WHACK-A-DRONE: EXAMINING THE EFFECTIVENESS OF U.S. EXPORT CONTROLS ON SEMICONDUCTORS AND OTHER COMPONENTS USED IN THE PRODUCTION OF UNMANNED AERIAL VEHICLES

OLIVIA KAEMPF*

* J.D. Candidate, American University Washington College of Law (2025); B.A. International Business, San Diego State University (2022). My sincerest thanks go to Meggie Weiler, Kirsten Companik, and the entire *Administrative Law Review* staff for their immense support and valuable contributions to this piece. I would also like to express my gratitude to my family, who have always been my biggest supporters. This Comment is dedicated to all those whose lives are impacted by the devastations of armed conflict.

INTRODUCTION

The use of drone warfare is taking center stage in armed conflict due to recent innovations in drone technology.[1] The Russian war in Ukraine,[2] one of the most significant and well-documented international armed conflicts of the twenty-first century,[3] marks the highest number of airborne drones (known as unmanned aerial vehicles, or UAVs) that have ever been used in a military confrontation.[4] Ukraine alone is estimated to use (and lose) an

---

1. STACIE PETTYJOHN, CTR. FOR A NEW AM. SEC., EVOLUTION NOT REVOLUTION: DRONE WARFARE IN RUSSIA'S 2022 INVASION OF UKRAINE 2 (2024), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Defense-Ukraine-Drones-Final.pdf [https://perma.cc/9HPT-DA3Z] ("The accessibility and affordability of drones is creating new capabilities at a scale that previously did not exist and transforming the battlefield.").

2. This Comment primarily focuses on developments in the war since Russia's invasion of Ukraine on February 24, 2022. However, these recent developments should be viewed in the broader context of the conflict, which dates back to Russia's invasion and illegal annexation of Crimea in 2014. G.A. Res. 68/262, Territorial Integrity of Ukraine (Mar. 27, 2014); Press Release, U.N. General Assembly, General Assembly Adopts Resolution Calling Upon States Not to Recognize Changes in Status of Crimea Region (Mar. 27, 2014), https://press.un.org/en/2014/ga11493.doc.htm [https://perma.cc/8SDB-ENGL] (affirming the international community's "commitment to Ukraine's sovereignty"); U.S. Dep't of State, Bureau of Democracy, H.R. & Lab., Ukraine 2021 Human Rights Report 73 (2021) ("The United States does not recognize the attempted annexation of Crimea by the Russian Federation."). *But see* Juergen Bering, *The Prohibition on Annexation: Lessons From Crimea*, 49 N.Y.U. J. INT'L L. & POL. 747, 780 (2017) (noting a small group of "disreputable states" whose position differs from the vast majority of the world) (quoting Ryan Goodman, *How "Overwhelming" was the U.N. General Assembly Vote on Crimea?*, JUST SEC. (Apr. 24, 2014), https://www.justsecurity.org/9809/overwhelming-general-assembly-vote-crimea/[https://perma.cc/93C4-FZP6]). *See generally How Russia's Grab of Crimea 10 Years Ago Led to War with Ukraine and Rising Tensions With the West*, AP NEWS (Mar. 18, 2024, 2:53 PM), https://apnews.com/article/russia-putin-ukraine-crimea-seizure-8245aec572fb71236febfa8735c42879 [https://perma.cc/E277-9BC2] (providing a high-level overview of the conflict in the years since the annexation of Crimea).

3. Greg Myre, *From Drone Videos to Selfies at the Front, Ukraine is the Most Documented War Ever*, NPR (Aug. 2, 2023 10:41 AM), https://www.npr.org/2023/08/02/1191557426/ukraine-war-news-coverage [https://perma.cc/RW3D-DRCV] (noting that the rise in social media and accessibility to global news is a large contributor to the "overload of information").

4. Cédric Pietralunga, *Russia and Ukraine Take Drone Warfare to Unprecedented Scale*, LE MONDE (June 18, 2023, 3:00 AM), https://www.lemonde.fr/en/international/article/2023/06/18/russia-and-ukraine-take-drone-warfare-to-unprecedented-scale_6033281_4.html [https://perma.cc/2DC4-JCRC]; *see also* Ulrike Franke, *Drones in Ukraine and Beyond,*

unprecedented 300 UAVs per day.[5] The rise in the use of UAVs in armed conflict is due to both the advancement in aerial defense systems, which have largely neutralized manned aviation, and the cost-effectiveness and relative energy efficiency of UAVs themselves.[6] UAVs serve a myriad of functions in military operations, including conducting reconnaissance missions, carrying out precision strikes within enemy territory, and covertly monitoring adversaries' movements.[7] A unique use for UAVs has been the documentation of conflict itself; in the Russian war in Ukraine, UAVs have documented the destruction of Ukrainian cities and infrastructure.[8]

In response to the recent outbreak of conflict in Ukraine in February 2022, the United States and other countries imposed sanctions and export controls on Russia, sometimes as part of a collaborative effort.[9] Where sanctions involve the withdrawal of customary trade and financial relations with another state—including the imposition of arms embargoes or asset freezes—export controls directly regulate the export, re-export, and transfer of certain

---

Everything You Need to Know, EUR. COUNCIL ON FOREIGN RELS. (Aug. 11, 2023), https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/ [https://perma.cc/W8LE-R9WG] (describing the uses of unmanned aerial vehicles (UAVs) in conflict and their role in the Russian war in Ukraine).

5. Pietralunga, *supra* note 4; *see also* Jack Watling & Nick Reynolds, *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*, ROYAL UNITED SERVS. INST. (May 19, 2023), https://rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine [https://perma.cc/W8RR-UWLU] ("Ukrainian UAV losses remain at approximately 10,000 per month.").

6. John Dyson, *How Semiconductors Are Enhancing National Security Advantage*, KARVE INT'L (Nov. 21, 2023), https://www.karveinternational.com/insights/how-semiconductors-are-enhancing-national-security-advantage [https://perma.cc/GM82-3CSE] (noting drones' cost-effectiveness, in both procurement and operational costs, when compared to manned aircraft); *see, e.g.*, EDWARD G. KEATING, JOHN KERMAN & DAVID ARTHUR, CONG. BUDGET OFF., 57090, USAGE PATTERNS AND COSTS OF UNMANNED AERIAL SYSTEMS 8 (2021) (identifying 17% and 38% decreases in life-cycle costs and recurring costs, respectively, when compared to one type of manned aircraft).

7. Kristen D. Thompson, *How the Drone War in Ukraine Is Transforming Conflict*, COUNCIL ON FOREIGN RELS. (Jan 16, 2024, 2:12 PM), https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict [https://perma.cc/Z8UV-YMYP]; Franke, *supra* note 4.

8. Franke, *supra* note 4.

9. *See, e.g.*, *Common High Priority List*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM. (Feb. 23, 2024) [hereinafter *Common High Priority List*], https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items [https://perma.cc/TPF3-8QV6] (identifying fifty "common high priority items" sought by Russia for its weapons programs, collaboratively identified by the U.S. Department of Commerce's Bureau of Industry and Security (BIS), the European Union, Japan, and the United Kingdom).

items.[10] "Items" refers collectively to software, technology, and commodities (any articles, materials, or supplies other than software and technology).[11] In addition to regulating particular items based on their technical characteristics, export controls may also be based on the intended end-user, the country of destination, or the intended end-use of the items concerned.[12] Because of the significant rise in the use of drone warfare, export controls aimed at Russian entities have focused on semiconductors and other microelectronics used in the production of UAVs.[13]

Semiconductors—also referred to as integrated circuits or microchips (colloquially, chips)—are conductive materials used in the fabrication of electronic devices.[14] Microelectronics, the broad term covering different types of semiconductor devices and integrated circuits, are used in every major industry in the world and are often called the "'DNA' of technology" because of their importance across industries.[15] They are found in medical devices, broadband technology, mobile phones, solar panels, and military technology.[16] For a reference of how prolific the use of semiconductors is across industries, simply consider the vast impact that the 2020–2021 global chip shortage had on supply chains around the world.[17] Semiconductors, specifically graphics processor units (GPUs), are also used extensively to train

10. Jonathan Masters, *What Are Economic Sanctions?*, COUNCIL ON FOREIGN RELS. (June 24, 2024, 10:40 AM), https://www.cfr.org/backgrounder/what-are-economic-sanctions [https://perma.cc/Q7SX-7FSX].

