has called *advanced-node equipment*, is subject to countrywide restrictions. In contrast, a broader set of equipment that is intended to produce legacy-node chips in addition to advanced-node chips (CSIS has called this *node-agnostic equipment*) is subjected to end-user and end-use restrictions. Most of the node-agnostic equipment targeting is done through end-user restrictions. These regulations are intended to prevent the use of multipatterning, through which deep ultraviolet lithography systems

[44] Allen, 2024b.

[45] These countries are identified at 15 C.F.R. Part 740, Supplement 1, Country Groups.

[46] Allen, 2024b.

[47] In this context, a via is a connection between two ICs.

[48] Allen, 2024b.

can produce advanced chips that would not be possible otherwise. This is critical to prevent Huawei's production of 7-nm node chips, and effects will be greatly improved with cooperation from allies.[49]

The new FDP rules and the update of de minimis provisions are meant to secure cooperation with allies and partners. This is notable because these are attempts to greatly expand the applicability of U.S. export controls to other countries' transfer of advanced chip–related technology. The de minimis update changes the threshold percentage of a foreign product that can contain restricted U.S. equipment and still be designated a U.S. product and be subject to U.S. export control provisions—although, in some cases, having any U.S. content means that a product is subject to U.S. rules. The new rule means that any piece of SME that includes a U.S. semiconductor chip made using U.S. SME or is made with U.S. SME or U.S. chip design software could be subject to U.S. export controls.[50] This could apply to all SME globally such that even Chinese-made SME made in China could be subject to the FDP rule. The United States does not expect success in enforcing compliance with Chinese firms, but the FDP rule should affect the behavior of U.S. companies and of foreign companies with headquarters in U.S.-allied countries, exposing those companies to significant financial and legal risk. This rule prevents U.S. SME firms that have left the United States to skirt export controls from seeking loopholes by outsourcing manufacturing. It also prohibits foreign companies, such as Advanced Semiconductor Materials Lithography (ASML), Tokyo Electron, and SEMES, from exporting U.S. equipment. However, this rule does not apply to reexports or exports from abroad when made from a country's home market as long as that market has controls that align with those of the United States. This rule covers lithography tools (deep ultraviolet) and extreme ultraviolet and advanced etching and deposition SME. The SME FDP rule will apply country-based restrictions to lithography tools, and the FDP rule for Footnote 5 entities imposes stricter regulations on those technologies on those entities.[51]

The exemptions in the FDP rules reduce the incentives for Dutch and Japanese firms to outsource manufacturing abroad. ASML threatened to relocate in 2024; these new export controls apply to firms even if they move their headquarters abroad. Supplement 4 to 15 C.F.R. Part 742 lists 33 countries that are excluded from some SME restrictions; these include Japan, Australia, the United Kingdom (UK), and various European Union (EU) countries but not some others in the supply chain, such as Taiwan, the ROK, and Singapore. It is notable that these excluded countries have not aligned their export controls with those of the United States, so all of their exports of SME are subject to the revised FDP rule. This creates an incentive for the ROK to align its export controls with those of the three major players in chip manufacturing—United States, Japan, and the Netherlands—although the potential for retaliation from China still provides a negative incentive.[52]

---

[49] Allen, 2024b.

[50] Allen, 2024b.

[51] Allen, 2024b. *Footnote 5* is a reference to 15 C.F.R. § 734.9(h)(1), Product Scope of Advanced Computing FDP Rule, note 5:

> See Note 1 to ECCN 3A090, because when a "front-end fabricator" or "OSAT" [outsourced semiconductor assembly and test] company is seeking to export, reexport, or transfer (in-country) an "applicable advanced logic integrated circuit," there is a presumption that the commodity is 3A090.a and designed or marketed for datacenters."

[52] Allen, 2024b.

The October 2022 export controls created end-use restrictions on semiconductor fabrication plants in China that were producing certain logic and memory semiconductors. These controls restricted U.S. firms from knowingly transferring virtually any goods or services to restricted end users. However, the controls were not as effective as intended. Industry sources have claimed that Chinese firms used networks of shell companies and partner firms to acquire U.S. equipment through deception. In response, the 2024 controls increased due-diligence requirements, adding eight red flags for firms' assessments of customers. These more-stringent requirements will make it more difficult for exporters to unknowingly violate export controls.[53]

The controls also added 140 new firms to the Entity List for risk of diversion. The renewed focus on the Entity List helps both Japan and the Netherlands mitigate their lack of resources and staff for export controls and gives them clear guidance. The Entity List additions also address gaps in allied controls.[54]

Historical Context for Uncrewed Aircraft System Controls

The Missile Technology Control Regime

The Missile Technology Control Regime (MTCR) applies to two categories of missile systems and UASs based on range and payload capabilities. Category I is for systems capable of reaching a range of 300 km and carrying a payload of 500 kg; typically, their potential military use warrants a strong presumption of denial for exporting these items. Category II encompasses systems that also have a range of 300 km but lack the payload capacity of Category I items. The export of Category II systems is considered more leniently, being evaluated on a case-by-case basis.[55] Items that do not meet the specifications of Category I or II are not controlled under the MTCR. The control of most complete systems from Categories I and II usually falls under the jurisdiction of DOS. However, these classifications also influence the licensing decisions for dual-use commodities, which are controlled by DOC. Classifications of systems consider the intended end use of the items, the capabilities of the destination country, and the risk that the items will be diverted to unintended users.[56]

In 2021, the MTCR guidelines were amended to ease restrictions on some UASs previously considered Category I to increase global trade opportunities and expand opportunities for U.S. companies to engage in the international UAS market. According to DOS's Bureau of Political–Military Affairs, this policy was also intended to strengthen bilateral and multilateral relationships and support international security and counterterrorism objectives by allowing the transfer of advanced and other UAS technologies to international partners and allies.[57] Under the new guidelines, export licensing for UASs that fall under Category I but have a maximum true airspeed of less than 800 km per hour are to be reviewed on case-by-case basis under the same flexible review policies applied to

[53] Allen, 2024b.

[54] Allen, 2024b.

[55] BIS, DOC, "BIS Website: Missile Technology FAQs," webpage, undated.

[56] BIS, undated.

[57] Bureau of Political–Military Affairs, DOS, "U.S. Policy on the Export of Unmanned Aerial Systems," fact sheet, undated.

Category II UASs.[58] The policy allows transfers of armed and unarmed UASs through either direct commercial sales or foreign military sales. According to the policy, recipients must obtain U.S. government permission to integrate non-U.S. systems with U.S. systems transferred under the MTCR or to arm UASs that were transferred unarmed. It also contains strict controls for any UAS, including advanced combat UASs, that is capable of delivering WMD. Additionally, the policy contains provisions for the monitoring of adherence to U.S. policies on end use of all UASs transferred under the MTCR, which also obligate recipients to operation such systems within the bounds of international humanitarian and human rights law.[59]

Uncrewed Aircraft Systems and the Wassenaar Arrangement

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA) is an international framework that was put in place in 1996 following the Cold War, in which member states voluntarily participate to implement export controls on specific items through national laws, as agreed upon in a collective List of Dual-Use Goods and Technologies and Munitions List.[60] Members are required to report every six months on the transfer of regulated dual-use items and to exchange information about potential transfers with other members. Every December, the WA participant states convene in Vienna to review and update the list of controlled items, share relevant information, and adopt new measures to enhance the enforcement of export controls.[61] The WA currently has 42 signatories, including North America, the majority of Europe, Argentina, Australia, India, Japan, New Zealand, the ROK, Russia, South Africa, Turkey, the UK, and Ukraine.[62] The geopolitical environment at the time of this writing, however, including Russia's invasion of Ukraine, poses challenges to the WA's utility. The recent export controls targeting Russia, which include limits on semiconductors, were developed outside the WA because Russia is a WA member state. Furthermore, it is unlikely in the current environment that Russia would agree to any new export controls under the WA.[63]

The 2023 List of Dual-Use Goods and Technologies and Munitions List includes uncrewed aerial vehicles (UAVs) and related equipment; it also includes components that have a maximum endurance of at least 30 minutes and that are designed to take off and have stable flight in wind gusts of at least 25 knots, or a maximum endurance of 1 hour or more.[64] Per the WA, participating states are to ensure, through national export control policies, that the export of items on the List of Dual-Use

[58] BIS, DOC, "Change to the License Review Policy for Unmanned Aerial Systems (UAS) to Reflect Revised United States UAS Export Policy," *Federal Register*, Vol. 86, No. 7, January 12, 2021a (final rule).

[59] Bureau of Political–Military Affairs, undated.

[60] Gregory C. Allen and Emily Benson, "Clues to the U.S.–Dutch–Japanese Semiconductor Export Controls Deal Are Hiding in Plain Sight," CSIS, March 1, 2023; WA Secretariat, *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public Documents*: Vol. II, *List of Dual-Use Goods and Technologies and Munitions List*, 2023.

[61] Sujai Shivakumar, Charles Wessner, and Hideki Tomoshige, "Toward a New Multilateral Export Control Regime," commentary, CSIS, January 10, 2023.

[62] WA, "About Us," webpage, undated.

[63] Shivakumar, Wessner, and Tomoshige, 2023.

[64] WA Secretariat, 2023. A UAV is an aircraft; a UAS is the system of technologies needed to operate it (e.g., ground control, communication, software). A UAV is part of a UAS.

Goods and Technologies and Munitions List do not contribute to military capabilities that undermine the goals of regional and international security and stability. Through its reporting requirements, the WA seeks to promote transparency and accountability among member states for the transfer of such dual-use goods and technologies.[65]

Uncrewed Aircraft Systems and the International Traffic in Arms Regulations: U.S. Munitions List

DOS, through the Directorate of Defense Trade Controls (DDTC), is responsible for the export and import of defense-related articles and systems. These defense-related articles and systems listed on the U.S. Munitions List (USML) are covered and regulated by the ITAR.[66] The statutory basis for the ITAR is the implementing provisions of the Arms Export Control Act, which governs all U.S. military transfers, as described in Title 22 of the Code of Federal Regulations.[67] The ITAR sets out licensing policy for exports and temporary imports of USML items based on the nature of the item rather than that of the end use or user of the item. A U.S. person can face severe fines if they have, without proper authorization or use of an exemption, provided a foreign person with access to a defense article, service, or technical data protected under the ITAR. Presumptions of denial (the initial assumption that any request for license to export will be denied) still exist for UAVs specifically designed for a defense purpose and will therefore be controlled under the ITAR. Any firm involved in the manufacturing or exporting of any item on the USML must register with DDTC and pay a yearly fee. DDTC is also tasked with updating the ITAR on a regular basis. The ITAR provides a mechanism for the U.S. government to authorize the manufacture of U.S.-origin defense articles abroad; the mechanism requires a contract between the U.S. manufacturer and foreign party.[68]

The USML categorizes defense articles and services based on their military utility (both intended and potential use as a military weapon). UAVs are classified and controlled by the USML under Categories VIII(a)(5) and VIII(h)(12). Category VIII, covering aircraft and related articles, specifically controls UAVs in the former with controlling UAVs "specially designed to incorporate a defense article" and in the latter with controlling UAV "flight control systems and vehicle management systems with swarming capability."[69] Components of UAVs are also subject to ITAR-related controls, including fire control systems, launching systems, guidance and navigation systems, and anticollision capabilities.[70]

---

[65] WA, undated.

[66] Global Information Services, Bureau of Administration, DOS, "Defense Export Control and Compliance System (DECCS)," privacy impact assessment, January 4, 2022.

[67] Public Law 90-629, Arms Export Control Act, October 22, 1968; U.S. Code, Title 22, Chapter 39, Arms Export Control.

[68] Bureau of Political–Military Affairs, DOS, "Myths and Facts About U.S. Defense Export Controls," fact sheet, July 10, 2023.

[69] Code of Federal Regulations, Title 22, Chapter I, Subchapter M, Part 121, Section 121.1, The United States Munitions List, Category VIII(a)(5), UAVs specially designed to incorporate a defense article; 22 C.F.R. § 121.1, Category VIII(h)(12), aircraft capable of being refueled in flight, including hover-in-flight refueling.

[70] 22 C.F.R. § 121.1, Category VIII(h)(6), reserved; 22 C.F.R. § 121.1, Category XII, Fire Control, Laser, Imaging, and Guidance Equipment; 22 C.F.R. § 121.1, Category VIII(h)(12).

Uncrewed Aircraft Systems, the Export Administration Regulations, and the Commerce Control List

DOC, through BIS, is charged with implementing and enforcing the EAR to protect U.S. national security. The EAR regulate exports of *commercial items* that might have dual military uses. The CCL is part of the EAR (Supplement 1 to Part 774) and is maintained by BIS. The CCL contains all dual-use items that are subject to BIS export licensing authority. To export any item on the CCL, an export license might be required, although this depends on the item and intended country of export.[71] Any item on the CCL that has been designated with a specific ECCN requires an export license. Any item that falls under DOC's jurisdiction but that is not listed on the CCL with a specific ECCN is designated as EAR99. Such an item is generally low-technology and might not require a license in all situations. It might, however, require an export license if it is being exported to an embargoed country, to a user that is of concern, or for a prohibited end use.[72]

The CCL contains numerous items related to UASs that can reach a range equal to or greater than 300 km and includes associated systems and components for such UASs, including engines, software, navigation and guidance systems, fuselages, and propulsion systems.[73]

Export Control Measures Under the Export Administration Regulations to Address Iranian Uncrewed Aerial Vehicles and Their Use by the Russian Federation Against Ukraine, February 27, 2023

In February 2023, DOC's BIS introduced amendments to the EAR with stringent new export controls against Iranian UAVs and their use by Russia in its conflict with Ukraine. These measures were responding to U.S. national security and foreign policy concerns: The deployment of these UAVs would enhance Russia's military capabilities, potentially degrading international peace efforts by refilling depleted Russian stockpiles.[74] With these updates, the EAR now include additional licensing requirements for a subset of EAR99 items, which can generally be exported without a license.[75] These items, often destined for Iran, are identified by Harmonized Tariff Schedule (HTS) 6 codes, detailed in a new supplement added to the EAR.[76] Their inclusion allows the United States to more effectively track and restrict exports that could support the production of Iranian UAVs. In addition, these amendments introduced a new FDP rule tailored to Iran, targeting CCL Categories 3 through 5 or 7 and the aforementioned EAR99 items.[77] The FDP rule stipulates that certain foreign-produced items, either as direct products of U.S.-origin technologies or software or produced in

---

[71] BIS, DOC, "Supplement No. 1 to Part 774: The Commerce Control List," Export Administration Regulations, Chapter VII, last updated January 6, 2025a.

[72] BIS, 2025a.

[73] Code of Federal Regulations, Title 15, Subtitle B, Chapter VII, Subchapter C, Part 774, The Commerce Control List, Supplement 1; Baums, 2024; BIS, DOC, "Request for Comments Concerning Imposition of Export Controls on Brain–Computer Interface (BCI) Emerging Technology," *Federal Register*, Vol. 86, No. 204, October 26, 2021b (proposed rule).

[74] BIS, DOC, "Export Control Measures Under the Export Administration Regulations (EAR) to Address Iranian Unmanned Aerial Vehicles (UAVs) and Their Use by the Russian Federation Against Ukraine," *Federal Register*, Vol. 88, No. 38, February 27, 2023 (final rule).

[75] International Trade Administration, "Export Control Classification # (ECCN) and (EAR99)," webpage, undated.

[76] BIS, 2023.

[77] BIS, 2023.

facilities that are themselves products of U.S.-origin technologies or software, are subject to their EAR when their destination is Iran. Simultaneously, the existing FDP rule for Russia and Belarus has been revised to incorporate those foreign-produced items, ensuring equivalence in the level of control for these countries.[78] This revision was added as part of a broader strategy to align with international efforts to degrade the operational capabilities of the Iranian UAV program and curtail Russia's military use of such UAVs in Ukraine. These changes were enacted along with measures from U.S. allies and partners, including restrictions imposed by the EU on identified Iranian drone companies.[79] These efforts, both domestic and international, are aimed at preventing Iran from obtaining the components necessary for manufacturing UAVs—in particular, those that are destined for Russian use.

Guidance to Industry on Iran's Uncrewed Aerial Vehicle–Related Activities, June 9, 2023

The United States and the United Nations (UN) have established various sanction regimes aimed at curbing Iran's procurement and proliferation of UAVs and associated components. These sanctions are detailed in several U.S. and international legal frameworks, described as follows.[80]

- The Iran, North Korea, and Syria Nonproliferation Act mandates periodic reports to Congress about foreign individuals involved in transferring specific items to Iran, Syria, or North Korea. Sanctions on items listed in the reports can include bans on U.S. government procurement, assistance, imports, and the export or reexport of dual-use items and munitions.[81]
- The Arms Export Control Act and the Export Administration Act of 1979 authorize sanctions against foreign persons who transfer items that aid missile production in non-MTCR countries, with penalties that might include denial of U.S. government contracts or export licenses.[82]
- Executive Orders 12938 and 13382 call for sanctions against foreign persons who contribute to the proliferation of WMD and their delivery systems, including activities that pose a risk of such proliferation. They also confer the authority to impose one or more blocking sanctions on entities that provide support to already-sanctioned entities and orders the relevant federal agencies to do so as they deem necessary.[83]

[78] BIS, 2023.

[79] BIS, 2023.

[80] Office of Foreign Assets Control (OFAC), U.S. Department of the Treasury, "Guidance to Industry on Iran's UAV-Related Activities," undated.

[81] OFAC, undated; Public Law 106-178, Iran Nonproliferation Act of 2000, March 14, 2000, as amended by Public Law 109-353, North Korea Nonproliferation Act of 2006, October 13, 2006.

[82] OFAC, undated; Public Law 90-629, 1968; Public Law 96-72, Export Administration Act of 1979, September 29, 1979.

