Issue 41

October 2020

Legal Gazette

Legal Aspects of Innovation

Contents

Publisher:
Monte DeBoer, ACT Legal Advisor

Editor-in-Chief:
Sherrod Lewis Bumgardner, ACT SEE Legal Advisor

Editors:
Mette Prassé Hartov, HQ SACT Deputy Legal Advisor
Galateia Gialitaki, ACT SEE Legal Assistant

Copy Editors:
Robert 'Butch'Bracknell, HQ SACT Staff Legal Advisor
Col Xavier Labarriere, HQ SACT Staff Legal Advisor
Miles S. Porter, HQ SACT Legal Extern
Malia Kenza Chenaoui, ACT SEE Legal Extern

Copy Proofreader:
Caitlin Fendon, HQ SACT Legal Intern
Lola Chanfreau, ACT SEE Legal Extern

Source: www.nato.int

U.S. Export Controls: The Future of Disruptive Technologies[1]

by Christopher Timura,[2] Judith Alison Lee,[3] R.L. Pratt[4] and Scott Toussaint[5]

Introduction

Export controls administered by the United States and other NATO

[1] The views expressed in this article are solely those of the authors and may not necessarily represent the agreed upon views of NATO, ACO, ACT or Gibson, Dunn & Crutcher LLP.

[2] Christopher Timura is an attorney in the Washington D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's International Trade Practice Group. Mr. Timura helps emerging technology clients across sectors solve regulatory, legal, and political problems that arise at the intersection of national security, trade, and foreign policy. He earned a Juris Doctor and a Ph.D. in Cultural Anthropology at the University of Michigan.

[3] Judith Alison Lee is a partner in the Washington, D.C. office of Gibson Dunn & Crutcher LLP and Co-Chair of the firm's International Trade Practice Group. Ms. Lee practices in the area of international trade regulation, including USA Patriot Act compliance, economic sanctions and embargoes, export controls, and national security reviews.

[4] R.L. Pratt is an associate in the Washington D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's International Trade Practice Group. Mr. Pratt counsels clients on compliance with U.S. economic sanctions, export controls, foreign investment, and international trade regulatory issues and assists in representing clients before the U.S. Departments of State, Treasury, and Commerce.

[5] Scott Toussaint is an associate in the Washington, D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's International Trade Practice Group. A former adviser to a member of the U.S. House of Representatives, his practice focuses on compliance with U.S. laws governing international business transactions, including economic sanctions, export controls, and foreign investment in the United States.

Member States restrict the sharing of sensitive goods, services and technology, with significant impacts on NATO's ability to develop and deploy on the battlefield emerging technologies like artificial intelligence-enabled and hypersonic defensive and offensive weapons systems. Indeed, recent export control legislation enacted by the United States—and implementing regulations that are currently being written—will play a major role in determining the NATO community's ability to field interoperable equipment and prevent hostile powers from dominating leading-edge research and development.

On August 13, 2018, President Trump signed into law the most sweeping changes to the U.S. export control regime in decades.[6] Among other things, the Export Control Reform Act of 2018 ("ECRA") modernises the United States' primary authority for export controls on dual-use items (items with both civil and military applications) by requiring the President for the first time to identify and establish both export and foreign investment controls on "emerging" and "foundational" technologies that are essential to national security. The U.S. Department of Commerce has now begun the process of drafting regulations to identify particular "emerging" and "foundational" technologies and to develop corresponding licensing requirements for transfers of these technologies with U.S. allies and adversaries. In addition to new export licensing requirements, any investments, including investments that do not result in foreign person control, in U.S. businesses working with the technologies identified will also be subject to foreign investment review and potential blocking by the Committee on Foreign Investment in the United States ("CFIUS").[7]

How the United States implements these new controls will significantly shape when, where and how disruptive dual-use technologies like artificial intelligence ("AI") and hypersonics ultimately develop.[8] Unilateral implementation of stringent controls on these important new technologies could restrict international cooperation on their development or use, even

[6] *See, e.g.*, Congressional Research Service, 'The U.S. Export Control System and the Export Control Reform Initiative' R41916, (Jan. 28, 2020) 2; Samuel Rubenfield, 'Law Formalizes Export Control Rules' *Wall Street Journal* (Aug. 17, 2018).

[7] CFIUS is an interagency committee authorized to review the national security implications of investments made by foreign companies and persons in U.S. businesses ("covered transactions"), and to block transactions or impose measures to mitigate any threats to U.S. national security.