11. Export Administration Regulations, 15 C.F.R. § 772.1 (2024).

12. *U.S. Export Controls*, INT'L TRADE ASS'N, U.S. DEP'T OF COM., https://www.trade.gov/us-export-controls [https://perma.cc/E82Y-5JSF] (last visited Nov. 11, 2024).

13. Steven Feldstein & Fiona Brauer, *Why Russia Has Been So Resilient to Western Export Controls*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Mar. 11, 2024), https://carnegieendowment.org/research/2024/03/why-russia-has-been-so-resilient-to-western-export-controls?lang=en [https://perma.cc/8KFL-E4BM].

14. *What is a Semiconductor?*, SEMICONDUCTOR INDUS. ASS'N, https://www.semiconductors.org/semiconductors-101/what-is-a-semiconductor/ [https://perma.cc/U6G9-82ZA] (last visited Nov. 11, 2024).

15. BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., ASSESSMENT OF THE STATUS OF THE MICROELECTRONICS INDUSTRIAL BASE IN THE UNITED STATES 10 (2023) [hereinafter MICROELECTRONICS INDUSTRIAL BASE REPORT], https://www.bis.doc.gov/index.php/documents/technology-evaluation/3402-section-9904-report-final-20231221/file [https://perma.cc/7NPV-S2WB].

16. *Id.* at 11.

17. *See, e.g.*, Daniel Howley, *These 169 Industries are Being Hit by the Global Chip Shortage*, YAHOO FIN. (Apr. 25, 2021), https://finance.yahoo.com/news/these-industries-are-hit-hardest-by-the-global-chip-shortage-122854251.html [https://perma.cc/7RR4-L2N9].

advanced artificial intelligence (AI) models because of GPUs' capacity for parallel information processing.[18] Parallel processing capability, whereby multiple pieces of information can be processed simultaneously, is a significant advancement over semiconductors used in earlier AI models, which only possessed the capacity to process a single piece of information at once.[19] The U.S. semiconductor industry invests very heavily in the research and development of GPUs and other high-performance chips used in the development of AI models.[20] This investment has positioned the United States as a global leader in the field, subsequently raising concerns about protecting intellectual property surrounding the development and design of semiconductor technology in the United States.[21] These concerns also stem from the mass migration of the semiconductor manufacturing industry to East Asia, which currently houses approximately three-quarters of global semiconductor manufacturing capacity.[22] The United States, which once boasted a 37% share of global semiconductor manufacturing, now only retains 13%.[23] Given the fierce competition between the United States and China to design and develop AI technology, it is no surprise that both the U.S. government and the U.S. semiconductor industry want to further restrict foreign adversaries' access to U.S.-origin technology and goods.[24]

On the other hand, industry actors are concerned that more stringent export controls may hinder the dominance of U.S. fabricators and designers on the global market.[25] Developers and manufacturers worry that over-control

---

18. LAURIE A. HARRIS, CONG. RSCH. SERV., IF12497, SEMICONDUCTORS AND ARTIFICIAL INTELLIGENCE 1 (2023).

19. *See id.*

20. MICROELECTRONICS INDUSTRIAL BASE REPORT, *supra* note 15, at 5; *see also* HARRIS, *supra* note 18, at 2.

21. MICROELECTRONICS INDUSTRIAL BASE REPORT, *supra* note 15, at 5.

22. André Brunel, *A Proposal for a Semiconductor Export Control Treaty*, 19 J. BUS. & TECH. L. 1, 4 (2023); Jiyoung Sohn, *The U.S. Is Investing Big in Chips. So Is the Rest of the World.*, WALL ST. J. (July 31, 2022, 5:30 AM), https://www.wsj.com/articles/the-u-s-is-investing-big-in-chips-so-is-the-rest-of-the-world-11659259807 [https://perma.cc/N3VM-5N38].

23. Brunel, *supra* note 22, at 4–5.

24. Alexis Keenan, *The AI Arms Race Between the US and China is Heating Up*, YAHOO FIN. (Mar. 11, 2024, 4:11 AM), https://finance.yahoo.com/news/the-ai-arms-race-between-the-us-and-china-is-heating-up-160000539.html [https://perma.cc/H9M5-JRWD] (describing the "horse race" for global artificial intelligence (AI) supremacy and noting that the United States and China are first and second, respectively, in AI investment, innovation, and implementation).

25. *See, e.g.*, Robert D. Atkinson, *Stronger Semiconductor Export Controls on China Will Likely Harm Allied Semiconductor Competitiveness*, INFO. TECH. & INNOVATION FOUND. (Oct. 12, 2023),

of U.S.-origin semiconductors places the U.S. industry at a global disadvantage, as foreign buyers may seek their supply elsewhere to avoid the risk of facing export control violations.[26] In fact, U.S. industry survey respondents "identified foreign competition as their third greatest organizational challenge, . . . with the highest share of respondents listing foreign competition as their single greatest organizational challenge."[27] From a national security standpoint, the loss of U.S. leadership in the global semiconductor industry could also negatively affect U.S. military superiority.[28] Falling behind in the "horse race" for AI technology and microelectronics development would give military adversaries access to more advanced weapons systems.[29] The federal agencies charged with export control creation and enforcement have the difficult task of balancing U.S. foreign policy and national security objectives that restrict adversaries' access to these items with the interests of the domestic industry in protecting the United States' global market superiority.

This Comment explores the existing regime of U.S. export controls against Russia and other military adversaries regarding weapons components developed and manufactured in the United States, focusing primarily on semiconductors and other microelectronics used in the production of UAVs. The current system makes exporting, re-exporting, and transferring of any U.S.-origin item designated by the U.S. Department of Commerce to Russia as an end destination unlawful without an export license.[30] However, the proliferation of re-exports through third countries and shell companies to hide unlawful end-users or end destinations has made enforcing U.S. export controls extremely difficult.[31]

---

https://itif.org/publications/2023/10/12/stronger-semiconductor-export-controls-on-china-will-likely-harm-allied-semiconductor-competitiveness/ [https://perma.cc/8FDX-3QAU]; *SIA Statement on New Export Controls*, SEMICONDUCTOR INDUS. ASS'N (Oct. 17, 2023, 9:00 AM), https://www.semiconductors.org/sia-statement-on-new-export-controls-2/ [https://perma.cc/362N-T7GZ] ("Overly broad, unilateral controls risk harming the U.S. semiconductor ecosystem, . . . as they encourage overseas customers to look elsewhere.").

26. *See* Natasha Bertrand, *Exclusive: Biden Task Force Investigating How US Tech Ends Up in Iranian Attack Drones Used Against Ukraine*, CNN [hereinafter Bertrand, *Biden Task Force*], https://www.cnn.com/2022/12/21/politics/iranian-drones-russia-biden-task-force-us-tech-ukraine/index.html [https://perma.cc/U962-B2V4] (Dec. 21, 2022, 2:27 PM).

27. MICROELECTRONICS INDUSTRIAL BASE REPORT, *supra* note 15, at 4.

28. NAT'L SEC. COMM'N ON A.I., AD1124333, FINAL REPORT 214 (2021) ("If a potential adversary bests the United States in semiconductors over the long term . . . it could gain the upper hand in every domain of warfare.").

29. *See* Keenan, *supra* note 24.

30. *See infra* note 67 and accompanying text.

31. *See, e.g.*, Press Release, U.S. Dep't of Justice, Iranian National Charged with

Part I explains the current system of export controls, particularly within the Commerce Department, and how its enforcement measures have fallen short in light of the sheer number of schemes to evade controls. Part II provides a background of U.S. foreign policy concerning Russia and the Commerce Department's growing focus on semiconductors and other dual-use weapons components. Part III examines the opportunities for interagency cooperation, particularly through the Emerging Technology Technical Advisory Committee (Advisory Committee) and with the U.S. Intelligence Community (IC), addressing their roles in advising the Bureau of Industry and Security (BIS) about new dual-use technologies and efforts to circumvent U.S. export controls thereof. Part IV recommends that BIS direct the Advisory Committee to coordinate with the Director of National Intelligence (DNI) to identify U.S.-origin UAV components found in Russian drones and release further guidance to the industry regarding how U.S. companies themselves can more effectively monitor their own supply chains for compliance. Specifically, BIS should work with both industry actors and the IC to identify these unlawful actors, encourage domestic and foreign industries to adopt more advanced traceability technology for their microelectronics, and direct the Advisory Committee to work with the DNI to identify UAV components escaping the net of U.S. export controls.