[83] OFAC, undated; William J. Clinton, "Executive Order 12938 of November 14, 1994: Proliferation of Weapons of Mass Destruction," *Federal Register*, Vol. 59, No. 220, November 16, 1994; George W. Bush, "Executive Order 13382 of June 28, 2005: Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters," *Federal Register*, Vol. 70, No. 126, July 1, 2005.

- Executive Order 13949 targets individuals involved in transferring arms to or from Iran and those supporting Iran's paramilitary organizations; it authorizes imposing blocking sanctions.[84]
- The Iran Freedom and Counter-Proliferation Act of 2012 mandates sanctions on those involved in the transfer to or from Iran of specific materials and on those providing certain services, such as insurance or financial transactions that support sanctioned Iranian entities.[85]
- Countering America's Adversaries Through Sanctions Act (CAATSA), Section 107, imposes sanctions on persons who contribute to the supply, sale, or transfer of military equipment to or from Iran or who provide Iran with related training and services.[86]
- UN Security Council Resolution 2231 (2015) controlled the transfer of items listed under the MTCR to or from Iran, requiring the UN Security Council's permission for such transfers until October 18, 2023.[87]

These provisions reflect a comprehensive effort to limit Iran's capabilities in UAV development and proliferation through stringent controls and sanctions on international transactions and activities.[88]

DOC, the U.S. Department of Justice (DOJ), DOS, and the U.S. Department of the Treasury have jointly issued an advisory to globally alert individuals and businesses about the increasing threat posed by Iran's activities in procuring, developing, and proliferating UAVs. This advisory emphasizes the need for vigilance and appropriate measures to prevent any support for Iran's UAV program and highlights the potential risks associated with involvement in transferring technology or components. The United States is actively working to counter Iran's UAV initiatives by preventing the misuse of the U.S. financial system and disrupting the procurement of foreign-sourced components essential for these programs. The advisory calls on private industry to be aware of its legal obligations under U.S. export controls and sanctions, recommending robust due diligence, compliance structures, and internal controls to ensure adherence to legal standards across supply chains. It is intended to prevent companies from indirectly or directly contributing to Iran's UAV programs through transfers to third-country suppliers, thereby protecting broader U.S. and international security interests. This proactive approach underscores a commitment to international peace and security by mitigating the risks associated with Iran's expanding UAV capabilities.[89]

The United States enforces a comprehensive trade embargo against Iran through the Department of the Treasury's OFAC, as outlined in the Iranian Transactions and Sanctions Regulations (ITSR).[90] This embargo generally prohibits U.S. persons and entities from engaging in most transactions

[84] Donald J. Trump, "Executive Order 13949 of September 21, 2020: Blocking Property of Certain Persons with Respect to the Conventional Arms Activities of Iran," *Federal Register*, Vol. 85, No. 185, September 23, 2020.

[85] OFAC, undated; Public Law 112-239, National Defense Authorization Act for Fiscal Year 2013, January 2, 2013, Division A, Title XII, Subtitle D, Iran Sanctions.

[86] OFAC, undated; Public Law 115-44, Countering America's Adversaries Through Sanctions Act, August 2, 2017, Section 107, Enforcement of Arms Embargos.

[87] OFAC, undated; UN Security Council, Resolution 2231 (2015), S/RES/2231 (2015), July 20, 2015.

[88] OFAC, undated.

[89] OFAC, undated.

[90] Code of Federal Regulations, Title 31, Subtitle B, Chapter V, Part 560, Iranian Transactions and Sanctions Regulations.

involving Iran, including commercial, financial, or trade activities, unless these actions are exempted by statute or authorized by OFAC. Additionally, U.S. persons must block any Iranian government's or financial institution's transaction, financial property movement, and access to data or defense items that comes under a U.S. person's possession or control.[91]

The ITSR also restricts non-U.S. persons from reexporting any goods, technology, or services from third countries to Iran that originated from the United States, make up 10 percent or more of the content by value, and are still under U.S. export licensing requirements. A violation can occur if a non-U.S. person exports a service from the United States to Iran or engages in U.S. dollar–denominated transactions through U.S. financial institutions for goods or services related to Iran without proper authorization.[92]

Moreover, individuals or entities providing material support to those listed on the Specially Designated Nationals (SDN) and Blocked Persons List (SDN List) can face sanctions, including potential addition to the SDN List.[93] A foreign financial institution that facilitates a significant transaction for a designated individual or entity risks sanctions, which could include restrictions on its access to the U.S. financial system.[94]

The United States has also designated numerous Iranian entities and individuals under various sanctioning authorities, including Executive Orders 13382 and 14024.[95] These designations target those involved in the UAV sector, including those in production, development, procurement, and proliferation of UAV systems. Notable designations include Qods Aviation Industries, Shahed Aviation Industries, and Safiran Airport Services for their roles in enhancing Iran's UAV capabilities.[96]

DOJ is spearheading two major interagency law enforcement initiatives aimed at undermining Iran's capacity to acquire UAV technology. The first, Task Force KleptoCapture, was initiated in March 2022 to enforce the sanctions, export controls, and other economic countermeasures imposed on Russia following its unprovoked military invasion of Ukraine. A central goal of this task force is to sever the supply chain facilitating the transfer of UAVs from Iran to Russia, which are being deployed against the Ukrainian populace. Then, in February 2023, DOJ and BIS launched the Disruptive Technology Strike Force. This interagency collaboration is dedicated to investigating and prosecuting the illicit transfer of sensitive technologies to foreign-state adversaries, including Iran, thereby addressing a critical aspect of national security.[97]

In 2022 and 2023, BIS added a total of 42 entities to the Entity List:

- Eleven of these entities are directly involved in the Iran–Russia collaboration to establish a UAV production facility in Russia's Alabuga Special Economic Zone. This facility is

[91] OFAC, undated.

[92] OFAC, undated.

[93] OFAC, U.S. Department of the Treasury, "Specially Designated Nationals (SDNs) and the SDN List," released June 2, 2021.

[94] OFAC, undated.

[95] Bush, 2005; Joseph R. Biden, Jr., "Executive Order 14024 of April 15, 2021: Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation," *Federal Register*, Vol. 86, No. 74, April 19, 2021.

[96] OFAC, undated.

[97] OFAC, undated.

reportedly aimed at mass-producing Shahed-136 drones to bolster Russia's military actions in Ukraine.

- Two entities were specifically targeted for their roles in illicitly procuring and diverting critical U.S.-origin electronic components that have applications in military technologies, such as avionics, missiles, UAVs, electronic warfare receivers, and military radars.
- Thirteen entities were added for their transactions with other entities already on the Entity List or sanctioned by OFAC, indicating a network of collaboration that undermines international sanctions and export controls.
- Sixteen additional entities were listed following two major BIS enforcement actions that revealed schemes involving the acquisition and diversion of U.S.-origin electronic and avionics components to support Russian military endeavors.

These listings were part of a coordinated effort with the unveiling of an indictment by the U.S. Attorney's Office for the District of Oregon, targeting Belgian national Hans Maria De Geetere, following investigations by the Disruptive Technology Strike Force.[98]

These targeted entities have been actively involved in circumventing U.S. export controls to facilitate the acquisition of technology that can significantly enhance Russia's and Iran's military capabilities. Diverted technologies are critical for the development of advanced military systems, including precision-guided weapons, enhancing adversary states' military capabilities.[99] Actions were taken under the Export Control Reform Act of 2018, which empowers BIS to regulate exports that threaten national security.[100] Entities are added based on concrete evidence that they engage in activities contrary to U.S. national security or foreign policy interests.[101]

The newly added entities are in multiple countries, which highlights the global nature of the procurement networks that support Russia's and Iran's military advancements. Entities with a Footnote 3 designation are subjected to the Russia/Belarus—Military End User (MEU) FDP rule, which imposes strict licensing requirements and typically reviews license applications under a presumption of denial unless exceptions are justified for humanitarian reasons.[102]

These measures underscore U.S. resolve to leverage U.S. regulatory frameworks to combat the proliferation of military technologies in adversarial nations, thereby contributing to global security and stability.[103]

---

[98] Office of Congressional and Public Affairs, BIS, DOC, "Commerce Adds 42 Entities to the Entity List for Supporting Russia's Military, Including Co-Production of Drones with Iran," press release, December 6, 2023b.

[99] Office of Congressional and Public Affairs, 2023b.

[100] Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, August 13, 2018, Division A, Title XVII, Subtitle B, Export Control Reform.

[101] Office of Congressional and Public Affairs, 2023b.

[102] Office of Congressional and Public Affairs, 2023b. *Footnote 3* is a reference to 15 C.F.R. § 734.9(e)(3)(i)(B)(2), note 3:

> The product scope of paragraph (e)(3)(i) is met if a foreign-produced commodity contains an integrated circuit that is produced by a complete plant or 'major component' of a plant that itself is a "direct product" of U.S.-origin "technology" or "software" specified in the ECCNs described in paragraph (e)(3)(i)(B)(2). See Red Flag 26 in supplement no. 3 to part 732 for additional guidance on the scope of paragraph (e)(3)(i). Production of an integrated circuit includes fabrication of the integrated circuit in a wafer, as well as assembly, testing, and packaging of the integrated circuit.

[103] Office of Congressional and Public Affairs, 2023b.

Chapter 3

Performance of Export Control Measures: Challenges and Opportunities

This chapter provides analysis on insights we derived from our semistructured discussions with people from relevant agencies, the private sector, and academia. We held discussions with more than 25 individuals from DOC, DoD, and DOS, as well as private-sector stakeholders and other expert researchers. We developed a semistructured protocol that addressed our research questions that started with us asking what the de facto export control process was, what the most-relevant factors were, and what challenges and opportunities were prevalent in developing successful export control regulations for AI and UASs. In this chapter, we first review what the participants deemed the most-critical parts of the process and then review the types of challenges and opportunities that arose during that process.

A Review of the Dual-Use Export Control Process

The processes for establishing dual-use export controls on AI technologies and UASs involve a complex interplay of national and international regulatory frameworks. These frameworks are intended to balance national security concerns with trade and technological advancement. In each of our discussions, we asked participants to outline different organizations' roles in this process within these frameworks so we could map out the process as it occurs on the ground.

Initially, U.S. government agencies—including DOC, DoD, and DOS—identify technologies that could pose national security risks if exported. This includes AI- and UAS-related technologies that are critical to national security and those with dual-use potential.

Industry plays a significant role in this process, mainly through its involvement in technology advisory committees (TACs).[104] These committees, composed of representatives from both industry and government, provide technical advice to DOC on export controls for dual-use commodities and technologies. Members of TACs are appointed by the Secretary of Commerce, serve four-year terms, and must obtain Secret-level clearances. The responsibility of TACs has steadily increased over the decades, having integrated working groups from both DoD and the U.S. Department of Energy.[105] Technologies are submitted for regulation through industry, government, or a WA multilateral proposal.[106] Once identified, these technologies are added either to the CCL under the EAR or to the

[104] Stakeholder, interview with the authors, July 2024.

[105] Stakeholder, interview with the authors, July 2024.

[106] Stakeholder, interview with the authors, July 2024.

USML under the ITAR. This designation dictates the specific licensing requirements and restrictions applicable to the export of these technologies.

The implementation and enforcement of export controls include stringent licensing processes, end-use monitoring, and international cooperation to prevent proliferation. In this process, BIS plays a pronounced role, serving as both a legal authority and an implementer, although DoD does not enforce export policy. The licensing process is critical, involving a multiagency review that includes reviews by DOC, DOS, DoD, and the U.S. Department of Energy.[107] The fact that AI is developing rapidly means that licensing requirements and controls are frequently updated. As of January 2025, controls had been expanded to include AI model weights, which are the numerical parameters within a model that determine the model's outputs.[108]

BIS also maintains several lists of parties of concern for these technologies, all under the EAR. This includes the MEU List, the Entity List, and Unverified List.[109] The MEU List identifies end users in countries that, like China, Russia, and Venezuela, are considered high risks for military use or diversion and are thus barred from receiving items with military applications unless a license is obtained.[110]

The Entity List covers a broader population of end users subject to specific license requirements for exports, reexports, and transfers of items under the CCL. An entity is added to the list based on activities contrary to U.S. national security or foreign policy interests, with a significant portion of nominations coming from BIS export enforcement analysts and frequently having ties to investigations conducted by BIS law enforcement agents.[111] Most end users on the Entity List face a presumption of denial for their license applications; for those not fully restricted, the list specifies which items and transactions might be considered for approval on a case-by-case basis.

The Unverified List contains parties whose legitimacy or reliability in export transactions cannot be confirmed in the physical end-use checks conducted by BIS.[112] A party on this list is restricted from using license exceptions, and any license application involving such a party requires further checks by BIS. In October 2022, BIS updated its policy for the Unverified List, requiring that, if the physical end-use check is not completed within 60 days, the party be moved to the Entity List.[113]

The enforcement process relies on due diligence from exporters, requiring them to implement robust compliance measures to ensure adherence to U.S. export control laws. This involves verifying both the end user and end use of the technology to prevent unauthorized diversion. Compliance programs are essential for monitoring export activities and are incentivized by BIS through outreach

[107] Stakeholder, interview with the authors, September 2024.

[108] BIS, 2025b.

[109] Alan F. Estevez, "Statement of Alan F. Estevez, Undersecretary of Commerce for Industry and Security, U.S. Department of Commerce," testimony for U.S. House of Representatives Committee on Foreign Affairs hearing, Combating the Generational Challenge of CCP Aggression, February 28, 2023. These lists are Supplements 4, 6, and 7, respectively, of Title 15, Subtitle B, Chapter VII, Subchapter C, Part 744, Supplement 4, Entity List; Supplement 6, Unverified List; and Supplement 7, "Military End-User" (MEU) List.

[110] Stakeholder, interview with the authors, November 2024.

[111] Stakeholder, interview with the authors, November 2024.

[112] BIS, DOC, "Revisions to the Unverified List; Clarifications to Activities and Criteria That May Lead to Additions to the Entity List," *Federal Register*, Vol. 87, No. 197, October 13, 2022 (final rule).

[113] Stakeholder, interview with the authors, November 2024.

programs, published advisories and best practices, and updated policies on voluntary self-disclosures.[114]

The United States engages in bilateral agreements and multilateral forums to align export control policies with those of allies, ensuring a unified approach to mitigate the risks associated with the proliferation of advanced UAS and AI technologies. This includes the MTCR, the WA, and working groups with the EU, Japan, the ROK, and Five Eyes partners.[115] This cooperation also exists between U.S. agencies. For example, in February 2023, BIS and DOJ announced the formation of the Disruptive Technology Strike Force, which aims to protect U.S. advanced technologies from being illicitly acquired and used by nation-state adversaries to support military modernization efforts designed to overcome U.S. military superiority or mass surveillance programs enabling human rights abuses.[116] This collaborative effort between agencies and international bodies is critical in maintaining global security and preventing the misuse of these systems.[117]

Overall, the current process of U.S. export controls for dual-use and commercial AI and UAS technologies is characterized by a multifaceted regulatory framework that involves extensive collaboration between government agencies and industry stakeholders. As technological advancements continue to evolve, ongoing adaptation and coordination will be necessary to ensure that export controls effectively address national security concerns while fostering innovation and international trade. The interplay between regulatory compliance, enforcement, and international cooperation remains critical in navigating the challenges associated with the export of sensitive technologies.

Export controls for military technologies go through a similar and parallel process through DDTC, which manages the ITAR, which contains the USML. Navigating the USML is generally a stricter process with mandatory registration.[118]

Challenges and Opportunities

A variety of factors are increasing the burden on agencies' ability to regulate, enforce and ensure compliance:[119]

- rapid evolution of AI and UAS technologies
- global demand spike for AI and UAS technologies
- increases in the number and strictness of regulations increasing case loads
- increases in dual-use cases
- staffing, funding and skill gaps within DOC's BIS
- interagency cooperation

[114] Stakeholder, interview with the authors, September 2024.

[115] *Five Eyes* refers to the Five Eyes Intelligence Oversight and Review Council (see National Counterintelligence and Security Center, Office of the Director of National Intelligence, "Five Eyes Intelligence Oversight and Review Council [FIORC]," webpage, undated).

[116] OFAC, undated.

[117] Stakeholder, interview with the authors, September 2024.

[118] DDTC, DOS, "ITAR and Export Controls," webpage, undated.

[119] Stakeholder, interview with the authors, September 2024.

- multilateral considerations.

As export controls for both AI and UASs become increasingly complicated and address a rapidly growing number of technologies and aspects of technologies, enforcement mechanisms become more intricate. This leads to a gap in resources, including staffing, skill sets, and materiel aspects. This is complicated by complex evasion networks and growing demand for regulated technologies. Agility is a critical measure for efficacy, but it is a difficult one to create a metric for. Enforcement mechanisms must be agile, and, for that to be possible, legal frameworks need to be explicit and detailed for enforcement to target, prosecute, and plug loopholes.[120]

Expanding Yard, Expanding Fence

The initial BIS strategy sought to restrict a small number of technologies and entities at a high level. However, subsequent rounds of export controls have indicated that the need to expand this grew rapidly alongside the technology.[121] At the core, policy and regulation do not keep up with the changes and dissemination of technologies, which leads to a variety of struggles, including the effort to keep regulatory language current with updates in technology language. Export controls ultimately serve as a delay rather than a permanent solution to the technological dangers posed by AI and UASs.[122] Some have concerns that export controls are increasingly proposed as a solution to the economic and technology competition problem in U.S. policy.[123] This expansion of controls increases the number and complexity of restrictions being put into place, which leads to increased numbers of licensing applications and increases the time and resources required to process licenses and enforce export controls.[124]

Funding and Access to Expertise

AI export controls have numerous hurdles with funding and access to staffing and expertise, particularly trying to control technologies with small, sometimes digital parts that are easy to smuggle and divert. BIS funding, staffing, and facilities have struggled to keep pace with the rapid expansion of AI technology and the rapid increase of export controls and export control products. In discussions, these challenges were often attributed to AI, but it is interesting that many of the underlying mechanisms could apply to UASs as well if volume were to increase. There is also evidence that BIS lags in access to the modern data-driven technology strategies used in other government organizations.[125] In 2023, the number of candidates for inspection was already greater than BIS

[120] Gregory C. Allen, Emily Benson, and William Alan Reinsch, "Improved Export Controls Enforcement Technology Needed for U.S. National Security," CSIS, November 30, 2022; Shivakumar, Wessner, and Howell, 2024.