[8] "Disruptive technology is an innovation that significantly alters the way that consumers, industries, or businesses operate. A disruptive technology sweeps away the systems or habits it replaces because it has attributes that are recognizably superior." Tim Smith, 'Disruptive Technology' *Investopedia* (Mar. 21, 2020).

among close U.S. allies. Application of these new authorities could, for example, hinder the interoperability of important military platforms even among the United States' NATO allies. There is some expectation that the U.S. Department of Commerce may make its efforts to control these technologies multilateral and collaborate with NATO Member States, among other U.S. allies, to impose uniform controls. But there is no guarantee that international agreement can be reached or that the United States will not "go it alone."[9] In fact, the United States has already shown some reluctance to offer favourable treatment for its NATO allies when applying both new and old international trade authorities under U.S. law.[10]

To help members of the NATO community better understand these coming developments, this article proceeds as follows. In Section I, we explain how U.S. export controls work and the policy rationale(s) behind them. In Section II, we provide a high-level overview of recent legislative changes to the U.S. export control regime, and explain the rulemaking process, currently underway, through which the United States will develop controls on so-called "emerging" and "foundational" technologies. In Section III, we describe the various factors, such as whether innovation of a particular technology is centralized or diffuse, that will affect how impactful these new controls are likely to be. Finally, in Section IV, we conclude by illustrating how U.S. export controls are likely to impact two areas of emerging technologies—hypersonics and artificial intelligence—the successful development and deployment of which will likely be critical to NATO's future military capabilities.

I. Background: U.S. Export Controls Explained

As a policy matter, U.S. export controls attempt to balance the needs to protect U.S. national security, support American industry and technological superiority, and permit coordination and exchange with U.S. allies. These controls are rooted in multilateral cooperation that allows for the supply of dual-use goods to allied nations and keeps these items and their underlying technology out of the hands of U.S. adversaries. The Wassenaar Arrangement[11]—the multilateral agreement that underlies much of the Export

[9] *See, e.g.*, Modification of License Exception Additional Permissive Reexports (APR), 85 Fed. Reg. 23,496 (Apr. 28, 2020).
[10] *See, e.g.*, Provisions Pertaining to Certain Investment in the United States by Foreign Persons, 84 Fed. Reg. 50,174, 50,179 (Sept. 24, 2019)
[11] WASSENAAR ARRANGEMENT, 'About Us' (May 30, 2019).

Administration Regulations ("EAR")[12]—grew out of Cold War-era coordination by the NATO nations to restrict the sale and shipment of strategically important, dual-use items to the communist nations closely allied with the Soviet Union. After the Cold War, as NATO's attention shifted, these nations initiated a renewed export control initiative to restrict the proliferation of arms and dual-use items to rogue states and terrorists.[13]

The agreement concluded in 1995 in the city of Wassenaar, Netherlands among these nations is not a treaty and, as such, does not independently have the force of law. The economic and security benefits of a standardized export control system continue to encourage Wassenaar nations to largely maintain multilateral export controls and have encouraged the development of additional international regimes to coordinate export controls, including the Nuclear Non-Proliferation Treaty, the Australia Group Controls, as well as UN Security Council Resolutions. However, there is no overarching legal requirement that these controls remain multilateral. Countries may implement unique, unilateral controls. Straying from the multilateral origins of the current export control regime by imposing unilateral controls, however, may negatively impact technological development, coordination and exchange among NATO allies.

A. What Do They Regulate?

U.S. export controls regulate the provision of U.S.-origin items to other countries or to foreign persons. The United States maintains two primary legal regimes for implementing these controls. The International Traffic in Arms Regulations ("ITAR") apply to certain items designed for and used in military and intelligence applications.[14] The EAR applies to certain military items, items in short supply, and items that may have military and civilian uses—"dual-use" items—a broad category covering almost all items not captured under the ITAR. Although these regimes have important distinctions, there are significant similarities in the scope of items and activities they regulate and the structure of their restrictions.

Items subject to these export control regimes include goods, software, and technology (i.e., information on the development, production or use of

[12] 15 C.F.R. § 730 *et seq*.
[13] In 1995, these nations met in Wassenaar, Netherlands to outline a new trade control regime. Significantly, China did not participate in these initial negotiations and remains outside of the current Wassenaar system.
[14] 22 C.F.R. § 120 *et seq.*

controlled items) that are physically present in the United States, as well as items that were produced in or otherwise originated from the United States.[15] Both export control regimes may also apply to items that are made outside of the United States. Under the ITAR, foreign-made items that incorporate an ITAR-controlled part or component are subject to the same restrictions as that part or component. The ITAR effectively "sees through" the end-item to its ITAR-controlled component and applies those same controls to the end-item. The ITAR also control items made from ITAR-controlled software and technology, the provision of defence services, and the brokering of defence articles and services.