I. BACKGROUND

A. The U.S. Export Controls System and Multilateral Regimes

The three primary agencies that administer export controls in the United States are the Department of State's Directorate of Defense Trade Controls (DDTC) (defense articles and defense services), the Department of the Treasury's Office of Foreign Assets Control (OFAC) (economic sanctions-related controls), and the Commerce Department's BIS (dual-use items).[32] Dual-use items have both commercial and military applications.[33] Many of the components used in the production of UAVs, including microelectronics, are

Unlawfully Procuring Microelectronics Used in Unmanned Aerial Vehicles on Behalf of the Iranian Government (Dec. 19, 2023), https://www.justice.gov/opa/pr/iranian-national-charged-unlawfully-procuring-microelectronics-used-unmanned-aerial-vehicles [https://perma.cc/4ZQF-X5FE].

32. David Noah, *A Summary of Government Agencies that Regulate U.S. Exports*, SHIPPING SOLS.: INT'L TRADE BLOG (Jan. 18, 2023), https://www.shippingsolutions.com/blog/government-agencies-that-regulate-us-exports [https://perma.cc/2MHB-YK6H].

33. *Dual Use Export Licenses*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.doc.gov/index.php/all-articles/2-uncategorized/91-dual-use-export-licenses [https://perma.cc/KU5S-KQDH] (last visited Nov. 11, 2024).

classified as dual-use items because of their varied commercial and military applications,[34] so BIS monitors their export by way of the Export Administration Regulations (EAR) rather than DDTC or OFAC.[35]

Export controls primarily serve to promote U.S. national security and foreign policy interests, and items are controlled for a multitude of reasons, both multilateral and unilateral.[36] Multilateral reasons for control are based on the multilateral export control regimes in which the United States participates.[37] These reasons include national security, missile technology, chemical and biological weapons, and nuclear proliferation.[38] Unilateral controls are those that the United States chooses to impose according to its own foreign policy objectives, outside of its responsibilities under the regimes.[39] These objectives include regional stability, crime control, and antiterrorism.[40] For example, because of their use in weapons development, most semiconductors and other integrated circuits are controlled for national security and regional stability reasons.[41] Some sub-categories of semiconductors are also controlled for missile technology, nuclear proliferation, and antiterrorism reasons.[42] A national security designation means that the items are controlled in alignment with the United States' policy of restricting the export, re-export, and transfer of items that "would make a significant contribution

34. See *supra* notes 15–16 and accompanying text for an explanation of semiconductors as a dual-use item.

35. *See About Export Administration Regulations (EAR)*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.gov/regulations [https://perma.cc/SEB4-JLKK] (last visited Nov. 11, 2024) (supporting that BIS oversees the Export Administration Regulations (EAR), which regulates dual-use items, while the Directorate of Defense Trade Controls and the Department of the Treasury's Office of Foreign Assets Control monitor items that do not fall under the EAR).

36. *See Multilateral Export Control Regimes*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM. [hereinafter *Multilateral Export Control Regimes*], https://www.bis.doc.gov/index.php/policy-guidance/multilateral-export-control-regimes [https://perma.cc/EQ3Y-XKSD] (last visited Nov. 11, 2024).

37. *See id.*; *see infra* text accompanying notes 47–55 (describing the multilateral export control regimes the United States participates in).

38. Export Administration Regulations, 15 C.F.R. §§ 742.2–.5 (2024).

39. *See Multilateral Export Control Regimes*, *supra* note 36; Export Control Reform Act of 2018, 50 U.S.C. § 4811(4)–(6) (differentiating U.S. policy regarding multilateral and unilateral controls).

40. 15 C.F.R. §§ 742.6–.8.

41. *See id.* § 774, Supp. No. 1 (noting reasons for control for items designated by the Export Control Classification Number (ECCN) 3A001, which includes most semiconductors). See *infra* text accompanying notes 65–76 for a discussion of ECCNs and their organization within the Commerce Control List (CCL).

42. 15 C.F.R. § 774, Supp. No. 1.

to the military potential of any other country or combination of countries that would prove detrimental to the national security of the United States."[43] Included in U.S. policy around export controls is an aim to "preserve the qualitative military superiority of the United States."[44] This policy is particularly important when export controls concern the United States' primary military adversaries, like Russia, China, and Iran, especially as China and Iran are known to be supplying Russia with military equipment in support of the war in Ukraine.[45] A regional stability designation denotes the United States' foreign policy objective to control the export of items that may contribute to the "destabilization of the region to which the items are destined."[46]

---

43. *Id.* § 742.4(a).

44. Export Control Reform Act of 2018, 50 U.S.C. § 4811(2).

45. *See, e.g.*, U.S. DEP'T OF COM., U.S. DEP'T OF JUST., U.S. DEP'T OF STATE & U.S. DEP'T OF TREASURY, GUIDANCE TO INDUSTRY ON IRAN'S UAV-RELATED ACTIVITIES 1 (June 9, 2023) [hereinafter IRAN'S UAV-RELATED ACTIVITIES] ("Since at least late August 2022, Iran has transferred hundreds of Shahed- and Mohajer-series UAVs to Russia."); Jeff Mason & Steve Holland, *Russia Received Hundreds of Iranian Drones to Attack Ukraine, US Says*, REUTERS (June 9, 2023, 8:51 PM), https://www.reuters.com/world/europe/russia-has-received-hundreds-iranian-drones-attack-ukraine-white-house-2023-06-09/ [https://perma.cc/FUT6-R8NY] (reporting White House statements that Iran is supplying UAVs themselves and the materials needed to build a drone manufacturing plant in Russia); Karen Gilchrist, *How Surging Trade with China is Boosting Russia's War*, CNBC, https://www.cnbc.com/2023/09/28/how-surging-trade-with-china-is-boosting-russias-war.html [https://perma.cc/D2XZ-R6XC] (Jan. 25, 2024, 8:58 AM) (reporting China's increase in support for Russia through the trade of "goods for use on the battlefield" and other commercial goods that are "providing direct and indirect support to Russia's war efforts"); Jacob Fromer, *Special Report: Russia Buying Civilian Drones from China for War Effort*, NIKKEI ASIA (July 1, 2023, 5:59 PM), https://asia.nikkei.com/Politics/Ukraine-war/Special-report-Russia-buying-civilian-drones-from-China-for-war-effort [https://perma.cc/4PMP-78AB] ("Between December 2022 and April 2023, Russian companies imported at least 37 Chinese unmanned aerial vehicles worth around $103,000 that were designated in customs clearance records as being 'for use in the special military operation . . . .'").

46. BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., 2018 REPORT ON FOREIGN POLICY-BASED EXPORT CONTROLS 15 (2018). Note also that BIS recently amended the EAR to include the foreign policy interest of protecting human rights as a basis for establishing export controls. Amendment To Confirm Basis for Adding Certain Entities to the Entity List Includes Foreign Policy Interest of Protection of Human Rights Worldwide, 88 Fed. Reg. 18,983, 18,983 (Mar. 30, 2023) (to be codified at 15 C.F.R. pt. 744). The use of drone warfare by Russia (and others) to commit human rights abuses supports the regulation of semiconductors and microelectronics on a foreign policy basis, which includes the regional stability designation. *See, e.g.*, Fionnuala Ní Aoláin (Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism), THE USE OF ARMED

Outside of the domestic export controls regime, the United States participates in four major multilateral export control regimes: the Australia Group (biological and chemical weapons), Missile Technology Control Regime (missiles and related technology), the Zanger Committee and Nuclear Suppliers Group (nuclear material), and the Wassenaar Arrangement (conventional arms and dual-use goods and technologies).[47] Multilateral regimes are significant in that they allow for the coordination of export controls among member governments.[48] As dual-use items, semiconductors and microelectronics fall under the jurisdiction of the Wassenaar Arrangement.[49] The Wassenaar Arrangement is not a binding treaty but a voluntary system by which member states agree upon a list of items to be controlled.[50] Its purpose is to "contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of . . . dual-use goods and technologies . . . ."[51] Because the arrangement is not self-executing, member governments have a responsibility to implement such controls in their own domestic regimes.[52] Unfortunately, as a purely voluntary system, the Wassenaar Arrangement suffers from a lack of adequate enforcement measures.[53] Member states have no ability to force other members to comply with the requirements of the Wassenaar Arrangement, and any one state can veto a proposal for additions to the list of controlled items.[54] There have been calls for the drafting of a new "Wassenaar Treaty," which would

---

DRONES IN THE CONTEXT OF COUNTER-TERRORISM 4 (Feb. 2022), https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/activities/20230103-Position-Paper-Use-Armed-Drones.pdf [https://perma.cc/4G8A-R26R] ("The use of armed drones worldwide . . . poses an ongoing risk to civilians and a challenge to human rights protection.").