[121] Shivakumar, Wessner, and Howell, 2024.

[122] Shivakumar, Wessner, and Howell, 2024.

[123] Stakeholder, interview with the authors, November 2024.

[124] Stakeholder, interview with the authors, November 2024; Shivakumar, Wessner, and Howell, 2024.

[125] Shivakumar, Wessner, and Howell, 2024; Allen, Benson, and Reinsch, 2022; Gregory C. Allen, director, Wadhwani Center for AI and Advanced Technologies, CSIS, "Advanced Technology: Examining Threats to National Security," statement before

staffing capacity. That same year, CSIS recommended an $18.4 million annual increase over the same period to address enforcement staffing. CSIS also recommended a five-year, $25 million annual increase in the BIS budget to increase the resources in BIS analytical staff and technology for analytical capabilities.[126] As of 2025, although BIS had received some additional funding ($223 million allocated in fiscal year 2025), the bureau fell greatly short of the overall five-year goal.[127] This level of investment would need to be sustained. Sources have indicated that BIS has performed admirably in enforcing a barrage of export controls in a technological and international environment that continues to shift rapidly but that BIS seems to be playing whack-a-mole.[128] Many of these same issues apply to the UAS field. UASs can be broken down into small components and even into digital assets that can be smuggled and diverted in a variety of ways. For instance, despite U.S. controls and sanctions on Iran and Russia drone manufacturers, a Ukrainian assessment of an Iranian Shahed-136 shot down in Ukraine found that 40 of the 52 components in the Shahed were made by U.S. manufacturers.[129] A separate investigation revealed similar findings.[130]

Increasing Amounts of Data

A major challenge for both AI and UAS export controls is the increasing amount of data, which can be difficult to track and manage. This challenge was frequently cited during our discussions as one of the biggest challenges that export control enforcement faces. This is exacerbated by the fact that the distinction between civilian and potential military use for some technologies (especially UASs) can be muddled, expanding the pool of data that must be monitored. This makes it difficult to ensure that technologies are not misused to compromise national security, and it means that staffing levels and having technology to reduce manpower needed are crucial. Staffing and access to modern technology to more efficiently process data are needed to address the surge of data.[131] In addition, increased access to expertise in the form of advisory panels and communication with the private sector is needed. Although BIS does have advisory committees and communicates with the private sector quite regularly, there is notably no centralized standing body able to provide the government with expertise. There have been calls from the private sector for increased engagement, both to protect its commercial interest and to better advise the government on how export controls can be better designed and rolled out to protect the government's interests. There is no rule set on the balance of interaction with industry. Companies might not like what BIS is doing, but they are nonetheless looking to engage.

---

the U.S. Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Emerging Threats and Spending Oversight, September 19, 2023c.

[126] Gregory Allen, director, Wadhwani Center for AI and Advanced Technologies, CSIS, "China's Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes," statement before the U.S.–China Economic and Security Review Commission, April 13, 2023a.

[127] DOC, "President Biden's Fiscal Year 2025 Budget Would Strengthen Commerce Department's Mission to Boost American Innovation and Competitiveness," press release, March 11, 2024; stakeholder, interview with the authors, September 2024.

[128] Stakeholder, interview with the authors, September 2024.

[129] Natasha Bertrand, "CNN Exclusive: A Single Iranian Attack Drone Found to Contain Parts from More Than a Dozen US Companies," CNN, January 4, 2023.

[130] Bertrand, 2023.

[131] Stakeholder, interview with the authors, July 2024.

Some companies are not used to this type of regulation. Some give good data but are also trying to lobby Capitol Hill.[132]

Interagency Cooperation

Interagency cooperation is an issue at multiple levels. DoD, DOC, and DOS cooperate on a regular basis in the creation and implementation of export controls and in various parts of enforcement. However, escalation of a license application because of an interagency dispute is one of the main causes of delay in reviewing and processing licensing applications for AI-related technologies.[133] Although the agencies share national security as their primary goal in the execution of export controls, they still differ in goals and priorities. In our discussions, it was suggested that DoD is losing part of its role as an adviser in the creation of export controls for AI. Although DoD is still involved in that process, a shift in the way export controls are implemented has given increased power to BIS shape de facto law during implementation.[134] For example, advisory opinion letters from BIS will be critical to the implementation and effectiveness of the December 2024 export controls. These letters are typically not public and are not subject to the interagency process. Although these opinions are meant to clarify existing policy, they can make policy de facto. For example, giving an opinion on whether a fabricator engages in advanced-node production or whether a particular entity is a diversion risk has a substantial effect on implementation and enforcement consequences. It is reported that advisory opinions played an important role in the expansion of legal allowances of SME exports to China. The December 2024 export controls went through the interagency process, but BIS typically creates advisory opinions unilaterally, which means that BIS can significantly affect the actual approach taken in implementation and enforcement, including the determination of license exemptions. Furthermore, government sources have indicated that DOC is more receptive to concerns of exporters than of other agencies' concerns, including those focused on national security and economic security.[135] Some of our interviews also suggested that agencies besides DOC lack positions that focus as heavily or at the same level on export controls as DOC does.[136] The issues previously mentioned are likely to contribute to resolving interagency disputes during the licensing process as well. It is worth noting that much of the interagency regulatory process for export controls either is informal and not codified or is loosely codified.[137]

Furthermore, interagency cooperation is one potential partial solution to the data problem faced by all parties. Agencies often develop their own tools and datasets, particularly because assessment and regulation of specific technologies can be siloed, both within agencies and on an interagency level. There are some examples of agencies sharing tools and access to expertise. For example, at the time of our interviews, BIS was leveraging a tool set with the Defense Technology Security Administration

[132] Stakeholder, interview with the authors, September 2024.

[133] Stakeholder, interview with the authors, July 2024.

[134] Stakeholder, interview with the authors, September 2024; Allen, 2024b.

[135] Allen, 2024b; stakeholders, interviews with the authors, July through November 2024.

[136] Stakeholder, interview with the authors, September 2024.

[137] Stakeholder, interview with the authors, September 2024.

(DTSDA), the National Security Agency, and the Bureau of International Security and Nonproliferation to address threats, including collaboration on proposed changes to multilateral export controls, amendments to the EAR, and the review of licensing applications to identify end users of concern.[138] Increasing cooperation and sharing of tools and datasets can make assessment more accurate and prevent duplication of efforts.

Multilateral Considerations

Multilateral considerations have been one of the most-difficult challenges to the U.S. AI export controls. Without multilateral support from other countries with firms in the supply chain, U.S. export controls on AI can prove not only ineffective but also disastrous by weakening U.S. companies and enabling China to potentially create new AI ecosystems that exclude the United States. Successful use of the FDP rule depends on countries' belief that the United States can enforce the rule and that they will be forced to bear the consequences. The PRC's retaliatory use of export controls and rare earth mineral bans provide pressure for countries to forgo joining the U.S. export regime as well.[139] Although the October 2022 export controls put in place were likely not a surprise to other countries, they were put in place unilaterally.[140] The unilateral nature of the October 2022 controls opened the door to such countries as Japan and the Netherlands to fill the gap the United States left in the market, and they took advantage of that gap even as the United States developed its export control regime.[141] The United States did secure a deal with the Netherlands and Japan to join the export regime, although it is suggested that this was an "understanding" as opposed to a formal deal. In retaliation, China implemented restrictions on the export of key raw materials used for the manufacturing of semiconductors.[142] The effect of Chinese pressure might be reflected in the PRC's ability to developed low-yield, low-volume production of 7-nm chips, which suggests circumvention of the export controls somewhere along the multilateral side of export controls. Still, the fact that production has remained in low-yield and low-volume levels means that multilateral efforts have been effective on some level.[143] Additionally, the United States has significantly increased its efforts at securing multilateral cooperation with the ambitious 2025 framework, pushing for cooperation from a much broader group of countries and aiming to engage further with allied countries to communicate about the balance of long-term security risks and immediate economic concerns, similar to how the United States targeted Huawei. The United States could aim to create coalitions outside of the WA member states, improve global customs coordination efforts and end-user verification capabilities, and develop a list of advanced technologies that is coherent across countries, particularly in granularity of

[138] Kendler, 2023. The Bureau of International Security and Nonproliferation was renamed *Bureau of Arms Control and Nonproliferation* in late spring 2025, several months after our project ended.

[139] Allen and Benson, 2023; David Pierson, "China Bans Rare Mineral Exports to the U.S.," *New York Times*, December 3, 2024.

[140] Alan F. Estevez, "A Conversation with Under Secretary of Commerce Alan F. Estevez," Center for a New American Security, October 27, 2022; Shivakumar, Wessner, and Tomoshige, 2023.

[141] Shivakumar, Wessner, and Tomoshige, 2023; Lili Yan Ing, "ASEAN's Role in the Global Semiconductor Race," ThinkChina, October 2, 2023.

[142] Ing, 2023.

[143] Allen and Benson, 2023.

restrictions.[144] The U.S.–EU Trade and Technology Council published "TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management" in December 2022; as of 2024, progress had been made, including the creation of three expert groups and the establishment of a shared AI vocabulary to facilitate cooperation in AI regulation.[145]

The WA is seen as outdated and ineffective for controlling advanced technology exports. This is particularly true for modern challenges from Russia. Russia is not likely to form a new consensus with Western countries to revise the list of controlled items. Additionally, Western countries cooperatively implemented semiconductor chip sanctions on Russia outside the WA following Russia's invasion of Ukraine, and initial enforcement cooperation was somewhat successful.[146]

Although the United States' interpretation of the MTCR and its subsequent export control policies kept armed drones out of adversaries' hands, it also prevented or limited the transfer of such systems to partners and allies. As of 2017, the United States had approved of the sale of armed drones to only the UK and Italy. It took DOS four years to approve the sale of armed Reaper drones to Italy.[147]

Mismatch Between Policy and Technology Timelines

Policy and regulation do not keep up with changes and dissemination of technologies, and export controls are playing a game of catch-up. Whether keeping pace with new technologies or keeping regulatory language consistent with changes in current technologies, stakeholders engage in a constant struggle to keep pace with AI and UAS technologies. The ability to catch up is hampered by a lack of flexibility in regulations. Regulations that could adapt to technological developments rather than requiring a new set of regulations would be ideal. This would require not only ongoing legislative adjustments but also continuous dialogue with industry to better understand the latest technological developments and their potential implications. Forums for such communication with industry exist, but not in the amount and speed that would be necessary to formulate more-adaptive, agile regulations.[148] One area in which timelines have been brought up as a major weakness is with the speed at which Chinese entities are added to the Entity List. BIS's inability to add Chinese company Cambricon Technologies in time for the implementation of the October 2022 policy was a critical signal early on.[149]

[144] Shivakumar, Wessner, and Tomoshige, 2023; BIS, 2025b.

[145] Emily Benson, "The Fifth Ministerial of the U.S.–EU Trade and Technology Council," *Critical Questions*, CSIS, February 7, 2024; U.S.–EU Trade and Technology Council, "TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management," December 1, 2022.

[146] Shivakumar, Wessner, and Tomoshige, 2023.

[147] Federico Borsari and Gordon B. "Skip" Davis, Jr., *An Urgent Matter of Drones*, Center for European Policy Analysis, September 27, 2023. This was the tipping point. Until then, the United States had made almost no sales. Then, in 2018, China made sales to a large number of countries, which made the United States want to shift its policy.

[148] Stakeholder, interview with the authors, November 2024.

[149] Allen, 2022.

Chapter 4

Effects on Private-Sector Development: Could Export Controls Have a Chilling or Warming Effect?

Export controls enforce rigorous restrictions on accessing and exporting sensitive technologies—notably, those with potential military applications—which profoundly influences the development of AI and UASs. These restrictions catalyze a state of *permacrisis*, a term that reflects continuous global instability and the complex challenges it poses.[150] In this environment, organizations are compelled to innovate through the development of alternative technologies that circumvent export controls or through modifications of existing technologies to comply while maintaining functionality. Additionally, to navigate the restrictive landscape, companies might relocate production facilities to jurisdictions with more-lenient regulations or reconfigure their supply chains to source essential components from markets free from such constraints. This strategy of adaptation and circumvention not only fosters significant local innovation in *other* countries but also highlights the necessity for policymakers to balance stringent security measures with the imperative for technological and economic advancement. Such a nuanced approach is crucial to ensuring that regulations are sufficiently flexible to accommodate rapid technological progress and the intricate web of global market interactions. The Ukrainian exemplar emphasizes the dual impact of export controls: Although they restrict international collaboration by erecting barriers, they also spur competitive innovation within localized contexts. Firms are often driven to intensify their research and development (R&D) efforts to surpass competitors in regions where international cooperation is limited, which can lead to a surge in innovation as companies strive to navigate and surmount these imposed barriers. This dynamic illustrates the critical need for policies that recognize the complexities of modern technological development and international cooperation, ensuring that innovation can flourish even amid ongoing global challenges.[151]

[150] Gordon Brown, Mohamed El-Erian, and Michael Spence, with Reid Lidow, *Permacrisis: A Plan to Fix a Fractured World*, Simon and Schuster, 2023.

[151] Jon Schmid, Jon, David Luckey, Erik E. Mueller, Clay Strickland, Thomas Goode, Hiwot Demelash, Will Shumate, Aleksandr Esparza Hartunian, Kyle Brady, Karlyn D. Stanley, and Paul Cormarie, *Fielding Artificial Intelligence During Conflict: Lessons from Ukraine's Deployment of Artificial Intelligence in the Russia–Ukraine War*, RR-A3453-1, forthcoming; Vera Bergengruen, "How Tech Giants Turned Ukraine into an AI War Lab," *Time*, February 8, 2024; Mykhailo Fedorov, "Ukraine's Vibrant Tech Ecosystem Is a Secret Weapon in the War with Russia," *UkraineAlert* blog, August 17, 2023; Gian Volpicelli, Veronika Melkozerova, and Laura Kayali, "'Our Oppenheimer Moment'—in Ukraine, the Robot Wars Have Already Begun," Politico, May 16, 2024.

The Economic Impact of Export Controls on Artificial Intelligence and Semiconductor Technologies

Export controls have profound implications on economic outcomes for businesses involved in the production of AI and semiconductor technologies. Restrictions on buying and selling products in specific markets or acquiring necessary components can significantly decrease sales and revenue, which can lead companies to assess the economic trade-offs and associated risks of these regulations for their competitive stance. For instance, U.S. policies limiting PRC access to critical AI chip technologies have directly affected some companies, such as Nvidia, which had previously dominated the market in China.[152] Such restrictions affect sales and compel companies to adjust their strategies in significant ways.[153] Despite significant challenges in processing speed, efficiency, and overall capabilities of AI chips comparable to those of market leaders Nvidia and Advanced Micro Devices (AMD)—both U.S. firms—Chinese semiconductor firms are aggressively advancing toward technological self-reliance. This shift, detailed in a 2024 CSIS report by Gregory C. Allen, is marked by strategic policy adaptations and robust state investments designed to reduce foreign dependence and enhance competitive capacities in the semiconductor sector.[154] Although these gaps hinder Chinese companies' ability to compete globally, they simultaneously reduce potential revenue for U.S. companies because of the stringent export controls that limit their market access in China. Conversely, export controls indirectly benefit Chinese firms in that these controls catalyze the growth of a domestic homegrown chip manufacturing ecosystem. The need to bridge these *performance gaps* drives Chinese companies to invest heavily in R&D, thereby cultivating innovation and gradually enhancing their technological capabilities, which could eventually lead to a more self-sufficient and competitive local industry.

Moreover, some companies, including Nvidia, have expressed that, although immediate financial impacts are mitigated by high global demand, long-term restrictions could result in substantial losses of market opportunities in China.[155] Similarly, a 2023 CSIS report highlighted how export controls from 2009 to 2012 resulted in an estimated loss of sales of approximately $988 million to $2 billion (equivalent to roughly $1.8 to $3.7 billion in 2025) for U.S. industries; these amounts provide a view into the chilling financial impacts these regulations have on industry.[156]

Thus, it is clear that export controls influence the semiconductor and AI industries by affecting a company's ability to access global markets and maintain competitive advantages in innovation in addition to manufacturing processes. There are layers to the challenges faced by industries in which field-programmable gate arrays (FPGAs) are critical components of technological platforms. For example, in 2022, the FPGA market was valued at approximately $10.46 billion, with expectations of

[152] Rajeswari Pillai Rajagopalan, "AI Chips for China Face Additional US Restrictions," *The Diplomat*, April 5, 2024.

[153] Semiconductor Watch, "Navigating the Impact of U.S. Export Restrictions on Nvidia: The Middle East Factor," press release, August 31, 2023.

[154] Gregory C. Allen, "The True Impact of Allied Export Controls on the U.S. and Chinese Semiconductor Manufacturing Equipment Industries," CSIS, November 26, 2024a.

[155] Dou, 2023; Asa Fitch, Yuka Hayashi, and John D. McKinnon, "U.S. Considers New Curbs on AI Chip Exports to China," *Wall Street Journal*, June 27, 2023.