The EAR takes a more permissive approach. Foreign-made items may incorporate a minimal amount of U.S.-origin content (typically 25%) and remain outside the scope of the EAR. However, foreign-made items that incorporate more than that allowable minimum are treated as U.S.-origin items and are subject to the EAR.[16] In certain limited circumstances, the EAR also controls foreign-made items that contain any amount of certain, highly controlled U.S.-origin content or that are the direct product of certain other U.S.-origin technology and software.[17]

Both the ITAR and EAR control the export of the items to which they apply. Under both programs, an export of a covered item must be authorized or exempt from the need for authorisation before the export occurs. Exports not only include the actual shipment or transmission of an item out of the United States, but also include the release of technology to a foreign person, even when that foreign person is physically located in the United States (a "deemed export").[18] For example, emailing design specifications of a controlled item to a French national colleague or discussing with that same colleague the process for using the item is considered an export of that controlled technology.

In addition to controlling the initial export of covered items from the United States, these regimes also restrict the re-export and transfer of those items. A re-export occurs when a covered item that has previously been exported out of the United States is again shipped or released to a third country. A transfer occurs when a controlled item previously exported to a

[15] 15 C.F.R. § 734, 22 C.F.R. § 120.
[16] 15 C.F.R. § 734.4.
[17] 15 C.F.R. § 734.3(a).
[18] 15 C.F.R. § 734.13; 22 C.F.R. § 120.17.

foreign country is provided to a different user or applied to a different end-use within that same country. In this regard, U.S. export controls typically follow the items they cover, even restricting transactions that occur entirely outside of the United States and that involve only non-U.S. persons.

Both regimes also generally restrict to whom covered items may be exported, re-exported, or transferred. The ITAR's restriction is quite broad: the provision of all covered defence articles and defence services to any foreign person must either be authorized or exempt from the need for authorisation.[19] The EAR only controls the provision of certain covered items to certain destinations or end-users or for certain end-uses. Different restrictions may apply to the export of an EAR-controlled item depending on where it is to be shipped, who will use it, and how it will be used. The same item exported to France, to a Russian energy company, or for use by the Chinese military would likely be subject to different EAR-based controls in each case.

B. Tools for Regulating – Item-Based, End-User and End-Use Controls

The U.S. Department of State (in the case of the ITAR) and the U.S. Department of Commerce (in the case of the EAR) implement these export controls through an item-based classification system and end-use and end-user controls, related licenses, and enforcement actions.

1. Item-Based Controls

Under both legal regimes, item-based controls are premised on classification systems that provide detailed descriptions of physical characteristics and performance parameters of the items subject to the controls. In order to evaluate what controls apply to an item for export, prospective exporters of U.S.-origin items must first determine which list—either the ITAR's United States Munitions List ("USML") or the EAR's Commerce Control List ("CCL")—includes a description of their item (i.e., the item's export controls jurisdiction) and then match their item to a description on the appropriate list to determine the item's classification (on the CCL, an item's classification is rendered as an alphanumeric sequence called the Export Controls Classification Number, or "ECCN"). The item's classification—taken together with its proposed destination, end-user, and end-use—determine which controls apply. On the CCL, different classifications of items are controlled for differing reasons (e.g., concerns about chemical weapons

[19] 22 C.F.R. § 123.1.

proliferation, human rights abuses, or crime control) and to differing extents. Depending on the applicable reasons for control and an item's destination, some exports may be effectively prohibited while others may be exported without further action.

These restrictions not only implement U.S. foreign policy but also often result from multilateral arrangements to impose similar controls among trading partners, including the Wassenaar Arrangement. This coordination helps to ensure a more equitable trading landscape among partner nations, but also slows the process for implementing new controls. Controls can always be imposed unilaterally in response to the United States' particular foreign policy concerns, but the U.S. is sensitive to the overreliance on unilateral controls as they may drive business away from the United States.