47. *Export Controls Policy*, BUREAU OF INT'L SEC. & NONPROLIFERATION, U.S. DEP'T OF STATE, https://www.state.gov/nonproliferation-export-controls [https://perma.cc/3QW2-3TSL] (last visited Nov. 11, 2024).

48. *Multilateral Export Control Regimes*, *supra* note 36.

49. *About Us*, THE WASSENAAR ARRANGEMENT: ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES [hereinafter *About Wassenaar*], https://www.wassenaar.org/about-us/#about-us [https://perma.cc/7RQ3-H4YT] (Dec. 1, 2023).

50. *See id.*; *Multilateral Export Control Regimes*, *supra* note 36.

51. *About Wassenaar*, *supra* note 49.

52. *Multilateral Export Control Regimes*, *supra* note 36; *see also* Brunel, *supra* note 22, at 9.

53. Sujai Shivakumar, Charles Wessner & Hideki Tomoshige, *Toward a New Multilateral Export Control Regime*, CTR. FOR STRATEGIC & INT'L STUD. (Jan. 10, 2023), https://www.csis.org/analysis/toward-new-multilateral-export-control-regime [https://perma.cc/5AHV-XEEG].

54. *Id.*

be both binding and self-executing (meaning that no further implementation through domestic legislation would be required).[55] But until a binding mechanism like this can be agreed upon, the burden of compliance continues to rest on individual member states' voluntary implementation of the agreed-upon controls.

Outside the formal multilateral regimes, smaller groups of allied states have made additional agreements regarding export controls and guidance to both domestic industry and enforcement authorities.[56] For example, the United States, the European Union, Japan, and the United Kingdom collaboratively identified fifty "high priority items" that Russia seeks to procure for its weapons programs.[57] While the items identified (which includes an array of integrated circuits) are generally already subject to controls in these countries, the competent authorities in each state published the list to "highlight for industry that [the] items pose a heightened risk of being diverted illegally to Russia . . . ."[58] Notifying the industry about the items of concern may "support due diligence and effective compliance by exporters" and allow for "targeted anti-circumvention actions by customs and enforcement agencies . . . ."[59] The United States is particularly concerned about situations where such procurement would run contrary to the United States's national security and foreign policy objectives of limiting adversaries' military advancement and protecting human rights worldwide.[60]

B. The Commerce Department's Bureau of Industry and Security

The Export Control Reform Act of 2018 (ECRA) authorizes the Commerce Department to regulate the export, re-export, and transfer of U.S.-origin dual-use items.[61] The ECRA includes a specific mandate to maintain lists of controlled items, prohibited end-uses, and prohibited end-users.[62] It

55. Brunel, *supra* note 22, at 9.

56. *See, e.g.*, *Common High Priority List*, *supra* note 9.

57. *Id.*

58. *Id.*

59. *List of Common High Priority Items*, FIN. SERVS. & CAP. MKTS. UNION, DIRECTORATE-GENERAL FOR FINANCIAL STABILITY, https://finance.ec.europa.eu/document/download/5a2494db-d874-4e2b-bf2a-ec5a191d2dc0_en? [https://perma.cc/QHE3-9CNP] (Feb. 22, 2024).

60. *Id.*; *see* Export Control Reform Act of 2018, 50 U.S.C. § 4811(2); Amendment to Confirm Basis for Adding Certain Entities to the Entity List Includes Foreign Policy Interest of Protection of Human Rights Worldwide, 88 Fed. Reg. 18,983, 18,984–85 (Mar. 30, 2023) (to be codified at 15 C.F.R. pt. 744).

61. 50 U.S.C. §§ 4801–52.

62. *Id.* § 4813(a).

also directs the Commerce Department to establish licensing requirements and processes.[63] The Commerce Department implements this authority through BIS's administration of the EAR.[64] Within the EAR, BIS maintains the Commerce Control List (CCL), a list of many items controlled under the EAR and subject to heightened export license requirements.[65] Based on evolving national security and foreign policy concerns, BIS periodically adds items to the CCL through its formal rulemaking process and accepts public comments from the affected industries on proposed additions and classifications.[66] Currently, the export of any item on the CCL to Russia or neighboring Belarus requires an export license, which is granted through an application to BIS.[67] Items that are controlled under the EAR have an Export Control Classification Number (ECCN), an alpha-numeric code that describes the item, denotes the reason for its control (e.g., multilateral or unilateral), and indicates where it may be found on the CCL.[68] For example, most semiconductors are listed on the CCL under the ECCN 3A001, which spans nearly nine pages of the *Code of Federal Regulations* and describes the controls on many types of semiconductors.[69] Within the ECCN, "3" indicates the category of items within the CCL (Electronics).[70] "A" indicates the product group (end items, equipment, accessories, attachments, parts, components, and systems).[71] Additionally, "00" indicates the primary reason(s) for control (national security).[72] The final digit, "1," is used to organize within the CCL items of the same general type.[73] Some items fall under the Commerce Department's jurisdiction but are not included on the CCL—including low-technology consumer goods—so the CCL is not an exhaustive

63. *Id.*

64. Export Administration Regulations, 15 C.F.R. §§ 730–74 (2024).

65. *Id.* § 774, Supp. No. 1.

66. *See, e.g.*, Implementation of Additional Export Controls: Certain Advanced Computing Items, 88 Fed. Reg. 73,458 (Oct. 25, 2023) (to be codified at 15 C.F.R. pts. 732, 734, 736, 740, 742, 744, 764, 748, 758, 770, 772, 774) (interim final rule) (creating new ECCNs for certain classes of advanced computing items, including integrated circuits).

67. *Resources On Export Controls Implemented in Response to Russia's Invasion of Ukraine*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/russia-belarus [https://perma.cc/9BLU-NKE6] (Feb. 23, 2024).

68. *Commerce Control List (CCL)*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM. [hereinafter *Commerce Control List*], https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl [https://perma.cc/S3F2-KHBF] (last visited Nov. 11, 2024).

69. *See* Export Administration Regulations, 15 C.F.R. § 774, Supp. No. 1 (2024).

70. *Id.* § 738.2.

71. *Id.*

72. *Id.*

73. *Id.*

list of regulated items.[74] Generally, such goods are only subject to license requirements if they are headed for a destination or end-user of concern.[75] Items that are subject to the EAR but do not appear on the CCL are designated as EAR99.[76]

The designated reason (or reasons) for control indicated on the CCL affect license requirements based on the destination country, as each designation will reference a particular country group listed on the Commerce Country Chart or Country Groups List.[77] Once an exporter determines that an item is subject to controls for a particular reason, the Commerce Country Chart will inform them which destination countries would trigger an export license requirement for that item.[78] Alternatively, the Commerce Country Chart can also inform the exporter that the item is eligible for export No License Required.[79] This would mean the transaction can go through without requiring the exporter to apply for an export license through BIS.[80] If the item is subject to a license requirement, the exporter will refer to the Country Groups List to determine whether a license exception applies.[81]

Focusing on the two primary reasons for control of semiconductors (national security and regional stability), the Commerce Country Chart reveals that exports of these items require export licenses when destined for Russia, China, and Iran.[82] Iran is subject to the "special controls" described in § 746.7 of the EAR, but the effect is the same: items on the CCL with national security and regional stability designations require a license.[83] Moving to the Country Groups List, all three countries are placed in Country Group D, the second-most restrictive Country Group in terms of the license exceptions allowed.[84] Finally, referring back to § 740 of the EAR on license exceptions, exceptions are not permitted for semiconductors being exported, re-

74. *See generally Commerce Control List*, *supra* note 68.

75. *See id.*

76. *Id.*

77. *See* Export Administration Regulations, 15 C.F.R. § 738, Supp. No. 1 (2024) (Commerce Country Chart); *id.* § 740, Supp. No. 1 (Country Groups List); *see supra* text accompanying notes 36–46 (discussing multilateral and unilateral reasons for control).

78. See 15 C.F.R. § 738, Supp. No. 1.

79. *See id.* § 738.4.