[156] William A. Reinsch, Emily Benson, Thibault Denamiel, and Margot Putnam, *Optimizing Export Controls for Critical and Emerging Technologies*, CSIS, May 2023, p. 16.

a compound annual growth rate of 10.8 percent from 2023 to 2030.[157] The Asia-Pacific region, led by China, held the highest revenue share, largely because of China's continuous investments in military and aerospace applications. North American companies, such as Intel, Qualcomm, and Nvidia, although they are major players in FPGA design, rely heavily on manufacturing in Taiwan, which presents significant security and supply chain vulnerabilities.[158] Furthermore, because this offshore production is driven by cost, the loss of revenue and increasing competitiveness that U.S. firms face in the wake of export controls make it even more difficult to incentivize the creation of a domestic production base.[159]

The implementation of stringent U.S. export controls in 2022 led to significant market shifts. Some companies, such as ASML, Keep Looking Ahead (KLA), Lam Research, and Applied Materials, saw declines in market share and have had to adjust their financial forecasts significantly. For instance, Applied Materials reduced its first-quarter sales forecast for 2023 by $400 million because of these new regulations,[160] which emphasizes the direct impact on revenue and the potential long-term effects on R&D efforts necessary for technological leadership.[161]

Impact on Company Revenue

Export controls significantly shape company review streams by limiting access to global markets and critical components, which affects their overall business operations and strategic positioning. A 2022 CSIS report highlights that the September 2022 announcement of export controls resulted in unintended benefits for Chinese companies at the expense of U.S. firms, such as Nvidia and AMD, primarily because the restrictions enabled "the growth of [Chinese companies] by strengthening the Chinese ecosystem for domestic chip development," essentially forcing a reconfiguration of supply chains and customer bases that might initially hinder but then eventually benefit Chinese firms in the long term.[162]

Despite the extensive global demand for Nvidia and AMD advanced semiconductors and AI chips, the newly imposed export controls were not expected to significantly affect their financial results in the near term. Nvidia financial resilience is due to strong sales in other international markets that compensate for the restrictions in specific regions, such as China. However, Nvidia expressed concerns about the potential long-term impacts of these controls. If the restrictions persist, they could eventually hinder Nvidia's ability to fully exploit global market opportunities, which could lead to significant adverse effects on its business and financial outcomes in the future.[163] Nvidia's response to export controls reflects a complex balance between compliance and market strategy. Although global demand can act as a buffer against negative impacts, Nvidia's chief financial officer, Colette Kress, expressed concerns about long-term restrictions in China, which she said would "result in a permanent

[157] Reinsch et al., 2023.

[158] Reinsch et al., 2023.

[159] Reinsch et al., 2023.

[160] Shivakumar, Wessner, and Tomoshige, 2023.

[161] Shivakumar, Wessner, and Tomoshige, 2023.

[162] Allen, 2022.

[163] Dou, 2023.

loss of opportunities for the U.S. industry to compete," which could lead to substantial revenue losses over time.[164] Kress's statement captures the critical trade-off between adhering to national security measures and sustaining business growth in competitive international markets.

Moreover, industry responses to export controls suggest a pervasive concern about the potential for these regulations to stifle innovation and economic development. Overly stringent restrictions could compel companies to transfer their research facilities to jurisdictions without such restrictions, which could reduce the United States' technological and economic superiority.[165] Potential relocations of research facilities and other business components could lead to a significant decrease in domestic revenue because companies might shift operations abroad to maintain competitive advantage and access to global markets. Further corroborating this sentiment, Ian King and Jenny Leonard reported that some companies, such as Applied Materials, Lam Research, and KLA, expressed concerns about the new export controls cutting into their revenue, indicating a significant risk to their market share (which could be absorbed by competitors) in China and their ability to compete globally.[166]

Impact on Market Share Dynamics

Export controls significantly influence global competitive dynamics, affecting the international market positioning of firms and nations within the technology sector. Export control regulatory measures are pivotal in shaping market shares, which reflects the measures' direct impacts on corporate strategies and national economic policies. By determining which technologies firms can access and sell, export controls serve as barometers of current market conditions and forecasters of future trends—readings that are crucial for long-term strategic business planning.

The significant effects that export controls have on market share are exemplified by the experience of U.S. semiconductor companies. Following the announcement of stringent controls, some firms, such as Lam Research, anticipated losses up to $2.5 billion, which highlights the immediate financial impact and broader implications for U.S. industries. The Chinese government's push for domestic sourcing further exacerbates this challenge: U.S. companies faced the threat of being designed out of critical supply chains. This scenario is complicated by the proactive measures of U.S. executives, such as those from Intel and Nvidia, who have argued against these restrictions to preserve their access to one of their largest markets: China.[167]

Moreover, the global landscape of semiconductor manufacturing illustrates a strategic shift as companies in Japan, Korea, and Europe consider replacing U.S. technology with alternatives to penetrate the Chinese market. This shift could precipitate significant market share losses for U.S.

[164] Yuka Hayashi and Asa Fitch, "U.S. Tightens Curbs on AI Chip Exports to China, Widening Rift with Nvidia and Intel," *Wall Street Journal*, October 17, 2023.

[165] Ana Swanson, "Trump Officials Battle over Plan to Keep Technology Out of Chinese Hands," *New York Times*, October 23, 2019.

[166] Ian King and Jenny Leonard, "US Chip-Gear Makers Told to Wait for Relief from China Curbs," Bloomberg, November 3, 2022.

[167] Reinsch et al., 2023.

firms, a concern substantiated by the reduced revenue forecasts from some companies, such as Applied Materials.[168]

These dynamics underscore a broader trend, whereby Chinese policies and market strategies are rapidly diminishing U.S. firms' market shares, compelling the U.S. companies to innovate within constrained environments. China's aggressive investment strategies in semiconductor technology not only challenge U.S. market dominance but also suggest a strategic decoupling that could reshape global high-tech industries. This is evidenced by substantial Chinese investments in next-generation technologies and the supportive measures provided by state policies, which are intended to bolster domestic capabilities and reduce reliance on foreign technology.[169]

Against the backdrop of stringent export controls, China is fortifying its domestic semiconductor industry, reducing its reliance on U.S. technology, thereby reshaping global market shares. This strategic shift not only diminishes the market presence of U.S. firms but also affects their revenue streams crucial for further technological advancements. Over time, such measures could erode U.S. entities' competitive edge in this critical sector.[170]

As a result, export restrictions have prompted U.S. allies in the Middle East and Africa to seek alternatives for military drones, which has led to a decline in the U.S. market share as Chinese manufacturers fill the void. This transition, catalyzed by U.S. policies, reveals the export controls' significant impact on the global positioning of U.S. firms in the drone industry. The reliance in Chinese drones illustrates a shift in global market dynamics, which might have resulted from U.S. export policies. The United States saw a reduction in its share of the global drone market as allies in the Middle East and Africa have turned to Chinese manufacturers because of restrictive U.S. export policies. This trend has been highlighted by Jeremy Page and Paul Sonne, who noted that the United States was relinquishing its market dominance in military drones as allies sought alternatives that were not constrained by U.S. regulations.[171] This shift showcases how U.S. restrictions are reshaping the competitive landscape in the drone industry, driving strategic realignments within global markets.[172] Additionally, this shift to reliance on Chinese drones has further security effects, which we discuss in the next chapter.

The implementation of new export controls in 2023 has markedly affected U.S. semiconductor companies, notably causing Nvidia's stock to tumble by nearly 5 percent. This decline signals the immediate financial repercussions and raises concerns about the long-term viability of U.S. semiconductor enterprises operating under increasingly restrictive trade conditions.[173] In response to stringent export controls, China has adopted a comprehensive national strategy, the *juguo tizhi* or whole-of-the-nation approach, to bolster its self-sufficiency in critical sectors, such as semiconductors and quantum computing. This strategic infusion of resources is intended to diminish the reliance on U.S. technology and fortify domestic capabilities, thereby shifting the balance of power in high-tech

[168] Shivakumar, Wessner, and Tomoshige, 2023.

[169] Shivakumar, Wessner, and Howell, 2024.

[170] Shivakumar, Wessner, and Howell, 2024.

[171] Jeremy Page and Paul Sonne, "China Seizes Market for Military Drones: U.S. Allies in Mideast and Africa That Can't Buy American Turn to Beijing," *Wall Street Journal*, July 18, 2017.

[172] Page and Sonne, 2017, p. 279.

[173] Hayashi and Fitch, 2023.

industries globally.[174] Tencent Holdings has proactively amassed a significant stockpile of Nvidia's AI chips, safeguarding its future AI development projects against U.S. export controls. This strategic accumulation underscores the resilience and foresight of Chinese firms in securing their technological futures despite international trade pressures. Tencent's ability to maintain its developmental trajectory underlines the adaptability required in today's geopolitically charged economic landscape.[175]

Strategic and Policy Responses

As nations and businesses navigate the intricate world of export controls, they continually adapt and refine their strategies to mitigate these regulations' effects on their operations. The landscape of international trade is marked by a complex interplay of policy responses and strategic realignments. For instance, when a country imposes strict export controls, it not only affects the immediate supply chain but also sets in motion a series of strategic countermeasures by affected nations and industries. Companies might relocate their manufacturing bases or alter their supply routes to bypass restrictions, which just showcases their agility in the face of regulatory challenges.

Moreover, governments might respond with policies that either tighten their own export controls in retaliation or engage in diplomatic negotiations to ease the restrictions. This dynamic creates a feedback loop in which policy adjustments lead to further strategic shifts within industries, prompting a continual reassessment of both business strategies and national policies. The result is a perpetual state of adaptation, in which businesses and governments strive to maintain economic stability and competitive advantage in a global market that is constantly being reshaped by new regulatory measures.

Retaliatory Export Regimes

When nations implement export controls, reciprocal actions often follow, which leads to cycles of retaliatory export regimes. Such dynamics escalate trade barriers, thereby complicating international trade relationships. For example, U.S. restrictions on high-tech exports to China have prompted countermeasures, disrupting global supply chains in semiconductors and other key industries. The World Trade Organization's analysis of trade measures highlights how these policies influence global trade patterns, with secondary or ripple effects across multiple sectors.[176] Ralph Ossa's economic modeling further illustrates how retaliatory trade policies reshape market access, compelling businesses to reconfigure operations to mitigate losses.[177] Understanding these measures is vital for anticipating shifts in trade relationships and crafting policies that enhance resilience amid geopolitical tensions.

---

[174] Keyu Jin, "How China Is Fighting the Chip War with America," *New York Times*, October 27, 2022.

[175] Vlad Savov and Debby Wu, "Tencent Stockpiled Nvidia AI Chips for 'a Couple of Generations,'" Bloomberg, November 15, 2023.

[176] World Trade Organization, "World Trade Report 2024: Trade and Inclusiveness—How to Make Trade Work for All," webpage, 2024.

[177] Ralph Ossa, "Trade Wars and Trade Talks with Data," *American Economic Review*, Vol. 104, No. 12, December 2014.

Benefits of Targeting Across the Supply Chain

Strategically implementing export controls targeting specific, interconnected points in the supply chain offers the potential to safeguard national security while preserving economic vitality and fostering innovation. For example, the 2022 semiconductor export controls targeted advanced chips, chip design software, and both access to and the ability to develop SME. This allowed the export controls to more effectively prevent PRC access to and development of chips and to minimize unintended consequences. An example of an unintended consequence is that, if the export controls had targeted solely advanced chips, China's access to other countries' SME would have created an intense demand for China or another country to develop its own chip design software, which would have endangered Nvidia's monopoly in chip design software and ultimately advanced chips.[178] By identifying and targeting critical nodes, policymakers can design measures that mitigate risks associated with the transfer of sensitive technologies without overly burdening industries that rely on global supply chains. Such an approach requires careful planning to minimize unintended consequences, such as disruptions to domestic production or retaliation from affected trade partners. Effective export control strategies balance the dual goals of protecting national interests and maintaining industry competitiveness, ensuring the resilience of domestic supply chains and the broader economy. Through strategic intervention, governments can maintain security while supporting innovation in rapidly advancing technological sectors.

Targeting specific points along the supply chain through export controls can disrupt global trade relationships and destabilize existing supply chain networks. The 2024 U.S. restrictions on AI chip exports to China illustrate how targeted measures create tensions and provoke retaliatory actions. For instance, in response to U.S. policies, the Chinese Communist Party banned sales of chips produced by U.S.-based Micron Technology and restricted the export of essential materials for semiconductor manufacturing.[179] More recently, China escalated the U.S.–China supply chain war by instituting a ban on rare-mineral exports to the United States.[180] China's responses to U.S. restrictions highlight the dual-edged nature of supply chain–targeted controls: Although they might bolster national security, they can simultaneously weaken global supply chain reliability and hurt domestic industries by triggering countermeasures.[181]

Export controls on AI technologies present complex challenges that extend beyond national borders, affecting innovation and competitiveness in unexpected ways. Concerns about restrictive measures emphasize the risk of unintended consequences, such as fostering accelerated technological development in other nations. According to Cade Metz, technology experts have argued that controls aimed at limiting AI exports could inadvertently enable other countries, particularly China, to strengthen their AI capabilities by bypassing U.S. collaboration and driving localized innovation. This dynamic raises questions about the global competitiveness of U.S. companies under increasingly stringent regulations.[182]

---

[178] Shivakumar, Wessner, and Howell, 2022; Allen, 2022.

[179] Hayashi and Fitch, 2023.

[180] Pierson, 2024.

[181] Hayashi and Fitch, 2023.

[182] Cade Metz, "Curbs on A.I. Exports? Silicon Valley Fears Losing Its Edge," *New York Times*, January 1, 2019.

The collaborative nature of AI development complicates the effectiveness of export controls. AI research relies on global networks of scientists and engineers, with breakthroughs often representing the collective efforts of multiple institutions. As Jack Clark, then policy director at OpenAI, observed, "The number of cases where exports can be sufficiently controlled are very small,"[183] which highlights the risks of error and potential harm to the broader AI community. These interconnected research efforts make it difficult to designate proprietary AI developments as strictly national products, which creates challenges for implementing effective and targeted controls without stifling innovation.[184]

Strategically, this underscores the need to balance national security priorities with the realities of global research ecosystems. Overregulation risks not only dampening domestic competitiveness but also accelerating advancements abroad. Policymakers must therefore navigate these dynamics carefully, ensuring that measures are precise, flexible, and supportive of innovation while maintaining necessary safeguards. This delicate balancing act is central to preserving U.S. leadership in AI and fostering a collaborative yet secure global technology landscape.

Security Externalities Resulting from Financial Impact

As shown in preceding sections, export controls can have broad and substantial implications. They are critical tools for balancing national security concerns with economic impacts, but their implementation introduces complex security and economic externalities. These controls can influence global trade relationships, reshape supply chains, and affect long-term R&D investments, all of which have significant implications for national security and technological leadership.

Export controls often lead to reduced revenues for firms that depend on global market access, which can, in turn, hinder investments in R&D and innovation. The imposition of the 2022 U.S. semiconductor export controls disrupted the ecosystem supporting chip research and production, causing firms to face unpredictable policy environments that affected their long-term strategic planning.[185] The challenge of balancing security needs with economic considerations is critical for nations and companies engaged in high-tech industries. Export controls are intended to prevent adversaries from acquiring sensitive technologies, but the associated economic impacts, such as reduced market access and financial strain on domestic firms, complicate this balancing act. Strategic approaches are essential to ensure that national security objectives do not come at the expense of economic competitiveness or innovation capacity.

[183] Metz, 2019.

[184] Metz, 2019.

[185] Shivakumar, Wessner, and Howell, 2022.

Chapter 5

Effects on U.S. National Security

In this chapter, we examine export controls' potential effects on U.S. national security. This includes the effects of either tightening or loosening such controls for a variety of national security factors.

Threats from Uncrewed Aircraft Systems

The intended goal of export controls is to limit the ability of adversaries and others to use UASs contrarily to U.S. interests. This goal is motivated by the current and anticipated threats from the advancing capabilities for UASs.

Uncrewed Aircraft System Capabilities and Threats

UASs are emerging as capable threats, both on the battlefield and domestically. As UAS technology continues to develop (e.g., battery size and capacity, electric motors, and sensor payloads), so do their capabilities in range, payload, and power, which magnifies their potential for misuse.[186] UASs provide maneuverable, cheap, and asymmetric airpower; they can deliver explosives (precision and nonprecision) and other payloads, conduct discreet surveillance, provide a platform for electronic and cyber warfare, and transport small items for last-mile logistics.

These capabilities are being demonstrated on the battlefield. In Ukraine and in the Middle East, use of UASs has become commonplace on every side of conflict for a wide variety of tasks. Furthermore, the use of small UASs (sUASs) has begun to displace larger UASs,[187] such as the MQ-9 Reaper, which was used extensively on the battlefield in the early years of the 21st century. Their low cost and ease of access make them a preferred choice over more-expensive UASs, the purchase of which has been typically limited to well-funded state militaries.[188]

UASs have provided Ukrainian forces an asymmetric capability that has disrupted Russian forces and logistics. Early in the war, the Turkish-made Bayraktar TB2 proved effective at helping halt Russia's advance into Ukraine. After Russian air defenses started countering these, Ukraine opted for

[186] Bradley Wilson, Shane Tierney, Brendan Toland, Rachel M. Burns, Colby Peyton Steiner, Christopher Scott Adams, Michael Nixon, Raza Khan, Michelle D. Ziegler, Jan Osburg, and Ike Chang, *Small Unmanned Aerial System Adversary Capabilities*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-3023-DHS, 2020.

[187] A UAS is an sUAS if it weighs less than 55 lb or corresponds to North Atlantic Treaty Organization (NATO) UAS Class I or II. For more on NATO UAS classes, see Yuksel Kutuk, *UAS (Unmanned Aircraft Systems): The Force Multiplier for Law Enforcement Agencies and the Potential Contributor to Stability Policing*, Stability Policing Centre of Excellence, NATO, 2025, p. 16.

[188] Brandi Vincent, "'Stark Reminders': Experts Assess How Military Tech Must Adapt After Deadly Drone Attack on US Troops," DefenseScoop, February 2, 2024.

larger numbers of smaller, lower-flying UASs. These can be used for kamikaze missions, in which the UAS is lost in the attack, or for missions that allow the UAS to return to base for reuse. Small quadcopter UASs can be used to loiter above Russian forces and drop explosives no bigger than a grenade onto entrenched infantry or through an open hatch of an armed vehicle.[189] Larger and longer-range Ukrainian UASs have destroyed almost 15 percent of Russia's crude oil refining ability through repeated kamikaze attacks. These UASs were originally commercial off-the-shelf (COTS) platforms, such as the Da-Jiang Innovations (DJI) Mavic 3 (a miniature autonomous vehicle with an intelligent controller), but the operational successes of these platforms have buoyed a domestic industry of custom-built Ukrainian UASs.[190]

Ukraine has also found success using UASs in support roles, such as for Ukrainian soldiers who have been using large attack drones to deliver not only ammunition but also essential supplies, such as medicine, power banks, antenna parts, and even fire extinguishers. To improve efficiency, soldiers have attached glow sticks to packages, making them easier to locate in the dark. Additionally, Ukraine has been using DJI Mavic drones for intelligence, surveillance, and reconnaissance to enhance its operational capabilities on the ground.[191] Ukraine's military and other government entities have also used commercial technology in UASs as nodes in communication relay chains and for spotting in support of artillery fire.[192]

The United States' competitors and adversaries have increased their use of UASs for military purposes beyond the war in Ukraine. Iran has boosted its domestic development and production of UASs and has begun supplying hundreds of loitering kamikaze drones to Russia to be used in Ukraine.[193] Reports suggest that China has begun using long-range UASs for covert surveillance in the South China Sea and that North Korea has used UASs to incur into ROK airspace and harass ROK operations.[194] Chinese-made UASs have also appeared in smaller conflicts in a variety of battlefield roles across the Middle East and Africa, including by some U.S. allies.[195] In Syria, U.S. air defenders have reported an increasing volume of hostile surveillance UASs in the airspace, including both COTS and Iranian-made platforms.[196]

---

[189] Philip E. Ross, "Budget Drones in Ukraine Are Redefining Warfare: Smart, Low-Cost Tech Enables New Military Tactics," *IEEE Spectrum*, May 17, 2023. *Loiter* in this context refers to a drone's technical capability to stay in one area and attack when a target presents itself.

[190] Vasco Cotovio, Clare Sebastian, and Allegra Goodwin, "Ukraine's AI-Enabled Drones Are Trying to Disrupt Russia's Energy Industry. So Far, It's Working," CNN, April 2, 2024.

[191] Ian Lovett and Nikita Nikolaienko, "Inside a Ukrainian Vampire Drone Squad's Mission to the Front Lines," *Wall Street Journal*, May 10, 2024.

[192] Emelia Probasco, "The Future of Drones in Ukraine: A Report from the DIU-Brave1 Warsaw Conference," Center for Security and Emerging Technology, November 13, 2023.

[193] Barbara Starr and Katie Bo Lillis, "US Trying to Speed Up Delivery of Key Air Defense Systems to Ukraine After Russia's Iranian-Supplied Drone Attacks," CNN, October 17, 2022.

[194] Sonenshine, 2023.

[195] Page and Sonne, 2017.

[196] Clifford Lucas, "The Drone Dilemma and the US Air Force," War on the Rocks, May 7, 2024.

Autonomous Uncrewed Aircraft System Capabilities and Threats

In the hands of a trained pilot, UASs have proven quite capable, but, when enhanced with autonomous technologies, UAS capabilities on the battlefield increase in both kind and degree. Autonomy allows UASs to conduct a variety of tasks with less or no human interaction, such as perceiving the physical world via sensors and machine vision, analysis and sense-making via data fusion of sensor feeds and mission data, decisionmaking via prioritization algorithms, and execution via automatically adjusting movement capabilities or payload.[197] UASs can have greater autonomy for any one or more of these kinds of tasks. This autonomy can also be used for increasingly consequential decisions and actions, such as obstacle avoidance during human-controlled flight or full mission planning and execution based on human-provided goals.

UASs with assisted remote-control capabilities are ubiquitous and widely available to state actors, nonstate actors, and the public. Nearly all commercial vertical-lift UASs provide automated flight stabilization and can hover or descend without human intervention. Most have in-built Global Positioning System (GPS) capabilities that allow a UAS to follow a preprogrammed flight pattern, and these GPS positions can be tied to other actions, such as descending or delivering a payload.[198] These capabilities are sufficiently accessible that, in 2020, the Azerbaijan Air Force used them to send pilotless 80-year-old crop duster aircraft on preprogrammed routes as bait for Armenian air defenses.[199] The United States used the same concept of operations (CONOPS) to great effect to decoy Iraqi defenders in the opening of the 1991 Operation Desert Storm campaign.

Autonomous Uncrewed Aircraft Systems in Ukraine

Semiautonomous UASs are becoming similarly ubiquitous. Ukraine, for instance, has begun using machine vision in its drones to conduct operations with minimal human control, like the technology of U.S. systems, such as that in the Harpoon. Ukrainian manufacturer Saker has taken algorithms originally intended to assist in sorting and classifying fruit and put them into mass-produced single–circuit board computers attached to small kamikaze UASs so the machines can autolock onto a human-defined target. The UAS then flies on its own to the target, even if the target moves.[200] This machine-vision technology has allowed Ukraine to carry out strikes on distant Russian refineries without needing a human operator proximate to the target.[201] Machine vision can also allow UASs to fly long distances without even GPS to guide them, flying based on dead reckoning of ground conditions.[202] This terrain contour–matching navigation technology was first deployed in the MGM-1 Matador in 1952. Semiautonomy also serves as a force multiplier: Instead of one pilot operating one UAS, one pilot can operate several simultaneously, intervening to direct the platforms in key moments

[197] National Institute of Standards and Technology, *Autonomy Levels for Unmanned Systems (ALFUS) Framework*: Vol. II, *Framework Models*, Version 1.0, Special Publication 1011-II-1.0, December 2007.

[198] Benjamin Fogel and Andro Mathewson, "The Next Frontier in Drone Warfare? A Soviet-Era Crop Duster," *Bulletin of the Atomic Scientists*, February 10, 2021.

[199] Fogel and Mathewson, 2021.

[200] Paul Mozur and Adam Satariano, "A.I. Begins Ushering in an Age of Killer Robots," *New York Times*, July 2, 2024.

[201] Cotovio, Sebastian, and Goodwin, 2024.

[202] Jon Harper, "Drone Swarms with 1,000 Unmanned Aircraft Could Be Possible Within 5 Years, DARPA Leader Says," DefenseScoop, April 5, 2022.

during the operation. Ukrainian pilots, for instance, have claimed that they can manage up to seven UASs at once with these capabilities.[203] The need for a human overseer actively identifying and picking targets for these UASs might also be fading. Ukrainian forces, for instance, are experimenting with a system of systems, in which one reconnaissance UAS uses AI to identify individual targets and then dispatches one or more autonomous kamikaze UASs to kill the target. Human involvement would be a level above, defining acceptable targets and developing the patterns of behavior for these UASs.

Fully autonomous UASs—that is, UASs for which humans set the mission and scope and let one or more UASs meet the mission on their own terms and at their own direction, such as the current U.S. Harpoon or high-speed antiradiation missile (HARM)—have a long track record of military success.

Although the basic CONOPSs of sUASs in the Ukraine war often resemble CONOPSs that the United States and other nations have employed for decades, the advent of small, light, and cheap computer guidance means that the missions can be performed by systems much smaller and cheaper than those employed in the past.

Uncrewed Aircraft System Swarms

The development of fully autonomous UASs also opens the potential for another level of the UAS threat: swarms. A UAS swarm "consists of multiple UASs flying in a coordinated manner, which is either controlled remotely or self-controlled based on algorithms and programming that has been built into the system."[204] Coordination between platforms is what separates swarms from simply a large number of UASs. It allows the collective group of UASs to react as a whole to threats or changes in the environment or the mission. It also allows for division of labor across UASs and prioritization of actions among the different platforms of the swarm. In a 2024 report, RAND researchers defined three levels of swarming capability, based on the amount of coordination and autonomy of the swarm:

- level 1: multioperator-coordinated groups of individual drones (that is, multiple operators controlling multiple groups of drones operating simultaneously)
- level 2: drones that have been programmed in a coordinated manner to fly individually, in a leader–follower configuration, or in multidrone formations with a human operator controlling multiple drones
- level 3: intelligent drone swarms in which individual drones can communicate with each other and respond to external stimuli.[205]

Level 3 swarm capability presents a new capability and threat. The collective sensor feeds of the entire swarm are analyzed either by a central controller UAS (centralized) or across the distributed computing power of the swarm (decentralized). The centralized controller or the decentralized distributed mass then makes decisions based on prioritization algorithms then tasks individual UASs

[203] Mozur and Satariano, 2024.

[204] Daniel M. Gerstein and Erin N. Leidy, *Emerging Technology and Risk Analysis: Unmanned Aerial Systems Intelligent Swarm Technology*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-A2380-1, 2024.

[205] Gerstein and Leidy, 2024.

to complete objectives to serve the swarm's overall goal. The swarm as a whole acts in a synchronized fashion and reacts as its actions affect the environment. This recursive action and reaction across a network of UASs with minimal human intervention allows emergent behavior. The synchronicity, speed, and unpredictability of an intelligent swarm create far more capability than individual UAS operating independently can have.

Although such a threat has not yet fully manifested on a current battlefield at the time of this report, this capability is on the horizon. The Defense Advanced Research Projects Agency (DARPA) demonstrated a swarm of 150 UASs in 2022, and the project leader predicted that such swarms with 1,000 UASs might be possible by 2027.[206] In 2023, China similarly demonstrated a swarm of 48 loitering munitions UASs.[207] The level of autonomy and emergent behavior these demonstrated swarms possessed is unclear.

Swarms are not without their limitations. The limits of the individual sUAS platforms in terms of endurance, speed, and payload capacity mean that swarms cannot travel too far or too fast. Launching so many UASs simultaneously without causing an aerial pileup is also a challenge, as is maintaining command and control of the swarm and its individual members once they are airborne.[208] Mothership UASs, which are larger UASs that house and control smaller UASs that make up a swarm, are one approach to deal with these shortcomings in the short term.[209]

Countering Threats from Uncrewed Aircraft Systems

Right of Launch

Countering UASs, especially sUASs, can be a challenge. The fact that they are so small presents both a small radar cross-section for traditional sensors to observe and a small target for traditional munitions to hit. Their relatively inexpensive nature means they can trade very cost-effectively with traditional air defense capabilities. Swarms will further complicate these challenges.

For remotely controlled sUASs, the traditional means of countering these systems is through electronic warfare targeting the radio frequency command link between a pilot and a UAS. Receivers can detect this signal and decode it, identifying the UAS and locating it. Jammers can deny the ability for this signal to reach the UAS, although a transmitter with the right communication protocol and a stronger signal can override the pilot's commands and take over the UAS. Additionally, the GPS signal allowing UASs to navigate can also be jammed.[210] Both Russia's and Ukraine's forces have developed jamming and counterjamming capabilities to deny an adversary's ability to use remote-controlled UASs while enabling their own.[211]

---

[206] Harper, 2022.

[207] Ross, 2023.

[208] Harper, 2022.

[209] David Hambling, "The US Navy Wants Swarms of Thousands of Small Drones," *MIT Technology Review*, October 24, 2022.

[210] National Urban Security Technology Laboratory, Science and Technology Directorate, U.S. Department of Homeland Security, *Counter–Unmanned Aircraft Systems: Technology Guide*, CUAS-T-G-1, September 2019.

[211] John M. Cantin, "Ukrainian Unmanned Aerial System Tactics," *Red Diamond*, U.S. Army Training and Doctrine Command Operational Environment Enterprise, October 8, 2024.

For semi- or fully autonomous UASs, right-of-launch counter options are more limited. There is no control link to be detected, jammed, or overridden, and many of these systems have begun employing machine vision to navigate in GPS-denied environments, so that, even if their communication abilities and GPS are denied, they can still operate as a swarm through their individual ability to respond to external stimuli.[212] For detecting these UASs, radar systems (particularly those operating in the long band [L-band]) have had success detecting UASs, though potentially not within an operationally relevant range or with sufficient ability to differentiate especially sUASs from other flying objects (e.g., birds). For defeating these UASs, tools include net guns, impactors, and other UASs.[213] However, even kinetic impactors have physical limitations: Fast-moving impactors can face challenges colliding with a maneuverable and autonomous sUAS. Each of these approaches individually can have a low success rate but could find success in a layered situation. For instance, Ukraine has deployed six Shahed drone-hunter systems, which combine radars and jammers with a friendly autonomous drone that uses radar control and AI to intercept and neutralize hostile drones at speeds exceeding 100 km per hour.[214]

The challenge with current kinetic approaches to countering massed UASs is that these approaches do not scale. A swarm of hundreds or thousands of sUASs can quickly overwhelm such defenses and reach their targets largely unimpeded. Even a complex and layered countering system can exhaust itself on a few dozen or so UASs and then have nothing left to counter the rest.[215] Directed-energy weapons, which do not have a limited supply of ammunition to shoot or platforms to launch, might be able to effectively handle swarming threats, but these are still in testing and have not been demonstrated in combat situations.[216] Instead, other solutions that can help fight adversary UASs before they take off might be more effective.

Left of Launch

Given the challenges that current counter-UAS capabilities have, especially with handling large numbers of adversary UASs simultaneously, finding solutions left of (before) launch could prove more valuable. These strategies hamper adversaries' ability to acquire UASs or limit the capabilities and numbers of UASs adversaries do acquire. As a subject-matter expert we interviewed said, "Look at what's being developed and the numbers that are being developed—it's just incredible . . . . You got to find a way on the left of launch to be able to get after this to level the battlefield."[217]

There are several methods to counter UAS threats left of launch. The United States can work with allies and competitors to develop global norms and treaties to limit the spread of lethal autonomous systems, similar to the regime that developed for nuclear, chemical, and biological weapons. The United States could also engage the UN to put controls on the proliferation of lethal

[212] Cotovio, Sebastian, and Goodwin, 2024.

[213] National Urban Security Technology Laboratory, 2019.

[214] Katya Soldak, "Russia's War on Ukraine: Daily News and Information from Ukraine," *Forbes*, January 27, 2023.

[215] Harper, 2022.

[216] An example of such a weapon is the Leonidas system from Epirus, homepage, undated.

[217] Jon Harper, "DOD 'Moving Fast' to Update Counter-Drone Strategy," DefenseScoop, November 14, 2023; stakeholders, interviews with the authors, June to November 2024.

UASs.[218] Given the utility of real-world training data for UASs, the United States could work with its partners in active combat zones, such as in Ukraine, to limit the distribution of these data.[219]

Additionally, as discussed in Chapters 3 and 4, the United States could engage its own export controls to limit adversaries' ability to use U.S.-developed technologies for illicit ends. There are real opportunities to limit the effectiveness of adversary AI-enabled UAS capabilities well before they take off or even leave the factory. However, as we have discussed, these restrictions have their own challenges as well, including for U.S. security posture.

Opportunities from Tightening Export Controls

Export controls face challenges in the UAS market, but there are opportunities available to BIS, especially in limiting the capabilities of countries that have less advanced UASs and in limiting the proliferation of capable UASs. However, these opportunities can be realized only if BIS has staff and funding commensurate with the tasks it needs to undertake.

U.S. Uncrewed Aircraft System Export Controls Likely Would Have Minimal Effect on Chinese Firms

Unlike certain technology areas—those in which the United States, and especially the U.S. defense industrial base, has a significant technology edge over its adversaries—foreign and domestic commercial-sector producers have technology parity in many parts of the UAS technology spaces. The Association for Uncrewed Vehicle Systems International, a U.S.-based trade group, has estimated that companies based in China and subsidized by the Chinese government control 90 percent of the consumer UAS market, at least 70 percent of the enterprise UAS market, and 92 percent of the state and local first responder UAS markets.[220]

Much of this stems from the market dominance of the Chinese company DJI. Trade experts have estimated that DJI owned 76 percent of the global commercial UAS market as of 2021.[221] A 2020 study by Bard College, based on data from the Federal Aviation Administration, showed that DJI products accounted for about 90 percent of law enforcement UAS use.[222] Despite DJI's focus on consumer products, DJI-made UASs can be found on battlefields worldwide, including in the service of both countries in Ukraine.[223] Though not explicitly a UAS manufacturer for the Chinese military, DJI has received funding from the Chinese government as part of the PRC's civilian–military fusion

[218] Zachary Kallenborn, "Meet the Future Weapon of Mass Destruction, the Drone Swarm," *Bulletin of the Atomic Scientists*, April 5, 2021a.

[219] Probasco, 2023.

[220] Association for Uncrewed Vehicle Systems International, "American Drone Competitiveness," press release, undated.

[221] Asia Perspective, "Global Market Share of Consumer and Commercial Drone Manufacturers in March 2021, Based on Sales Volume," *Statista*, June 9, 2021.

[222] Dan Gettinger, "Public Safety Drones," 3rd ed., Center for the Study of the Drone at Bard College, March 2020.

[223] Chris Vallance, "Chinese Drone Firm DJI Pauses Operations in Russia and Ukraine," BBC, April 27, 2022.

strategy, so DoD has labeled it as a Chinese military company.[224] Given the investments from state firms, it is possible that DJI's engineering knowledge has been shared with the Chinese government.