80. *See id.*

81. *See id.* § 740, Supp. No. 1. See, for example, *id.* §§ 740.1–.22 for a comprehensive list of license exceptions.

82. 15 C.F.R. § 774, Supp. No. 1.

83. *Id.* § 746.7(a)(1)(i).

84. *Id.* § 740, Supp. No. 1. Country Group D is second in restrictiveness only to Country Group E, which includes four countries under general embargo, all of which appear in both Group D and Group E. *Id.*

exported, or transferred to or within countries listed on Country Group D.[85] Therefore, even disregarding BIS's more recently promulgated rule imposing "highly restrictive license requirements on all categories of items on the [CCL] to Russia and Belarus," other regulations already stringently control many UAV components when they are destined for countries that pose national security concerns.[86]

Apart from the CCL, BIS also maintains the Entity List within the EAR, a comprehensive list of entities to whom exports are subject to heightened license requirements.[87] BIS identifies entities for the Entity List "for which there is reasonable cause to believe, based on specific and articulable facts, that the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States."[88] Once BIS identifies a qualifying entity, representatives from multiple federal agencies vote as part of the End-User Review Committee to approve additions to the Entity List.[89] These additions, like amendments to the CCL, are promulgated through BIS's rulemaking process.[90] BIS has added over 900 entities to the Entity List in connection with Russia's invasion of Ukraine, including entities within Russia itself and in other countries found to be involved in the unlawful transshipment of Western goods to Russia.[91]

---

85. *Id.* § 740.2(a)(9)(ii).

86. Press Release, Bureau of Indus. & Sec., U.S. Dep't of Com., Commerce Department Expands Restrictions on Exports to Russia and Belarus in Response to Ongoing Aggression in Ukraine (Apr. 9, 2022), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2954-2022-04-09-press-release-bis-expands-restrictions-on-exports-to-russia-and-belarus/file [https://perma.cc/4GG9-M7PZ]. *See generally* Expansion of Sanctions Against Russia and Belarus Under the Export Administration Regulations (EAR), 87 Fed. Reg. 22,130, 22,130 (Apr. 8, 2022) (to be codified at 15 C.F.R. pts. 734, 738, 746) (final rule) (imposing license requirements to all items on the CCL when destined to Russia and Belarus).

87. *See* 15 C.F.R. §§ 744, Supp. No. 4, 744.16(a) (2024).

88. Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Entity List Modification, 87 Fed. Reg. 62,186, 62,191 (Oct. 13, 2023) (to be codified at 15 C.F.R. pts. 734, 736, 740, 742, 744, 762, 772, 774).

89. 15 C.F.R § 744, Supp. No. 5; *see also* Additions of Entities to the Entity List, 88 Fed. Reg. 85,095, 85,095–96 (Dec. 7, 2023) (to be codified at 15 C.F.R. pt. 744).

90. *See, e.g.*, Addition of Entities to and Revision of Entry on the Entity List, 89 Fed. Reg. 25,503 (Apr. 11, 2024) (to be codified at 15 C.F.R. pt. 744) (adding eleven entries to the Entity List for their actions contrary to the national security or foreign policy interests of the United States).

91. Press Release, Bureau of Indus. & Sec., U.S. Dep't of Com., Commerce Stands

Exporters themselves have a duty to exercise due diligence in ensuring that no entities in their supply chain evade U.S. export controls.[92] This duty includes an obligation to identify and evaluate any red flags within the company's supply chain, including any abnormal transaction circumstances.[93] Examples of red flags include inconsistencies between the specifications of the item and the needs of the purchaser, the purchaser's reluctance to offer information about the end-use of the item, or an incompatibility with the destination country's technical level (e.g., in a transaction for semiconductor manufacturing equipment, the destination country has no electronics industry).[94] The exporter is required to obtain and document certain information about the transaction and report it to BIS, and while companies are allowed to rely on representations from customers, they are obligated to take additional verification steps if any red flags arise.[95]

Penalties for violations of the EAR can be severe; willful violations carry criminal penalties of up to $1 million in fines or up to twenty years imprisonment for individuals.[96] In contrast, civil fines of up to twice the value of the transaction are imposed regardless of intent.[97] BIS itself may also impose administrative penalties at the advice of the Administrative Case Review

---

Strong with Ukraine, Takes Further Action Against Ongoing Russian Aggression (Feb. 23, 2024), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3452-2024-02-23-bis-press-release-russia-two-year-actions/file [https://perma.cc/RV9K-GCR9]; *see also* Press Release, Bureau of Indus. & Sec., U.S. Dep't of Com., Russia Export Controls Communique (Feb. 2024), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3450-2024-02-22-bis-communique-russia-export-controls/file [https://perma.cc/SP34-UZ8Z] (stating that "over 200 companies located in third countries outside Russia have now been added to the. . . . Entity List" for their involvement in the transshipment of Western items to Russia).

92. *Know Your Customer Guidance*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM. [hereinafter *Know Your Customer Guidance*], https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/47-know-your-customer-guidance [https://perma.cc/R4QT-R4WA] (last visited Nov. 11, 2024).

93. *Id.* ("[W]hen 'Red Flags' are raised in the information that comes to [a] firm, [it has] a duty to exercise due diligence to inquire regarding the suspicious circumstances and ensure appropriate end-use, end-user, or ultimate country of destination in the transactions [it proposes] to engage in.").

94. *Red Flag Indicators*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/51-red-flag-indicators [https://perma.cc/PL2W-7SKR] (last visited Nov. 11, 2024) (outlining a nonexhaustive list of potential red flags).

95. *Know Your Customer Guidance*, *supra* note 92.

96. 50 U.S.C. § 1705(c).

97. *Id.* § 1705(b).

Board, levying additional fines and denying export privileges.[98] The denial of export privileges may take the form of a Temporary Denial Order (TDO) issued by the Assistant Secretary for Export Enforcement within BIS, which denies "any or (typically) all of the export privileges of a company or individual to prevent an imminent or ongoing export control violation," including both the right to export goods from the United States and the right to receive U.S.-origin exported goods.[99] While TDOs are in effect for a renewable 180-day period, Section 1760(e) denials, which are issued when a person is convicted of "certain criminal violations," can last up to ten years.[100]

BIS's Office of Export Enforcement undertakes various prevention and compliance measures, including the performance of end-use checks, which verify the identities of the parties to the transaction and "seek to ensure the recipients of the exported items are or will be using the items as authorized" and in accordance with license conditions.[101] End-use checks are performed by Export Enforcement officers stationed at U.S. embassies worldwide and take place both preshipment (when either sensitive items or unreliable parties may be involved) and post-shipment (so as to monitor transactions to their conclusion).[102] In 2021, 26% of BIS end-use checks resulted in follow-up actions like license denials, Entity List designations, or referrals for further investigation of the end-user.[103] This figure demonstrates the effectiveness of end-use checks across the globe in enforcing U.S. national security and foreign policy.

II. FOCUSING EXPORT CONTROLS ON RUSSIA IN SUPPORT OF U.S. NATIONAL SECURITY AND FOREIGN POLICY OBJECTIVES

A. The Emergence of Semiconductors and Other Dual-Use Weapons Components as an Area of Concern for Export Controls

In 2021, President Biden declared a national emergency to deal with the "harmful foreign activities" of the Russian Federation.[104] Later, following

98. *Penalties*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.doc.gov/index.php/enforcement/oee/penalties [https://perma.cc/5RT5-WNU6] (last visited Nov. 11, 2024).

99. *Id.*

100. *Id.*

101. BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., ANNUAL REPORT TO CONGRESS 45 (2021), https://www.bis.doc.gov/index.php/documents/pdfs/3140-annual-report-of-the-bureau-of-industry-and-security-for-fiscal-year-2021/file [https://perma.cc/NHH8-QXKA].

102. *Id.* at 45–46.

103. *Id.* at 46.