PRC dominance of the worldwide civilian UAS sector has other ancillary benefits for the PRC's military UAS capabilities. The civilian–military fusion strategy is designed to harness the full potential of the country's science and technology development for both civilian and military benefits. It achieves this by leveraging civilian technological advancements to bolster military science and technology and to transition civilian innovations smoothly into the military sector. This strategy extends to strengthening R&D in advanced dual-use technologies and fostering collaboration between civilian and military research entities, including for UAS capability research. The comparative dynamism and efficient management of civilian-sector companies also help address deficiencies with the PRC's largely state-owned military companies.[225]

For larger military UASs, China is similarly well positioned. It already has a suite of platforms that serve a combat role analogous to that of the U.S. Air Force's MQ-9 Reaper and RQ-4 Global Hawk. These include the WZ-7 and supersonic WZ-8, the GJ-11, and the BZK-005 and its newer counterpart, the TB-001. These systems are developed for use by the People's Liberation Army Air Force (PLAAF) and for export to aligned countries worldwide. In DoD's 2024 assessment, the PLAAF rapidly completed its efforts to modernize and indigenize its UAS manufacturing to U.S. standards.[226]

Given China's demonstrated UAS capabilities in both the commercial and military sectors, its strategy to mesh civilian and military manufacturing, and its willingness to export both commercial and military UASs, UAS-specific export controls are unlikely to limit the UAS capabilities of China or of countries that trade with China.

U.S. Uncrewed Aircraft System Export Controls Could Play a Significant Role with Non-China Countries

In targeting other countries, such as Iran or Russia, export controls on UASs and UAS parts might prove more effective. These countries lack the PRC's domestic technological capability and thus rely on foreign companies, including U.S. firms, for key components for their UASs. A U.S. assessment showed that Iran was seeking guidance, navigation, and control equipment, including transceiver modules, controllers, amplifiers, accelerometers, gyroscopes, and inertial measurement units. Iran was also seeking more-general computing and electronic components, such as processors, memories, capacitors, and other ICs.[227] As a result, the United States has long sanctioned various Iranian and Russian companies to limit their access to these technologies.

Despite controls, however, Iranian and Russian defense manufacturers appear capable of obtaining and integrating these sanctioned components into their systems. A Ukrainian assessment showed that

[224] Cate Cadell, "Drone Company DJI Obscured Ties to Chinese State Funding, Documents Show," *Washington Post*, February 1, 2022; DoD, "DOD Releases List of Chinese Military Companies in Accordance with Section 1260H of the National Defense Authorization Act for Fiscal Year 2021," press release, January 7, 2025.

[225] DoD, *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress*, 2024, pp. 30–31.

[226] DoD, 2024.

[227] OFAC, undated.

40 out of 52 components removed from an Iranian Shahed-136 drone were produced by 13 different U.S. companies.[228] A separate independent investigation into Iranian drones shot down in Ukraine, carried out by the UK-based research group Conflict Armament Research, revealed that 82 percent of the components were produced by companies located in the United States.[229] This is despite sanctions on selling U.S.-linked components to Iranian companies, including the manufacturer of the Shahed (which has been under sanction since 2008). Similarly, analyses have shown that sanctions and export controls have led to shortages in Russia for key parts used in UAS manufacturing, causing Russia to shift to relying on North Korean and Iranian suppliers for UASs and parts.[230] Iranian and Russian actors use shell companies, go-betweens, and smugglers to access restricted U.S. parts.[231] They also rely on ubiquitous commercial-grade parts and systems that sellers perceive as low technology and thus might not appear on the CCL of prohibited items.[232]

Iran is actively seeking various key commodities for its UAS development, focusing on specific electronics and guidance, navigation, and control equipment. The list of sought-after electronics includes transceiver modules, processors, controllers, memories, amplifiers, and other ICs. Notably, Iran shows a preference for U.S. brands for some items, such as FPGAs, radio frequency transceivers, microcontrollers, and capacitors. Although some of these items are considered low technology and might not appear on the CCL of the EAR, they are still subject to U.S. sanctions and export controls because of their potential applications.[233]

U.S. export controls could go further to limit prohibited firms in Iran, Russia, and other countries access to key technologies used for producing UASs. The U.S. government has begun to prosecute individuals who have been caught using shell companies in China, Europe, and the Middle East to route U.S.-linked UAS components to Iran.[234] According to our conversations with subject-matter experts, these investigations resemble a game of whack-a-mole: The cost and time involved in bringing them from initiation to prosecution limit the number of offenders that BIS can effectively apprehend or deter. With more funding and appropriately skilled personnel, BIS could support more of these investigations and either stop or divert more U.S.-linked components from reaching Iran or Russia. However, these countries are friendly with China and could shift to using Chinese-sourced parts instead if U.S. enforcement becomes more effective.

[228] The remaining 12 parts came from manufacturers in Canada, Switzerland, Japan, Taiwan, and China (Bertrand, 2023).

[229] Bertrand, 2023.

[230] Starr and Lillis, 2022.

[231] Bertrand, 2023.

[232] OFAC, undated.

[233] OFAC, undated.

[234] Office of Congressional and Public Affairs, 2022.

Limited Opportunities for Controlling Exports of Autonomous Capabilities for Uncrewed Aircraft Systems

As militaries develop greater capability, there might be opportunities for export controls to increase security, but those opportunities are unlikely to arise from limiting access to hardware.[235] For example, the People's Liberation Army (PLA) is exploring "intelligentized warfare" using such UAS concepts as intelligent-swarm cross-domain mobile warfare, AI-driven space confrontations, and cognitive control operations. PLA UAS efforts are aiming for greater autonomy in uncrewed systems across all domains to facilitate such capabilities as crewed–uncrewed teaming, swarm attacks, optimized logistic support, and distributed intelligence, surveillance, and reconnaissance.[236]

The export controls on AI-related hardware that we covered in Chapter 2 are unlikely to significantly constrain these types of autonomy. Current controls target primarily advanced chips and the computational scaling necessary for large language models. In contrast, most existing autonomous UAS applications require hardware that falls well below the thresholds established by the 2023 export controls. As a result, it would be challenging for the United States to regulate this level of hardware effectively.

Instead, opportunities to limit access to autonomous capabilities might lie in restricting the dissemination of training data that could enable UASs to operate effectively on the battlefield. Unlike the hardware required for autonomy, which is widely available and often dual-use, training data that are specific to military UAS operations are more specialized, potentially more amenable to control, and possibly less available or relevant to commercial end users.[237] Machine learning algorithms that developers have trained on data can be integrated into UASs to shape UAS behavior. These data should be extensive enough to cover the types of scenarios a UAS would encounter on the battlefield in order for the UAS to be sufficiently adaptive and capable without a qualified human in control of the platform. This type and extent of data would be difficult to come by on commercial markets and would not have an easily identified dual-use justification. Commercial UASs do not often need to be able to dodge incoming fire, operate in GPS-denied environments, maneuver around hostile UASs, or engage in any number of other operational scenarios that an UAS might encounter on the battlefield. Thus, the pilots and owners of these systems will not be collecting flight data for these scenarios or training their systems on these data. The only sources for these data would be contractors and developers creating UASs for wartime purposes and warfighters using such UASs. To be clear, this analysis is speculatory and does not reflect current conditions—rather, it suggests potential future issues.

Thus, BIS could, in theory, impose restrictions on the export of such data and any models derived from them. However, implementing such controls could be challenging in practice. The U.S. government would first need to establish clear criteria for what makes data military training data and develop reliable methods for distinguishing those data, and the resulting models, from other types of operational data. Achieving this would require specialized expertise that BIS does not currently

[235] DoD, *Military and Security Developments Involving the People's Republic of China 2023: Annual Report to Congress*, circa 2023, p. 97.

[236] DoD, 2023.

[237] Non–dual-use training data could include signature profiles of other military aircraft, data reflecting military tactics or strategy, or targeting and range information.

possess, plus ongoing engagement with the stakeholder community involved in developing autonomous UASs for DoD and U.S. allies.[238] But if BIS could work around these hurdles, controls on data and models could be a real means of limiting the proliferation of autonomous UASs to hostile countries. Again, this does not reflect current conditions in export control but instead suggests steps BIS could take to address autonomous UASs in the future.

Risks from Tightening Export Controls

Export controls for UAS have opportunities but also limitations. The U.S. government should weigh these risks before enacting a broader regime of export controls for these systems. As mentioned previously, the U.S. defense sector is not at the lead of the state of the art for the technology, and the nearest peer competitor, China, has significant and growing commercial and military capabilities in this area, and this limits the potential upside from U.S. controls.

Export controls can also pose risks to key U.S. security objectives. Some U.S. allies are limited in capabilities and could require access to large numbers of systems, particularly in the face of a protracted conflict similar to the war in Ukraine. U.S. export controls could limit those allies' ability to build up an effective UAS capability to defend themselves or support the United States. A 2023 study showed that many NATO member states had severe shortfalls of the minimum number of sUASs they would require to fight any near-peer or peer conflict.[239] Additionally, U.S.-based manufacturers, in both the commercial and military spaces, face significant foreign competition for their products, and export controls could risk limiting their ability to remain profitable and could empower manufacturers in competitor countries.

Consideration of these risks—that these can weaken international deterrence by providing allies inferior technology—motivated a 2018 revision to the MTCR to enable the United States to better export UASs. However, such risks seem to have only grown since 2018.[240]

Furthermore, autonomous UASs could present their own considerations. For example, allowing allies to purchase UASs from China could lead to interoperability and data security concerns in the event of a conflict in which U.S. and allied forces armed with Chinese and U.S. drones fought together. Additionally, allowing Chinese drones to fill the market gap that U.S. export controls create could decrease the U.S. ability to exercise influence over how such drones are used in other countries. An example of this is Ethiopia's purchases of military drones from China and other countries that were used in the wars in the Tigray and Amhara regions, resulting the deaths of nearly 200, including some civilians, in drone strikes.[241] It is possible that, if the United States had made these sales instead, it could have exercised influence by attaching stipulations to the sales and prevented some of these deaths. The United States could still decide to not make sales to such countries, but this consideration should be a part of the calculus of how tightly exports of UASs should be controlled. This could also extend to exercising influence over how countries control the chain of custody of such systems. The

[238] Stakeholder, interview with the authors, November 2024.

[239] Borsari and Davis, 2023.

[240] Glen Carey, "U.S. to Ease Export Controls on Military Drone Sales to Allies," Bloomberg, July 24, 2020.

[241] Zecharias Zelalem, "Deadly Skies: Drone Warfare in Ethiopia and the Future of Conflict in Africa," policy brief, European Council on Foreign Relations, February 28, 2025.

United States could exercise influence through stipulations attached to drone sales to target safeguard sales in an attempt to ensure that states with weaker infrastructure have proper systems in place to prevent UASs from falling into the hands of violent nonstate actors.[242] Export controls are designed to prevent these scenarios, but the crux of the issue is this question: If China is going to fill the market, and the buyers will have the drones one way or another, is the United States better off supplying the drones themselves and exercising influence after the sale?

Export Controls Could Limit U.S. Allies' Access to Needed Capabilities

As seen in Ukraine and elsewhere, sUASs can operate similar to both a platform, like an aircraft, and an expendable, like a missile. Thus, a key challenge for using these systems effectively is maintaining sufficient stockpiles, similar to those of other expendables. For instance, more-effective counter-UASs (C-UASs), operator error, and C-UASs' use as one-way attack or surveillance platforms have all caused high attrition of sUASs in Ukraine. Analysts have noted that technology advancements, especially in the capacity of cheap-to-manufacture UASs, are pushing warfare toward mass deployment of systems.[243] Maintaining the number of sUASs to meet the battlefield need would require significant industrial capacity and would require U.S. allies to supply themselves a sufficient number of capable UASs or rely on U.S.-produced systems, a reliance that tightening export controls could imperil.

Compared with capabilities of peer and competitor countries, non-U.S. NATO countries currently face shortfalls in their sUAS capabilities, particularly for engaging in high-intensity conflicts with peer adversaries in contested environments. An assessment by the Center for European Policy Analysis showed that NATO allies had "nowhere near the minimum number [of sUASs] that would be required in near-peer or peer adversary scenario."[244] This same analysis also showed significant qualitative and quantitative deficiencies in NATO's larger UAS capabilities for engaging in potential high-intensity conflicts. For instance, it showed that most NATO members, outside the United States, UK, France, Turkey, and Italy, have not weaponized their medium-altitude, long-endurance (MALE) UASs.[245] Deficiencies in U.S. allies' UAS capabilities are not confined to NATO countries: The ROK only recently began standing up a dedicated UAS capability, following a December 2022 incursion by North Korean UASs that the ROK needed to scramble fighter jets to respond to.[246]

To address these UAS and sUAS capacity deficiencies, U.S. allies are heavily reliant on U.S.-made systems. Current Class I and Class II systems in use by NATO-allied countries come primarily from U.S. suppliers, including the RQ-11B Raven, RQ-20 Puma, and ScanEagle tactical UAS.[247] For similarly sized loitering munitions, U.S.-made Switchblades are similarly popular, although other

[242] A safeguard sale is a type of weapon sale on which the United States puts stipulations to ensure that the purchasing country does not engage in war crimes or genocide.

[243] Ross, 2023.

[244] Borsari and Davis, 2023.

[245] Borsari and Davis, 2023.

[246] Tara Sonenshine, "Military Drones Are Swarming the Skies of Ukraine and Other Conflict Hot Spots—and Anything Goes When It Comes to International Law," The Conversation, May 19, 2023.

[247] Borsari and Davis, 2023.

countries have begun developing domestic alternatives, including the French Colibri and the Polish Warmate.[248] At the Class III level, there are more-robust non-U.S. NATO options, such as France's Patroller, Portugal's Ogassa OGS42, Norway's FX450, and, most notably, Turkey's TB2, Anka, and Akıncı. There is also an ongoing effort between Germany, France, Spain, and Italy to develop a Class III Eurodrone set to launch in 2028, although this effort has faced design and production challenges.[249] As of this writing in late 2025, though, these non-U.S. UAS platforms (other than the TB2) still lack significant battlefield experience, and, even at the Class III level, there is a preference for the tested, U.S.-made MQ-9.[250]

Limits on the exports of popular and effective U.S. UASs, their successor systems, or the components needed for U.S. allies to invest in their own burgeoning UAS capabilities risk harming U.S. allies' ability to develop needed UAS capabilities and capacities. U.S. allies are reliant on U.S.-made systems and components to build sufficient stockpiles of UASs to withstand expected attrition in a high-intensity engagement. U.S. export controls usually exempt purchases by allied countries, but crackdowns on shell companies and intermediaries in these countries could have negative secondary effects.

Export Controls Could Harm U.S. Uncrewed Aircraft System Manufacturers in Global Competition

As demonstrated earlier, UAS, especially sUAS, manufacturing is not an area of exclusive expertise or even comparative expertise for U.S. manufacturers. U.S.-made UASs and components face intense competition, especially from Chinese companies, and export controls to nonallied countries could allow these competing firms to corner the market for UASs in these countries. This not only closes off profitable opportunities for U.S. firms, which already face challenges breaking into the global UAS market; it also closes off opportunities for the United States to use access to these UASs as leverage for other policy outcomes.

Chinese UAS manufacturers have already shown success in selling their technology to a variety of global military buyers. DJI's dominance of the commercial UAS market has meant that jerry-rigged commercial sUASs for military purposes use Chinese-made systems. Both state actors and nonstate actors have employed modified DJI systems for lethal and nonlethal purposes.[251] To regulate this unauthorized use of UASs, including in the Ukraine conflict, China announced its first set of controls on the civilian and dual-use drone markets in 2023, including the sale of counter-UAV systems.[252]

---

[248] Tim Martin, "France Begins Delivery of 100 Loitering Munitions to Ukraine," Breaking Defense, November 5, 2024; WB Group, "WARMATE Loitering Munitions," webpage, undated.

[249] An example of such a challenge is heavy weight and configuration changes, as discussed in John Hill, "OCCAR Must Avoid Eurodrone Design Alterations After First Board Meeting," Airforce Technology, March 5, 2024.

[250] Borsari and Davis, 2023.

[251] Both Ukraine and Russia have used modified DJI systems for a variety of purposes. See, for instance, Starr and Lillis, 2022. Among the many possible examples of nonstate actors using these systems is the 2018 attempted assassination of Venezuelan president Nicolás Maduro, in which two DJI Matrice 600 UAS laden with plastic explosives were used. See Eliott C. McLaughlin, Joe Sterling, and Stefano Pozzebon, "Venezuela Says It Has ID'd Mastermind, Accomplices in Apparent Maduro Assassination Try," CNN, August 7, 2018.

[252] DoD, 2023, p. 15.

This success extends to explicitly military UASs. For instance, since 2014, China Aerospace Science and Technology has exported strike-capable Rainbow UASs to countries across the Middle East, Africa, and Asia, according to public information. These are not limited to just Chinese-made UASs: In March 2017, Saudi Arabia and China agreed to jointly produce up to 100 Rainbow drones.[253] Furthermore, in 2016, satellite images revealed the Chinese-made long-range Wing Loong UAS sitting in a Saudi-operated runway in Yemen, and additional satellite images have shown Chinese UASs at military bases in Egypt and the United Arab Emirates and involved in operations from Nigeria to Iraq.[254] More recently, DoD has identified sales to multiple countries in Africa, including the 2023 sale of nine armed UASs to the Democratic Republic of the Congo.[255] These countries, which include some U.S. allies, are often blocked from purchasing U.S. drones and thus have turned to Chinese alternatives.

China is not the only competitor country selling UASs to countries with which the United States will not do business; Iran has also had success selling its UAS capabilities to third parties around the globe. These include actors that are traditionally considered Iran-aligned groups, including sending UAS shipments to the Houthis in Yemen. It also includes sales of UASs and UAS production capabilities to other countries across Asia, such as Russia and Tajikistan, to enhance Iran's bilateral ties with these countries, evade sanctions on itself, and increase the profitability of its export sector.[256]

The expansion of sales of Chinese-made UASs has made the U.S. export market more challenging, and export controls further compound these challenges. Chinese-made UASs are already less expensive than their U.S.-made counterparts: The above-mentioned Class III Wing Loong cost about $1 million, compared with approximately $15 million for the MQ-9 that is popular with U.S. allies.[257] China also puts fewer restrictions on the use of its systems than the United States does. Export controls risk further limiting U.S. manufacturers' ability to sell to willing buyers on the global market and further entrenching Chinese-made UASs in that market without significantly limiting the capabilities of bad actors that can fall back on willing Chinese sellers. This also risks the United States' ability to use its considerable military technology as an inducement for diplomacy in these countries.

These considerations focus on the challenges for U.S. military UAS manufacturers, but U.S. firms making civilian UASs would also be challenged by any limitations on exporting, especially UASs. Some features, such as real-time data processing, automated flight paths, and improved payload capacities, have made sUASs even more effective in modern warfare but have also made these systems more effective at achieving innocuous ends as well. Limits on UASs that target these and similar capabilities will inevitably bite into commercial UAS firms' ability to offer competitive systems to global customers.[258] These capabilities are not exclusive to the United States or reliant on U.S.-linked components, so products with such capabilities are already proliferating across the global commercial

[253] Page and Sonne, 2017.

[254] Page and Sonne, 2017.

[255] DoD, 2023, p. 15.

[256] OFAC, undated, p. 2.

[257] Page and Sonne, 2017.

[258] Vincent, 2024.

UAS market. The dual-use nature of most relevant UAS capabilities complicates construction of overbroad regulatory and control measures.

Balancing Risks and Opportunities

Left-of-launch options (ways to defend against products before they leave the ground) for countering UASs offer opportunities and risks, not unlike right-of-launch options. However, these opportunities are greatest for limiting the capabilities of non-Chinese competitors and much more limited for restraining the capabilities of Chinese-made UASs. However, the presence of Chinese-made UASs in the global marketplace mean that the risks to U.S. allies and to U.S.-based manufacturers remain significant even for controls that do not apply to China.

Another key opportunity for U.S. policymakers might be limiting training data related to UAS operations in a conflict. Unlike UASs or UAS components, training data of this nature are not widely available on the commercial market. Additionally, unlike more-generalized limits on exports of UASs with specific AI-enabled capabilities, such as machine vision or automated decisionmaking, these data have limited dual-use applications, and this fact makes regulatory controls less complicated and lessens the collateral risks to U.S. manufacturers. The challenge for regulators will be defining a standard that can isolate these data and applying that standard to a variety of algorithms that might or might not have been trained on these or similar data.

A key complication for U.S. policymakers is that, regardless of U.S. controls, China is engaged in an industrial policy to boost its own capabilities and stave off global competition. As outlined in its state plans, China aims for self-sufficiency in key science and technology areas, including for UASs and AI. The Made in China 2025 policy further focuses on technological independence by setting import substitution quotas in these key technology areas, alongside fostering regional innovation centers and leveraging private-sector capabilities for robotics and AI in state-run firms to surpass foreign competitors' capabilities. U.S. export controls in the semiconductor space have limited the effectiveness of the PRC's import substitution–focused strategy but have also bolstered China's commitment to building a domestic state-of-the-art semiconductor capability. Current conditions strongly encourage China and, to some extent, third-party suppliers to China to minimize reliance on Western technology, which parallels U.S. efforts to limit PRC access to U.S. innovations. A final consideration for policymakers is that there are systemic risks beyond competition in the market and on the battlefield. As weapons evolve into large-scale drone swarms, their immense capability begins to approximate a new weapon of mass destruction. Furthermore, because autonomous systems can respond to and counter each other much more effectively than humans can, the only viable right-of-launch defeat capability will have to be similarly autonomous and capable.[259] As this arms race increases and highly capable UASs proliferate, policymakers might find themselves in a dire situation for global security that the United States cannot resolve alone.

[259] Zachary Kallenborn, "Applying Arms-Control Frameworks to Autonomous Weapons," commentary, Brookings Institution, October 5, 2021b.

Chapter 6

A Way Forward: Balance China Competition and National Security with Securely Guided Proliferation

In this chapter, we present our overarching findings, recommendations, and a road map for how DOC, DoD, DOS, other federal agencies, and the private sector could work together to address challenges and form solutions. Some of these findings, challenges, and recommendations could be salient in export control issues outside AI-enabled UASs as well, offering added value to solutions.

Overarching Findings

The findings reflect insights from the analysis of U.S. export controls on AI and UASs. They capture how current regulations affect national security, industry competitiveness, and international proliferation. Because UAS controls have a longer history than those on AI, many findings draw from that experience, although others extend to AI where regulatory gaps are more prevalent:

- The U.S. defense industrial base lacks a significant technology edge over adversaries' industrial bases in AI and UASs. This shifts the risk–reward calculation on tightening or relaxing export controls in these areas.
- The United States still maintains some lead in AI and in some areas of military UASs, but it no longer acts from a monopolistic technology position like it did with AI and military UASs before 2018.
- Overregulation of AI and UASs poses the risk of dampening domestic competitiveness, accelerating advancements abroad, and creating security risks driven by China arming or making transfers to U.S. allies and partners. Foreign governments could also respond to U.S. export controls with retaliatory or punitive policies affecting access to critical resources.
- AI and UAS export control dynamics create feedback loops in which export controls can either strengthen the United States' lead in technologies or create a death spiral of regulation that depletes the U.S. technological lead in areas in which the United States maintains an advantage.
- Export controls for AI and UASs make up a dynamic and adaptive system that could be evaluated more efficiently and regularly and that requires analysis looking further in the future.
- Growth in technology competition, larger volumes of export control–related data, new methods of export control circumvention, and increasingly blurred lines between civilian and military uses of AI and UASs will increase the need for efficiency and adaptiveness.

- AI is newer than UASs in a military context, and DTSA could benefit from developing increased knowledge of the industry's infrastructure and ecosystem.
- DOC is understaffed and underfunded for meeting current needs for AI and UAS export controls. If trends in technology advancement and diversion efforts continue, the gap between capabilities and needs will likely grow. The evolution of AI-enabled UASs will likely add new dimensions to this problem.
- Data regulation is a critical consideration for AI-enabled UASs in the future and an area in which BIS could theoretically limit adversaries' access; however, imposing such limits would require identifying the differences between military training data and commercial data and require BIS to increase its expertise and further its engagement efforts (ideally in a joint forum) with stakeholders developing AI and UASs for the United States and its allies.
- There might be opportunities for limiting access to autonomous capabilities via limiting the spread of training data required to develop an autonomous UAS capable of performing on the battlefield.
- The U.S. government—the legislative and executive branches—would need to task DOC, DoD, and DOS with identifying criteria that make data military training data (which could originate from commercial sources) as opposed to other operational data, along with a means of identifying such data and the models that result from training on those data.
- Regulating training data for autonomous UASs would require expertise that BIS does not currently have, as well as repeated engagement with the stakeholder community that is developing autonomous UASs for use by DoD and U.S. allies. If, however, BIS could work around these hurdles, controls on data and models could be a real means of limiting the proliferation of autonomous UASs to hostile countries.

There are more-traditional opportunities available to BIS in limiting the capabilities of countries with less advanced capabilities and in limiting the proliferation of capable, autonomous UASs. These opportunities can be realized only if BIS has the staff and funding commensurate with the tasks it needs to undertake.

Recommendations

The recommendations build on the analysis presented in earlier chapters and are intended to inform both immediate policy adjustments and longer-term regulatory design. The recommendations reflect the dual focus of this report on AI and UASs. Furthermore, both AI and UASs are addressed, but many of the qualitative insights are centered on UASs because export controls for these systems have legacy regulatory exemplars. As a result, many of the recommendations emphasize AI because it is emergent technology with less tested regulatory guidelines and frameworks. Together, these recommendations are intended to balance competition with China, sustain U.S. technological leadership, and guide the secure proliferation of AI and UAS technologies.

DoD should find ways to further develop innovation leadership with R&D for UASs and AI:

- In the past, military demands drove technological advancements, but commercial innovations have shifted the dynamic dramatically, and segmentation has increased.

- Although industry R&D funding might continue to surpass that of DoD, DoD could still play a leadership role in driving innovation and anticipating security and regulatory challenges.
- Deepening relationships with smaller, nontraditional defense industrial base firms at the forefront of innovation is critical to DoD's ability to inform export controls and mitigate risk.

DTSA should work more in depth with the AI industry to increase understanding of the infrastructure and ecosystem related to AI, mirroring BIS efforts:

- It should continue to increase interaction with industry and further capitalize on firms' desire to interact with DTSA early and often during the technology development process as they streamline their efforts to take technologies to global markets as military applications increase.
- Cooperation and learning from this process can enable DoD to better balance and manage increasingly segmented but overlapping technologies, such as AI and UASs, and can improve its ability to advise on export controls.

DTSA and DOC should conduct more-proactive analysis to identify and assess potential security risks associated with technological advancements:

- They should engage in analysis focused three to ten years in the future, outside the scope of current technology levels.
- They should perform technology forecasting to anticipate security challenges *before* they become critical issues.
- They should focus on the security implications of technological trends, highlighting potential dual uses.

The **U.S. government** should develop a more flexible and responsive regulatory framework for adaptive policymaking:

- It should improve DOC's, DoD's, and DOS's ability to quickly adjust export controls in response to new information or national security threats related to emerging technologies, thereby maintaining a balance between national security and technological advancement and decreasing the time from the identification of a national security threat to the drafting and implementation of export controls.
- The U.S. government needs to increase resources for BIS to engage more extensively with industry and to broaden emerging-technology expertise. BIS faces unique budgetary challenges, and DOC's focus on dual-use technology necessitates a great deal of complex interaction with industry.
- It should codify and publish the regulatory process and responsibilities in DoD, DOC, and DOS doctrine to address concerns about blurred lines and unclear responsibilities.

DOC should lead an effort with DOS and DoD to explore methods and procedures for more systematically tracking the effects and effectiveness of export regulations as perceived by each department.

DOC, DoD, and DOS should expand interagency efforts at technology assessments and forecasting to consider the *intersection* of emerging technologies, such as AI and UASs, and decrease stovepiping of relevant areas of expertise.

A Road Map for Regulatory Improvements

Table 6.1 provides a streamlined version of the challenges we found and our accompanying recommendations, organized using DOTmLPF. These are challenges and recommendations that apply to AI-enabled UASs but also to AI, UASs, and other technologies as well. They could provide benefits for multiple facets of export controls.

Table 6.1. A DOTmLPF Framework for Implementing the Road Map

DOTmLPF	Challenges	Recommendations
Doctrine	• There is no clear approach or rule set for BIS to balance regulation and application. • The regulatory process is not codified in doctrine or policy. • Policy and regulation do not keep up with technologies. • The effects of regulations are more difficult to track than the effectiveness of regulations is.	• The U.S. government should develop a more flexible and responsive regulatory framework. • The U.S. government should codify and publish the regulatory process and responsibilities in DOS, DOC, and DoD doctrine. • DOC should lead an effort to explore methods and procedures for tracking the effects and effectiveness of export regulations.
Organization	• The federal bureaucracy can restrict the state of practice. • Industry must interact with multiple siloed federal organizations. • BIS is underfunded. • Exchange between industry and the U.S. government is inconsistent; even with consistent change, though, it might be insufficient.	• The U.S. government should increase resources for BIS to engage more with industry.
Training		
Materiel	• Assessment and regulation of technologies are siloed.	• DoD should further develop innovation leadership with R&D for UASs and AI. • DTSA should better understand the infrastructure and ecosystem related to AI. • DTSA, DOC, and DOS should conduct more-proactive analysis to identify and assess potential security risks associated with technological advancements. • DOC, DoD, and DOS should expand technology assessments and forecasting to consider the *intersection* of various emerging technologies.
Leadership and education		
Personnel	• BIS has an insufficient talent pool both in numbers and in skills. • Resources might be insufficient for ensuring regulatory compliance.	• The U.S. government should increase resources for BIS.
Facilities		

Abbreviations

AI	artificial intelligence
AMD	Advanced Micro Devices
ASML	Advanced Semiconductor Materials Lithography
BIS	Bureau of Industry and Security
CCL	Commerce Control List
CONOPS	concept of operations
CSIS	Center for Strategic and International Studies
DDTC	Directorate of Defense Trade Controls
DJI	Da-Jiang Innovations
DOC	U.S. Department of Commerce
DoD	U.S. Department of Defense
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
DOTmLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
DRAM	dynamic random-access memory
DTSA	Defense Technology Security Administration
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
EU	European Union
FDP	foreign direct product
FPGA	field-programmable gate array
GB	gigabyte
GPS	Global Positioning System
HBM	high-bandwidth memory
IC	integrated circuit
IFCA	Iran Freedom and Counter-Proliferation Act of 2012
ITAR	International Traffic in Arms Regulations
MEU	military end user
MTCR	Missile Technology Control Regime
NAND	not and
NATO	North Atlantic Treaty Organization
nm	nanometer
OFAC	Office of Foreign Assets Control
PRC	People's Republic of China
R&D	research and development

ROK	Republic of Korea
SDN	specially designated national
SME	semiconductor manufacturing equipment
sUAS	small uncrewed aircraft system
UAS	uncrewed aircraft system
UAV	uncrewed aerial vehicle
UK	United Kingdom
UN	United Nations
USML	U.S. Munitions List
WA	Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies
WMD	weapons of mass destruction

References

Allen, Gregory C., "Choking Off China's Access to the Future of AI," Center for Strategic and International Studies, October 11, 2022.

Allen, Gregory, director, Wadhwani Center for Artificial Intelligence and Advanced Technologies, Center for Strategic and International Studies, "China's Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes," statement before the U.S.–China Economic and Security Review Commission, April 13, 2023a.

Allen, Gregory C., "Blocking China's Access to AI Chips Matters to U.S. National Security," commentary, Center for Strategic and International Studies, July 31, 2023b.

Allen, Gregory C., director, Wadhwani Center for Artificial Intelligence and Advanced Technologies, Center for Strategic and International Studies, "Advanced Technology: Examining Threats to National Security," statement before the U.S. Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Emerging Threats and Spending Oversight, September 19, 2023c.

Allen, Gregory C., "The True Impact of Allied Export Controls on the U.S. and Chinese Semiconductor Manufacturing Equipment Industries," Center for Strategic and International Studies, November 26, 2024a.

Allen, Gregory C., "Understanding the Biden Administration's Updated Export Controls," Center for Strategic and International Studies, December 11, 2024b.

Allen, Gregory C., and Emily Benson, "Clues to the U.S.–Dutch–Japanese Semiconductor Export Controls Deal Are Hiding in Plain Sight," Center for Strategic and International Studies, March 1, 2023.

Allen, Gregory C., Emily Benson, and William Alan Reinsch, "Improved Export Controls Enforcement Technology Needed for U.S. National Security," Center for Strategic and International Studies, November 30, 2022.

Asia Perspective, "Global Market Share of Consumer and Commercial Drone Manufacturers in March 2021, Based on Sales Volume," *Statista*, June 9, 2021.

Association for Uncrewed Vehicle Systems International, "American Drone Competitiveness," press release, undated.

Axelrod, Matthew S., "Remarks as Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod to the Society for International Affairs 2022 Fall Advanced Conference," Bureau of Industry and Security, U.S. Department of Commerce, November 14, 2022.

Baums, Ansgar, "The 'Chokepoint' Fallacy of Tech Export Controls," Henry L. Stimson Center, February 6, 2024.

Benson, Emily, "The Fifth Ministerial of the U.S.–EU Trade and Technology Council," *Critical Questions*, Center for Strategic and International Studies, February 7, 2024.

Bergengruen, Vera, "How Tech Giants Turned Ukraine into an AI War Lab," *Time*, February 8, 2024.

Bertrand, Natasha, "CNN Exclusive: A Single Iranian Attack Drone Found to Contain Parts from More Than a Dozen US Companies," CNN, January 4, 2023.

Biden, Joseph R., Jr., "Executive Order 14024 of April 15, 2021: Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation," *Federal Register*, Vol. 86, No. 74, April 19, 2021.

BIS—*See* Bureau of Industry and Security.

Borsari, Federico, and Gordon B. "Skip" Davis, Jr., *An Urgent Matter of Drones*, Center for European Policy Analysis, September 27, 2023.

Brown, Gordon, Mohamed El-Erian, and Michael Spence, with Reid Lidow, *Permacrisis: A Plan to Fix a Fractured World*, Simon and Schuster, 2023.

Bureau of Industry and Security, U.S. Department of Commerce, "BIS Website: Missile Technology FAQs," webpage, undated. As of January 5, 2025: https://www.bis.doc.gov/index.php/component/fsj_faqs/cat/19-missile-technologyfaqs

Bureau of Industry and Security, U.S. Department of Commerce, "Change to the License Review Policy for Unmanned Aerial Systems (UAS) to Reflect Revised United States UAS Export Policy," *Federal Register*, Vol. 86, No. 7, January 12, 2021a (final rule).

Bureau of Industry and Security, U.S. Department of Commerce, "Request for Comments Concerning Imposition of Export Controls on Brain–Computer Interface (BCI) Emerging Technology," *Federal Register*, Vol. 86, No. 204, October 26, 2021b (proposed rule).

Bureau of Industry and Security, U.S. Department of Commerce, "Revisions to the Unverified List; Clarifications to Activities and Criteria That May Lead to Additions to the Entity List," *Federal Register*, Vol. 87, No. 197, October 13, 2022 (final rule).

Bureau of Industry and Security, U.S. Department of Commerce, "Export Control Measures Under the Export Administration Regulations (EAR) to Address Iranian Unmanned Aerial Vehicles (UAVs) and Their Use by the Russian Federation Against Ukraine," *Federal Register*, Vol. 88, No. 38, February 27, 2023 (final rule).

Bureau of Industry and Security, U.S. Department of Commerce, "Supplement No. 1 to Part 774: The Commerce Control List," Export Administration Regulations, Chapter VII, last updated January 6, 2025a.

Bureau of Industry and Security, U.S. Department of Commerce, "Framework for Artificial Intelligence Diffusion," *Federal Register*, Vol. 90, No. 9, January 15, 2025b (interim final rule and request for comments).

Bureau of Political–Military Affairs, U.S. Department of State, "U.S. Policy on the Export of Unmanned Aerial Systems," fact sheet, undated.