104. Exec. Order No. 14,024, 86 Fed. Reg. 20,249, 20,249 (Apr. 15, 2021).

the February 2022 Russian invasion of Ukraine, President Biden prohibited the export and re-export from the United States or by a United States person, wherever located, of "any . . . items as may be determined by the Secretary of Commerce . . . to any person located in the Russian Federation."[105] Most recently, President Biden acknowledged the Russian Federation's "reliance on the international financial system for the procurement of dual-use and other critical items from third countries."[106] He subsequently empowered the Secretary of the Treasury to impose sanctions on financial institutions that are found to have conducted or facilitated any transactions with the Russian military-industrial base or for any person found to have operated in the technology, defense materiel, or other industries that support the Russian military-industrial base.[107] Though this order deals solely with sanctions, it is important to highlight the Biden Administration's prioritization of the reduction of Russian access to restricted dual-use items.[108]

Since the outbreak of the war in Ukraine, multiple groups have conducted studies of retrieved Russian UAVs, finding that a shockingly high number of U.S.-origin and other Western components are present despite the comprehensive system of export controls in place to stop Russia from gaining access to such materials.[109] The United Kingdom-based Royal United Services Institute (RUSI) acquired twenty-seven weapons systems and other pieces of equipment, including ballistic missiles and a variety of UAVs.[110] After examining the recovered items, "RUSI identified 450 unique components primarily sourced from Western manufacturers," including several subsets of microelectronics.[111] At least 318 of these components came from the United

105. Exec. Order No. 14,068, 87 Fed. Reg. 14,381, 14,381 (Mar. 11, 2022). This order empowered the Secretary of Commerce (along with the Secretaries of State and the Treasury) to "take such actions . . . as may be necessary to carry out the purposes of this order." *Id.* at 14,382.

106. Exec. Order No. 14,114, 88 Fed. Reg. 89,271, 89,271 (Dec. 22, 2023).

107. *Id.*

108. *See id.*

109. *See, e.g.*, JAMES BYRNE, GARY SOMERVILLE, JOE BYRNE, JACK WATLING, NICK REYNOLDS & JANE BAKER, SILICON LIFELINE: WESTERN ELECTRONICS AT THE HEART OF RUSSIA'S WAR MACHINE 5, 7–9, 12–16 (2022), https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf [https://perma.cc/MU7Y-JNCS]; *Dissecting Iranian Drones Employed by Russia in Ukraine*, CONFLICT ARMAMENT RSCH. (Nov. 2022) [hereinafter CAR REPORT], https://storymaps.arcgis.com/stories/7a394153c87947d8a602c3927609f572 [https://perma.cc/MY6Q-MBQ3].

110. Byrne et al., *supra* note 109, at 11.

111. *Id.* at 12. Several of the components found across different pieces of equipment were the same, meaning that the total number of American- and Western-origin components recovered was much higher than 450. *Id.*

States, the majority originating from fifty-seven U.S.-based companies, the most prevalent being leading microelectronics manufacturers.[112] Most of the components had serial numbers that could be traced back to the manufacturer, which allowed for the identification of the companies of origin.[113] In a similar study, Conflict Armament Research (CAR) found that in four Russian UAVs recovered in November 2022, 82% of the components were manufactured by U.S.-based companies.[114] CAR also found that many of these components were recently manufactured, with 56% manufactured in 2020 and 2021.[115]

Recognizing the issue, in 2022, the Biden Administration launched a task force headed by the White House National Security Council to investigate how U.S.- and Western-origin components are ending up in Iranian-made UAVs that Russia is using in the war in Ukraine.[116] This "all hands on deck" initiative involves all three cabinet departments responsible for export controls enforcement, as well as the Department of Justice and the Department of Defense.[117] One of the task force's first actions was to "notify all of the American companies whose components have been found in the drones."[118] It also coordinates with foreign allies whose components were also found in recovered Russian UAVs.[119] However, prior efforts to prevent more components from falling through the cracks proved extremely difficult.[120] Tracing these components through supply chains is nearly impossible because semiconductors and other microelectronics are so heavily commoditized, a problem exacerbated by the fact that the industry relies heavily on third-party distributors and resellers.[121] Some have criticized the failure of U.S. companies to monitor their own supply chains and called for U.S. authorities to crack down harder on enforcement.[122] But the truth is that oftentimes Western companies are not knowingly committing or aiding in export control violations; it often happens so far down a chain of re-exports that the original U.S. exporter remains unaware of any unlawful activity.[123] Unfortunately, the task force itself has not had any success in solving the problem;

112. *Id.* at 12–13.
113. *Id.* at 14.
114. CAR REPORT, *supra* note 109, at 4.
115. *Id.* at 4–5.
116. Bertrand, *Biden Task Force*, *supra* note 26.
117. *Id.*
118. *Id.*
119. *Id.*
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.*

no substantive updates as to its progress have been released, and it has faced criticism of its ineffectiveness at carrying out its mission.[124]

B. The Re-Export Problem

The ECRA defines re-export as "the shipment or transmission of [an] item from a foreign country to another foreign country, including the sending or taking of the item from the foreign country to the other foreign country, in any manner . . . ."[125] Essentially, re-export occurs when an item is exported a second (or third, fourth, and so on) time from the original importer to a third country.[126] This is distinct from in-country transfer, which is "a change in the end-use or end user of the item within the same foreign country."[127] Under the EAR, U.S. export controls continue to apply to re-exported U.S.-origin items.[128] This means that if an export license would be required to export the item from the United States directly to the third country, then a license would also be required to re-export the U.S.-origin item from the original importer to the third country.[129]

Though existing export controls are largely effective at eliminating exports of semiconductors and other microelectronics directly to Russian, Iranian, or Chinese entities, end-users who are seeking access to these goods have come up with a different strategy: creating chains of shell companies to act as lawful importers in order to make transactions look legitimate and evade U.S. export controls.[130] U.S. enforcement authorities identified some of

---

124. *E.g.*, Letter from Ted Cruz, Ranking Member, U.S. S. Comm. on Com., Sci., and Transp., to Jake Sullivan, Assistant to the President and Nat'l Sec. Advisor (July 22, 2024), https://www.commerce.senate.gov/services/files/900F9CC6-FA4B-4E3E-949D-8723CBBB99B2 [https://perma.cc/86M8-AGLF] (requesting specific information about the Task Force's activities and criticizing its failure to fulfill its mission).

125. Export Control Reform Act of 2018, 50 U.S.C. § 4801(9).

126. *See id.*

127. *Id.* § 4801(6).

128. Export Administration Regulations, 15 C.F.R. § 734.3(a)(2) (2024).

129. *Id.* § 734.3(a)(2); *see also Guidance on Reexports/Transfers (in-country) of U.S.-Origin Items or Non-U.S.-made Items Subject to the Export Administration Regulations (EAR)*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions [https://perma.cc/5WCU-SSYR] (Oct. 30, 2015) ("If the item is a U.S.-origin item and subject to the EAR, it remains subject to the EAR regardless of how many times it is reexported, transferred, or sold.").

130. Natasha Bertrand, *CNN Exclusive: A Single Iranian Attack Drone Found to Contain Parts From More Than A Dozen US Companies*, CNN (Jan. 4, 2023, 1:51 PM) [hereinafter Bertrand, *Iranian Attack Drone*], https://www.cnn.com/2023/01/04/politics/iranian-drone-parts-13-us-companies-ukraine-russia/index.html [https://perma.cc/FGY8-UYYS] ("[I]t is far easier for

these shell companies, resulting both in criminal penalties and additions to the Entity List.[131] This prohibits the shell companies from engaging in future transactions involving controlled items, but new ones appear at a much higher rate than they can be identified and penalized.[132] Because it is easier and less time-consuming for unlawful end-users to create and obscure new shell companies than it is to identify them, BIS ends up playing a proverbial game of whack-a-mole against a slew of middlemen.[133]

III. OPPORTUNITIES FOR INTERAGENCY COOPERATION

A. The Role of Technical Advisory Committees

There are six Technical Advisory Committees (TACs) that "advise the [Commerce Department] on the technical parameters for export controls applicable to dual-use commodities and technology and on the administration of those controls."[134] Each TAC is composed of industry representatives, chosen from a broad range of firms that produce goods, technologies, and software currently subject to U.S. export controls, along with

---

Russian and Iranian officials to set up shell companies to use to purchase the equipment and evade sanctions than it is for Western governments to uncover those front companies, which can sometimes take years . . . ."); Bertrand, *Biden Task Force*, *supra* note 26 ("[N]eutering some Iranian front companies . . . will be akin to 'a game of whack a mole,' . . . they 'can easily find another supplier.'").

131. *See, e.g.*, Press Release, U.S. Dep't of Justice, Iranian National Charged with Unlawfully Procuring Microelectronics Used in Unmanned Aerial Vehicles on Behalf of the Iranian Government (Dec. 19, 2023), https://www.justice.gov/opa/pr/iranian-national-charged-unlawfully-procuring-microelectronics-used-unmanned-aerial-vehicles [https://perma.cc/W2ZC-U5UR] ("[C]o-conspirators crafted a sophisticated web of front companies to obscure the illicit acquisition of American and foreign technology to procure components for deadly UAVs . . . . These very components have been found in use by Iran's allies in current conflicts, including in Ukraine.").