Bureau of Political–Military Affairs, U.S. Department of State, "Myths and Facts About U.S. Defense Export Controls," fact sheet, July 10, 2023.

Bush, George W., "Executive Order 13382 of June 28, 2005: Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters," *Federal Register*, Vol. 70, No. 126, July 1, 2005.

Cadell, Cate, "Drone Company DJI Obscured Ties to Chinese State Funding, Documents Show," *Washington Post*, February 1, 2022.

Cantin, John M., "Ukrainian Unmanned Aerial System Tactics," *Red Diamond*, U.S. Army Training and Doctrine Command Operational Environment Enterprise, October 8, 2024.

Carey, Glen, "U.S. to Ease Export Controls on Military Drone Sales to Allies," Bloomberg, July 24, 2020.

Clark, Joseph, "Hicks Underscores U.S. Innovation in Unveiling Strategy to Counter China's Military Buildup," U.S. Department of Defense, August 28, 2023.

Clement, Chris, and Sidney Traynham, *Economic Security Is National Security*, Global Economic Hub, U.S. Global Leadership Coalition, June 2025.

Clinton, William J., "Executive Order 12938 of November 14, 1994: Proliferation of Weapons of Mass Destruction," *Federal Register*, Vol. 59, No. 220, November 16, 1994.

Code of Federal Regulations, Title 15, Commerce and Foreign Trade; Subtitle B, Regulations Relating to Commerce and Foreign Trade; Chapter VII, Bureau of Industry and Security, Department of Commerce; Subchapter C, Export Administration Regulations.

Code of Federal Regulations, Title 22, Foreign Relations; Chapter I, Department of State; Subchapter M, International Traffic in Arms Regulations.

Code of Federal Regulations, Title 31, Money and Finance: Treasury; Subtitle B, Regulations Relating to Money and Finance; Chapter V, Office of Foreign Assets Control, Department of the Treasury; Part 560, Iranian Transactions and Sanctions Regulations.

Cotovio, Vasco, Clare Sebastian, and Allegra Goodwin, "Ukraine's AI-Enabled Drones Are Trying to Disrupt Russia's Energy Industry. So Far, It's Working," CNN, April 2, 2024.

DDTC—*See* Directorate of Defense Trade Controls.

Directorate of Defense Trade Controls, U.S. Department of State, "ITAR and Export Controls," webpage, undated. As of September 22, 2025:
https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landing

DOC—*See* U.S. Department of Commerce.

DoD—*See* U.S. Department of Defense.

Dou, Eva, "Commerce Department Moves to Cut Key Supply Lines to China's AI Industry," *Washington Post*, October 17, 2023.

Epirus, homepage, undated. As of March 4, 2025:
https://www.epirusinc.com/

Estevez, Alan F., "A Conversation with Under Secretary of Commerce Alan F. Estevez," Center for a New American Security, October 27, 2022.

Estevez, Alan F., "Statement of Alan F. Estevez, Undersecretary of Commerce for Industry and Security, U.S. Department of Commerce," testimony for U.S. House of Representatives Committee on Foreign Affairs hearing, *Combating the Generational Challenge of CCP Aggression*, February 28, 2023.

Fedorov, Mykhailo, "Ukraine's Vibrant Tech Ecosystem Is a Secret Weapon in the War with Russia," *UkraineAlert* blog, August 17, 2023.

Fitch, Asa, Yuka Hayashi, and John D. McKinnon, "U.S. Considers New Curbs on AI Chip Exports to China," *Wall Street Journal*, June 27, 2023.

Fogel, Benjamin, and Andro Mathewson, "The Next Frontier in Drone Warfare? A Soviet-Era Crop Duster," *Bulletin of the Atomic Scientists*, February 10, 2021.

Gerstein, Daniel M., and Erin N. Leidy, *Emerging Technology and Risk Analysis: Unmanned Aerial Systems Intelligent Swarm Technology*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-A2380-1, 2024. As of November 18, 2024: https://www.rand.org/pubs/research_reports/RRA2380-1.html

Gettinger, Dan, "Public Safety Drones," 3rd ed., Center for the Study of the Drone at Bard College, March 2020.

Global Information Services, Bureau of Administration, U.S. Department of State, "Defense Export Control and Compliance System (DECCS)," privacy impact assessment, January 4, 2022.

Hambling, David, "The US Navy Wants Swarms of Thousands of Small Drones," *MIT Technology Review*, October 24, 2022.

Harper, Jon, "Drone Swarms with 1,000 Unmanned Aircraft Could Be Possible Within 5 Years, DARPA Leader Says," DefenseScoop, April 5, 2022.

Harper, Jon, "DOD 'Moving Fast' to Update Counter-Drone Strategy," DefenseScoop, November 14, 2023.

Hayashi, Yuka, and Asa Fitch, "U.S. Tightens Curbs on AI Chip Exports to China, Widening Rift with Nvidia and Intel," *Wall Street Journal*, October 17, 2023.

Henshall, Will, "What to Know About the U.S. Curbs on AI Chip Exports to China," *Time*, October 17, 2023.

Hill, John, "OCCAR Must Avoid Eurodrone Design Alterations After First Board Meeting," Airforce Technology, March 5, 2024.

Ing, Lili Yan, "ASEAN's Role in the Global Semiconductor Race," ThinkChina, October 2, 2023.

International Trade Administration, "Export Control Classification # (ECCN) and (EAR99)," webpage, undated. As of February 27, 2025: https://www.trade.gov/eccn-and-export-administration-regulation-ear99

Jin, Keyu, "How China Is Fighting the Chip War with America," *New York Times*, October 27, 2022.

Kallenborn, Zachary, "Meet the Future Weapon of Mass Destruction, the Drone Swarm," *Bulletin of the Atomic Scientists*, April 5, 2021a.

Kallenborn, Zachary, "Applying Arms-Control Frameworks to Autonomous Weapons," commentary, Brookings Institution, October 5, 2021b.

Kendler, Thea D. Rozman, "Statement of Thea D. Rozman Kendler, Assistant Secretary of Commerce for Export Administration, Before the Senate Banking, Housing, and Urban Affairs Committee Hearing Entitled, 'Countering China: Advancing U.S. National Security, Economic Security, and Foreign Policy,'" May 31, 2023.

King, Ian, and Jenny Leonard, "US Chip-Gear Makers Told to Wait for Relief from China Curbs," Bloomberg, November 3, 2022.

Kutuk, Yuksel, *UAS (Unmanned Aircraft Systems): The Force Multiplier for Law Enforcement Agencies and the Potential Contributor to Stability Policing*, Stability Policing Centre of Excellence, North Atlantic Treaty Organization, 2025.

Lovett, Ian, and Nikita Nikolaienko, "Inside a Ukrainian Vampire Drone Squad's Mission to the Front Lines," *Wall Street Journal*, May 10, 2024.

Lucas, Clifford, "The Drone Dilemma and the US Air Force," War on the Rocks, May 7, 2024.

Macchiavelli, Marco, Navin Girishankar, and Matthew S. Borman, "Do Export Controls Erode the United States' Lead—or Protect It?" Center for Strategic and International Studies, Back and Forth 5, August 13, 2025.

Martin, Tim, "France Begins Delivery of 100 Loitering Munitions to Ukraine," Breaking Defense, November 5, 2024.

McLaughlin, Eliott C., Joe Sterling, and Stefano Pozzebon, "Venezuela Says It Has ID'd Mastermind, Accomplices in Apparent Maduro Assassination Try," CNN, August 7, 2018.

Metz, Cade, "Curbs on A.I. Exports? Silicon Valley Fears Losing Its Edge," *New York Times*, January 1, 2019.

Mozur, Paul, and Adam Satariano, "A.I. Begins Ushering in an Age of Killer Robots," *New York Times*, July 2, 2024.

National Counterintelligence and Security Center, Office of the Director of National Intelligence, "Five Eyes Intelligence Oversight and Review Council (FIORC)," webpage, undated. As of November 15, 2025: https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc

National Institute of Standards and Technology, *Autonomy Levels for Unmanned Systems (ALFUS) Framework*: Vol. II, *Framework Models*, Version 1.0, Special Publication 1011-II-1.0, December 2007.

National Urban Security Technology Laboratory, Science and Technology Directorate, U.S. Department of Homeland Security, *Counter–Unmanned Aircraft Systems: Technology Guide*, CUAS-T-G-1, September 2019.

OFAC—*See* Office of Foreign Assets Control.

Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce, "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)," press release, October 7, 2022.

Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce, "Commerce Strengthens Restrictions on Advanced Computing Semiconductors, Semiconductor Manufacturing Equipment, and Supercomputing Items to Countries of Concern," press release, October 17, 2023a.

Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce, "Commerce Adds 42 Entities to the Entity List for Supporting Russia's Military, Including Co-Production of Drones with Iran," press release, December 6, 2023b.

Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce, "Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Chip-Related Export Controls," press release, May 13, 2025.

Office of Foreign Assets Control, U.S. Department of the Treasury, "Guidance to Industry on Iran's UAV-Related Activities," undated.

Office of Foreign Assets Control, U.S. Department of the Treasury, "Specially Designated Nationals (SDNs) and the SDN List," released June 2, 2021.

Ossa, Ralph, "Trade Wars and Trade Talks with Data," *American Economic Review*, Vol. 104, No. 12, December 2014.

Page, Jeremy, and Paul Sonne, "China Seizes Market for Military Drones: U.S. Allies in Mideast and Africa That Can't Buy American Turn to Beijing," *Wall Street Journal*, July 18, 2017.

Pierson, David, "China Bans Rare Mineral Exports to the U.S.," *New York Times*, December 3, 2024.

Probasco, Emelia, "The Future of Drones in Ukraine: A Report from the DIU-Brave1 Warsaw Conference," Center for Security and Emerging Technology, November 13, 2023.

Public Law 90-629, Arms Export Control Act, October 22, 1968.

Public Law 96-72, Export Administration Act of 1979, September 29, 1979.

Public Law 106-178, Iran Nonproliferation Act of 2000, March 14, 2000.

Public Law 109-353, North Korea Nonproliferation Act of 2006, October 13, 2006.

Public Law 112-239, National Defense Authorization Act for Fiscal Year 2013, January 2, 2013.

Public Law 115-44, Countering America's Adversaries Through Sanctions Act, August 2, 2017.

Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, August 13, 2018.

Rajagopalan, Rajeswari Pillai, "AI Chips for China Face Additional US Restrictions," *The Diplomat*, April 5, 2024.

Reinsch, William A., Emily Benson, Thibault Denamiel, and Margot Putnam, *Optimizing Export Controls for Critical and Emerging Technologies*, Center for Strategic and International Studies, May 2023.

Reinsch, William Alan, Matthew Schleich, and Thibault Denamiel, "Insight into the U.S. Semiconductor Export Controls Update," *Critical Questions*, Center for Strategic and International Studies, October 20, 2023.

Ross, Philip E., "Budget Drones in Ukraine Are Redefining Warfare: Smart, Low-Cost Tech Enables New Military Tactics," *IEEE Spectrum*, May 17, 2023.

Savov, Vlad, and Debby Wu, "Tencent Stockpiled Nvidia AI Chips for 'a Couple of Generations,'" Bloomberg, November 15, 2023.

Schmid, Jon, David Luckey, Erik E. Mueller, Clay Strickland, Thomas Goode, Hiwot Demelash, Will Shumate, Aleksandr Esparza Hartunian, Kyle Brady, Karlyn D. Stanley, and Paul Cormarie, *Fielding Artificial Intelligence During Conflict: Lessons from Ukraine's Deployment of Artificial Intelligence in the Russia–Ukraine War*, RR-A3453-1, forthcoming.

Semiconductor Watch, "Navigating the Impact of U.S. Export Restrictions on Nvidia: The Middle East Factor," press release, August 31, 2023.

Shivakumar, Sujai, Charles Wessner, and Thomas Howell, "A Seismic Shift: The New U.S. Semiconductor Export Controls and the Implications for U.S. Firms, Allies, and the Innovation Ecosystem," Center for Strategic and International Studies, November 14, 2022.

Shivakumar, Sujai, Charles Wessner, and Thomas Howell, "Balancing the Ledger: Export Controls on U.S. Chip Technology to China," Center for Strategic and International Studies, February 21, 2024.

Shivakumar, Sujai, Charles Wessner, and Hideki Tomoshige, "Toward a New Multilateral Export Control Regime," commentary, Center for Strategic and International Studies, January 10, 2023.

Soldak, Katya, "Russia's War on Ukraine: Daily News and Information from Ukraine," *Forbes*, January 27, 2023.

Sonenshine, Tara, "Military Drones Are Swarming the Skies of Ukraine and Other Conflict Hot Spots—and Anything Goes When It Comes to International Law," The Conversation, May 19, 2023.

Starr, Barbara, and Katie Bo Lillis, "US Trying to Speed Up Delivery of Key Air Defense Systems to Ukraine After Russia's Iranian-Supplied Drone Attacks," CNN, October 17, 2022.

Swanson, Ana, "Trump Officials Battle over Plan to Keep Technology Out of Chinese Hands," *New York Times*, October 23, 2019.

Trump, Donald J., "Executive Order 13949 of September 21, 2020: Blocking Property of Certain Persons with Respect to the Conventional Arms Activities of Iran," *Federal Register*, Vol. 85, No. 185, September 23, 2020.

Trump, Donald J., "America First Investment Policy," memorandum for the Secretaries of the Treasury, Defense, Commerce, Labor, Energy, and Homeland Security; U.S. Attorney General; administrator of the U.S. Environmental Protection Agency; directors of the Office of Management and Budget, National Intelligence, the Office of Science and Technology Policy, and the Federal Bureau of Investigation; the U.S. Trade Representative; the chair of the Council of Economic Advisers; and the assistant to the President for national security affairs, White House, February 21, 2025.

Turkel, Nury, "AI, National Security, and the Global Technology Race: How US Export Controls Define the Future of Innovation," policy memo, Hudson Institute, March 24, 2025.

UN Security Council—*See* United Nations Security Council.

United Nations Security Council, Resolution 2231 (2015), S/RES/2231 (2015), July 20, 2015.

U.S. Code, Title 22, Foreign Relations and Intercourse; Chapter 39, Arms Export Control.

U.S. Department of Commerce, "President Biden's Fiscal Year 2025 Budget Would Strengthen Commerce Department's Mission to Boost American Innovation and Competitiveness," press release, March 11, 2024.

U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2023: Annual Report to Congress*, circa 2023.

U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress*, 2024.

U.S. Department of Defense, "DOD Releases List of Chinese Military Companies in Accordance with Section 1260H of the National Defense Authorization Act for Fiscal Year 2021," press release, January 7, 2025.

U.S.–EU Trade and Technology Council—*See* U.S.–European Union Trade and Technology Council.

U.S.–European Union Trade and Technology Council, "TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management," December 1, 2022.

Vallance, Chris, "Chinese Drone Firm DJI Pauses Operations in Russia and Ukraine," BBC, April 27, 2022.

Vincent, Brandi, "'Stark Reminders': Experts Assess How Military Tech Must Adapt After Deadly Drone Attack on US Troops," DefenseScoop, February 2, 2024.

Volpicelli, Gian, Veronika Melkozerova, and Laura Kayali, "'Our Oppenheimer Moment'—in Ukraine, the Robot Wars Have Already Begun," Politico, May 16, 2024.

WA—*See* Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

WA Secretariat—*See* Wassenaar Arrangement Secretariat.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, "About Us," webpage, undated. As of March 4, 2025: https://www.wassenaar.org/about-us/

Wassenaar Arrangement Secretariat, *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public Documents*: Vol. II, *List of Dual-Use Goods and Technologies and Munitions List*, 2023.

WB Group, "WARMATE Loitering Munitions," webpage, undated. As of March 4, 2025: https://www.wbgroup.pl/en/produkt/warmate-loitering-munnitions/

White House, "President Donald J. Trump Declares National Emergency to Increase Our Competitive Edge, Protect Our Sovereignty, and Strengthen Our National and Economic Security," fact sheet, April 2, 2025.

Wilson, Bradley, Shane Tierney, Brendan Toland, Rachel M. Burns, Colby Peyton Steiner, Christopher Scott Adams, Michael Nixon, Raza Khan, Michelle D. Ziegler, Jan Osburg, and Ike Chang, *Small Unmanned Aerial System Adversary Capabilities*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-3023-DHS, 2020. As of July 25, 2025: https://www.rand.org/pubs/research_reports/RR3023.html

World Trade Organization, "World Trade Report 2024: Trade and Inclusiveness—How to Make Trade Work for All," webpage, 2024. As of January 5, 2025: https://www.wto.org/english/res_e/publications_e/wtr24_e.htm

Zelalem, Zecharias, "Deadly Skies: Drone Warfare in Ethiopia and the Future of Conflict in Africa," policy brief, European Council on Foreign Relations, February 28, 2025.

NATIONAL DEFENSE RESEARCH INSTITUTE

China and the United States are developing technology for both artificial intelligence (AI) and unmanned aircraft systems (UASs). Both countries will be able to fill the demand in other countries for these systems. AI and UAS technologies, particularly those with dual uses, are advancing with increasing speed, but export controls lag. This deficiency in regulations can stifle appropriate national security, industry autonomy—and thus technological advances—and coordinated integration of the two technologies. In this report, authors review current export control systems for AI and UASs, examine their effectiveness, and consider how the United States could form a balanced system of export controls for AI and UASs. The report focuses on dual-use technologies. It covers the Export Administration Regulations, the International Traffic in Arms Regulations, and the interagency process.

For this report, the authors examined the current and potential future states of export control regulations on AI and UAS technologies; analyzed how current regulations are effective, inadequate, or even detrimental; and assessed how insights on AI and UAS export controls might be applicable to creating a system of export controls for AI and UASs that balances competition with China and securely guided proliferation of AI and UAS technologies.

www.rand.org

RR-A3296-1