132. *Id.*; Gregory C. Allen, Emily Benson & William Alan Reinsch, *Improved Export Controls Enforcement Technology Needed for U.S. National Security*, CTR. FOR STRATEGIC & INT'L STUD. 1, 11 (Nov. 2022), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/221130_Allen_Export_Controls.pdf [https://perma.cc/WM3V-3DG5].

133. *See* Bertrand, *Iranian Attack Drone*, *supra* note 130; Allen et al., *supra* note 132, at 11.

134. *Technical Advisory Committees (TAC)*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM. [hereinafter *Technical Advisory Committees*], https://tac.bis.doc.gov [https://perma.cc/YAU3-PMW3] (last visited Nov. 11, 2024). The Technical Advisory Committees (TACs) include: the Emerging Technology Technical Advisory Committee, Information Systems Technical Advisory Committee, Materials and Equipment Advisory Committee, Regulations and Procedures Technical Advisory Committee, Sensors and Instrumentation Advisory Committee, and Transportation and Related Equipment Advisory Committee. *Id.*

government representatives.[135] Members are appointed by the Secretary of Commerce and are required to hold a Secret-level security clearance so that they have access to relevant classified information while formulating recommendations to the Commerce Department.[136]

The Advisory Committee is directly overseen by BIS and is specifically charged with the "identification of emerging and foundational technologies . . . with potential dual-use applications," a subset of technologies that the Commerce Department is directed to control by § 1758 of the ECRA.[137] The Advisory Committee then reports trends of particular interest to BIS to improve enforcement of export controls concerning such technologies.[138] In identifying goods that fall under the "emerging and foundational" designation, BIS does not distinguish between "emerging" and "foundational," but rather refers to these technologies as "Section 1758 technologies," identifying that they are "essential to the national security of the United States."[139] BIS controls § 1758 technologies because of their potential use in creating weapons of mass destruction, committing human rights violations, and posing threats to the national security of both the United States and the rest of the world.[140] Once a § 1758 technology is identified and assessed by interagency groups and TACs, BIS publishes the control either as a notice of inquiry or an advance notice of proposed rulemaking in order to receive feedback, and the item is addressed within the multilateral export control regimes for

135. *Technical Advisory Committees*, *supra* note 134.

136. *Id.*

137. EMERGING TECH. TECH. ADVISORY COMM.: CHARTER, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., 1 (2020) [hereinafter CHARTER], https://tac.bis.doc.gov/index.php/documents/pdfs/279-ettac-charter/file [https://perma.cc/52P5-85Y8] (providing objectives and scope of activities); Export Control Reform Act of 2018, 50 U.S.C. § 4817 (directing the Secretary of Commerce to "establish appropriate controls under the [EAR] on the export, reexport, or in-country transfer" of "emerging and foundational technologies that []are essential to the national security of the United States").

138. CHARTER, *supra* note 137, at 1.

139. Commerce Control List: Controls on Certain Marine Toxins, 87 Fed. Reg. 31,195, 31,195–96 (May 23, 2022) (to be codified at 15 C.F.R. pts. 740, 742, 744) (detailing the semantic difficulties in drawing a meaningful distinction between "emerging" and "foundational," and officially coining the term "Section 1758 technologies"); 50 U.S.C. § 4817(a)(1).

140. Tongele N. Tongele, Michael Tu, Betty Lee, John Varesi & Wesley Johnson, Bureau of Indus. & Sec., U.S. Dep't of Com., Update Conference on Export Controls & Policy: Building A Network of Global Cooperation 6–7 (2022) [hereinafter Building A Network of Global Cooperation], https://www.bis.doc.gov/index.php/documents/2022-update-conference/3073-rev3-emerging-tech-update-2022-section-1758-controls-tongele/file [https://perma.cc/8JCJ-Y84R].

discussion.[141] For the control to be fully put into force, the ECCN is then published in the *Federal Register*, providing the applicable parameters and explaining the reasons for the control.[142]

In establishing export controls regarding these technologies, BIS must consider the degree to which they have already been developed in foreign countries, the effect that export controls may have on their development in the United States, and the potential effectiveness of export controls in limiting their proliferation in foreign countries.[143] Comprised of representatives from U.S. industry, the members of the Advisory Committee are uniquely placed to evaluate the potential impact of such controls on domestic industry and to solicit further input from industry representatives who are not themselves full-fledged members of the Advisory Committee.

In 2018, BIS published a list of fourteen representative general categories of technologies that would fall under § 1758, which is meant to serve as a dynamic guide for identifying new Section 1758 technologies rather than as an exhaustive list of technologies to be controlled.[144] Agencies other than the Commerce Department have also worked to identify emerging technologies that pose a risk to U.S. national security.[145] A common feature of these lists of emerging technologies is the inclusion of semiconductors and microelectronics.[146] It is, therefore, within the Advisory Committee's ability to advise BIS on export controls specifically concerning semiconductors and to consult with other federal agencies and industry representatives to formulate recommendations.

B. The Intelligence Community

The DNI is a Cabinet-level executive official who serves as the head of the IC and directs the National Intelligence Program.[147] They establish

141. *See id.* at 21.

142. *Id.*

143. 50 U.S.C. § 4817(a)(2)(B).

144. Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201, 58,202 (Nov. 19, 2018) (to be codified at 15 C.F.R. pt. 744); *see* Building A Network of Global Cooperation, *supra* note 140, at 20.

145. *See, e.g.*, FAST TRACK ACTION SUBCOMM. ON CRITICAL & EMERGING TECHS., EXEC. OFF. OF THE PRESIDENT, CRITICAL AND EMERGING TECHNOLOGIES LIST UPDATE (2022), https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf [https://perma.cc/5BMQ-8BET] (identifying "critical and emerging technologies").

146. *See id.*; Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201, 58,202 (Nov. 19, 2018) (to be codified at 15 C.F.R. pt. 744).

147. *Who We Are*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/who-we-are [https://perma.cc/8AHY-4TUS] (last visited Nov. 11, 2024).

"objectives, priorities, and guidance for the [IC] to ensure timely and effective collection . . . and dissemination . . . of national intelligence."[148] This includes the responsibility of ensuring that national intelligence, "based upon all sources available to the [IC]," is provided "to the heads of departments and agencies of the executive branch."[149] The DNI is charged with maximizing the availability of intelligence information within the IC, which includes any elements within agencies designated to be an "element of the [IC]."[150] Within the Commerce Department, the Office of Intelligence serves as the liaison between the Department and the IC and provides necessary intelligence information to Department leadership in support of the Department's policy objectives.[151] Through the Office of Intelligence, BIS can receive intelligence tailored to its need to combat export control evasion.[152]

Under the purview of the DNI, the IC releases an Annual Threat Assessment of the U.S. Intelligence Community (Threat Assessment), which reports on "worldwide threats to the national security of the United States" based on the "collective insights of the [IC]."[153] The 2024 Threat Assessment addressed both country-specific concerns surrounding Russia, China, and Iran, as well as thematic concerns about the proliferation of emerging technologies.[154] Among the activities covered are China's support of Russia's defense industrial base by providing dual-use weapons components, Iran's growing UAV capabilities, and military adversaries' use of emerging technologies in the field of AI to create advancements in weapons systems.[155] The IC is clearly focused on the proliferation of advanced UAVs used in opposition to U.S. foreign policy and national security objectives.[156] The DNI is, therefore, well placed to provide information that would assist BIS in controlling U.S.-origin UAV components.[157] The DNI, whether through its own

148. 50 U.S.C. § 3024(f)(1)(A)(i) (tasking and other authorities).

149. 50 U.S.C. § 3024(a) (provision of intelligence).

150. 50 U.S.C. §§ 3024(a), (g); 50 U.S.C. § 3003(4) (definition of "intelligence community").

151. *Office of Intelligence*, U.S. DEP'T OF COM., https://www.commerce.gov/bureaus-and-offices/os/cfo-asa/intelligence [https://perma.cc/N65P-BXXE] (last visited Nov. 11, 2024).

152. *Id.*

153. OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 3 (2024), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf [https://perma.cc/UH6N-EYRU].

154. *See id.* at 7, 14, 18, 30.

155. *Id.* at 8, 19, 30.

156. *See id.* (highlighting concerns within the intelligence community that U.S. adversaries will continue to rapidly develop "asymmetric threats" such as UAVs that threaten the United States and its allies).

157. *See, e.g.*, 50 U.S.C. § 3024(a).

powers or through coordination with foreign governments, has the authority to gather and analyze intelligence on the types of components that are evading U.S. export controls and ending up in the hands of unlawful end-users; and if they have not done so already, they should.[158]

IV. RECOMMENDATIONS

BIS should use existing fora, namely the Advisory Committee, to strengthen coordination efforts with the IC, identify U.S.-origin UAV components that evade export controls enforcement, and release more specific guidance to the U.S. microelectronics industry on effective traceability measures for their products. When reviewing license applications, the Commerce Department is already directed to consider information "provided by the [DNI] regarding any threat to the national security of the United States" that may be caused by a proposed export, re-export, or transfer of items related to emerging technologies.[159] BIS should specifically and continuously seek out information from the DNI—via the Office of Intelligence—related to components found in UAVs that are known (or suspected) to originate in the United States or an allied country.[160] BIS, via the Advisory Committee, should also recommend to the DNI that they direct the IC to perform studies similar to the RUSI and CAR examinations of recovered UAVs if they are not doing so already.[161] With this information, the Advisory Committee can tailor its recommendations to BIS regarding the types of items that are most often the subject of export control violations and give advice on BIS's own guidance that it releases to U.S. industry.

BIS, in turn, should give further guidance to U.S. companies whose goods have been found in Russian UAVs on how to monitor their own supply chains more strictly through in-depth verification measures for importers who raise red flags. Though the Departments of Commerce, Justice, State, and the Treasury have already advised exporters, manufacturers, and distributors of semiconductors and microelectronics to "establish multiple methods to track such items," they failed to offer any concrete suggestions on what these methods should be.[162] BIS should first advise industry actors to form an internal system of recording the serial numbers of the goods that they export, including which entities they exported certain "batches" to. If UAV components are traced back to a particular U.S. company, the

158. *Id.* §§ 3024(f), (k) (authority for collecting and analyzing intelligence and coordinating with foreign governments).

159. Export Control Reform Act of 2018, 50 U.S.C. §§ 4817(a)(2)(A)(ii), (b)(3)(B).

160. *See supra* notes 150–152 and accompanying text.

161. *See supra* notes 109–115 and accompanying text.

162. IRAN'S UAV-RELATED ACTIVITIES, *supra* note 45, at 3.

company itself can then more effectively identify which entities within its own supply chain committed or aided in the violation. In the event that serial numbers become unreadable due to attempts by unlawful end-users to obscure the origin of the items (as has happened by lasering off serial numbers), companies should be advised on other methods of tracking.[163]

Traceability measures other than serial numbers are used within the semiconductor manufacturing industry to track individual chips down the assembly line and through the supply chain, primarily to measure compliance with technical specifications and to identify errors in production.[164] Companies that provide traceability services to semiconductor manufacturers offer solutions that are both easy to implement into existing assembly lines and ideal for tracing items long-term.[165] One such company offers laser markers that can fit minuscule (a few thousandths of an inch) but detailed barcodes onto components, producing a high-resolution and weatherable mark that, when scanned, produces key identification information about the item.[166] Because these marks are so small, they would be more difficult for unlawful end-users (who may seek to remove or destroy identifying information) to find than a typical serial number. Industry actors can likely adapt the purpose of this traceability technology to further ensure compliance with export controls.[167] If components are recovered and cannot be identified by a regular serial number, this type of technology would provide another, possibly more durable and reliable, method for identifying the origin of these components and their path down the supply chain. Many manufacturers may already be using this kind of technology to optimize their production, so the additional

163. *Id.* at 3 (noting the "prevalence of methods used to obscure the sources of components found in Iranian UAVs, such as the lasering off of serial numbers and other identifying information.").

164. *See Harnessing the Power of Traceability in the Electronics Manufacturing and Semiconductor Industries: Three Trends, Three Challenges, and Numerous Technological Solutions*, OMRON 2 (Sept. 2018), https://assets.omron.com/m/55b80b2276c2aa60/original/Omron_Digi_Semi_Traceability_Whitepaper_2018_EN_201809_U66IE01-1-.pdf [https://perma.cc/E9XM-PMSV] ("Data-driven traceability systems . . . play a key role in internal processes that help with quality monitoring, production optimization and security.").

165. *See id.* at 7.

166. *Id.* at 4, 7.

167. *See* Hardy Schmidbauer, *How to Balance Regulating Semiconductors with Global Security and Technological Progress*, WORLD ECON. F. (Jan. 11, 2024), https://www.weforum.org/agenda/2024/01/balance-regulating-semiconductors-global-security-technological-progress/ [https://perma.cc/FHD5-ZUKT] (explaining that tamper-resistant traceability measures would "enable stringent security controls, verifying ownership, origin[,] and authenticity and allowing devices to be revoked or flagged if used unexpectedly.").

cost to companies would be minimal.[168] Even if manufacturers are not already taking advantage of advanced traceability solutions, their dual use in streamlining the production process and monitoring the supply chain for export controls compliance would likely motivate companies to adopt them. Beyond existing serial numbers and more advanced traceability technology, seeking to define other options for the suggested "multiple methods" of tracking is another opportunity to take advantage of the role of the Advisory Committee.[169] BIS should seek input from industry actors who have experience in semiconductor manufacturing, using it as a forum to identify other tracking mechanisms that may be used.

Beyond simply suggesting that entities within the United States utilize this kind of technology, BIS should advise implementation at all levels of the supply chain, including when the items are exported outside the United States. Because non-U.S. companies that re-export or transfer U.S.-origin goods are still subject to U.S. export controls,[170] they would benefit from and likely be willing to implement further suggestions from the U.S. government. The Commerce Department, in partnership with the Departments of Justice and the Treasury, previously released guidance to foreign-based persons on how to comply with U.S. sanctions and export controls, so this would not be unfamiliar terrain for BIS.[171]

Companies should then be directed to report such entities to BIS, who can take further action by, for example, placing that entity on the Entity List, issuing a TDO, or investigating the entity's compliance further. This would enhance enforcement of controls in compliance with U.S. foreign policy and national security objectives without BIS having to place more stringent controls on U.S. companies or risk overenforcement, which would tend to negatively impact the United States' leading position in the global semiconductor market.[172]

---

168. *See id.* (noting that companies tend to view the relatively low-cost increase of security measures (2–5%) as a "reasonable compromise given the benefits").

169. *See* IRAN'S UAV-RELATED ACTIVITIES, *supra* note 45, at 3.

170. Export Administration Regulations, 15 § 734.3(a)(2) (2024) ("All U.S. origin items wherever located" are subject to the EAR).

171. *See, e.g.*, U.S. DEP'T OF COM., DEP'T OF THE TREASURY & DEP'T OF JUST., TRI-SEAL COMPLIANCE NOTE: OBLIGATIONS OF FOREIGN-BASED PERSONS TO COMPLY WITH U.S. SANCTIONS AND EXPORT CONTROL LAWS 1 (2024), https://www.justice.gov/opa/media/1341411/dl?inline [https://perma.cc/C8K7-KE8K] (providing "an overview of compliance considerations for non-U.S. companies and compliance measures to help mitigate their risk").

172. *See supra* notes 25–26, 36–46 and accompanying text.

CONCLUSION

The rise in the use of UAVs in armed conflict across the globe has pushed semiconductor and microelectronics technology to the forefront of the export controls field. The existing regime of controls, though comprehensive in theory, has lacked effectiveness because of the prevalence of re-exporting within an industry that relies so heavily on third-party resellers that identifying unlawful actors becomes nearly impossible. BIS should act by directing the Advisory Committee to work with the DNI and the U.S. semiconductor industry to further identify the source of items that end up in Iranian and Russian hands. BIS should also advise the U.S. industry to implement more stringent recordkeeping practices and traceability measures with regard to the semiconductors and microelectronics that are imported out of the United States so that manufacturers can monitor their own supply chains for export control evasion more effectively. Though BIS may not be able to eliminate evasion via re-export entirely, taking these measures would increase the rate at which BIS is able to identify and respond to export control violations in this area. In doing so, BIS can further U.S. foreign policy and national security objectives without unduly burdening the U.S. semiconductor industry with overly strict controls.