Requiring prior government authorisation is the primary means for controlling the export, re-export, or transfer of covered items. Like the CCL, the USML implements both U.S. foreign policy and national security policies as well as multilateral arrangements and treaty obligations in its item-based controls. In contrast to the CCL, however, exports of all items on the ITAR's USML are controlled in the same way. Exporters must obtain authorisation from the U.S. Department of State—whether in the form of a license or approved agreement—before exporting any item listed on the USML to any foreign person, unless one of several exemptions applies. Licensing policies established in the ITAR or by the U.S. Department of State's Directorate of Defense Trade Controls ("DDTC"), which administers the ITAR, determine how requests for authorisation will be considered and, consequently, the relative strength of the ITAR controls. For example, the State Department will deny requests for authorisation to export ITAR-controlled defence articles to China, though requests for authorisation to export those same items to a different country may be reviewed and approved on a case-by-case basis. In addition to controlling exports with authorisation requirements, the ITAR requires that manufacturers, exporters, and brokers of covered defence articles and defence services register annually with the State Department and notify the agency of any changes to their ownership, location, or other identifying information.[20]

The EAR also relies primarily on license requirements and related licensing policies to control exports of subject items. However, unlike the ITAR,

[20] 22 C.F.R. § 122.1.

authorisation requirements under the EAR may vary based on an item's destination (as well as its end-user and end-use, as described further below). An item requiring a license for export to China may not generally require a license for export to France. Also, unlike the ITAR, the EAR does not require a license for exports of all covered items—or even for all items included on the CCL. However, like the ITAR, the EAR does use a system of licensing policies, in addition to its license requirements, that also determine the strength of the EAR's controls. In this regard, not all licensing requirements are created equal.

2. End-User Controls

The U.S. Department of Commerce's Bureau of Industry and Security ("BIS"), which administers the EAR, also employs several different types of end-user controls. These tools, which may be used to limit exports to broad categories of end-users or specific individuals or entities, are among the most powerful of these tools in BIS's arsenal. They are often implemented by designating the targeted end-user to one of several lists of prohibited parties, including, for example, the EAR's Denied Persons and Entity Lists—which include targeted end-users in at least 19 NATO Member States. Such end-user controls can be implemented unilaterally (i.e., without international coordination), independently (i.e., without further Congressional action), and relatively quickly.

Individuals or entities subjected to these restrictions may be designated to BIS's Entity List or Denied Persons List. Persons added to the Entity List are subject to additional licensing requirements and specific, often restrictive, licensing policies.[21] In some cases, this may effectively cut the designee off from U.S.-origin exports. Although the Entity List began as a way to restrict exports to entities known to divert items to weapons of mass destruction programs, it has since expanded to include entities that pose any number of risks.

Designation to the Denied Persons List results in even more severe restrictions. Denied persons may not apply for or use a license or license exception. They are also broadly prohibited from negotiations concerning, ordering, buying, receiving, servicing, or disposing of EAR-controlled items.[22] BIS may add a company to the Denied Persons List as a penalty for violating the EAR or as a protective restriction. As the recent actions against ZTE and

[21] 15 C.F.R. § 744.16.

[22] 15 C.F.R. Supplement No. 1 to Part 764.

Huawei illustrate, these tools can have a significant, negative impact, especially when imposed on entities operating in industries that are heavily dependent on U.S.-origin parts and components.

3. End-Use Controls

End-use controls prevent items from being exported for, *inter alia*, use in certain nuclear applications, for chemical and biological weapons proliferation, and in certain nations' military activities—potentially imposing license requirements on cooperative development by NATO Member States of certain weapons technologies. These controls are the least frequently deployed of the controls listed here, in part because concerns about an item's end use are also often indirectly addressed by end-user or destination-based controls. The difficulty of complying with these restrictions may also discourage their imposition. While the prohibited end-uses are described in the regulations, it can be difficult to discern how a customer intends to use an item. Exporters must rely on additional due diligence review, contractual protections, and in some cases, specific certifications that the item will not be applied to prohibited end-uses. However, there may be little recourse if these prohibitions are violated by customers.

Compliance with all the various types of export controls—including end-user, end-use, and destination-based controls—is predicated on a technical evaluation of a product's performance characteristics and careful comparison to the USML and CCL. From that standpoint, compliance with item-based and end-user controls is relatively straightforward. The positive lists of controlled destinations and targeted persons make clear which exports are subject to the relevant restrictions. Exporters often know the locations and parties to which they are sending their products and therefore typically have access to the information necessary to confirm compliance. Furthermore, because end-user controls are an essential feature of U.S. trade controls—both export controls and sanctions—screening for prohibited end-users is a regular part of most well-developed trade compliance systems and there are a variety of tools readily available to assist companies in maintaining compliance with these restrictions. However, as with end-use controls, exporters may also wish to conduct additional due diligence to confirm that the recipient of their products does not plan to re-export the products to a prohibited destination or end-user.

Importantly, the licensing policies for each type of control described above—including item-based, end-user, and end-use controls—have been

calibrated to facilitate trade and interoperability among allies, in keeping with the U.S. export control regime's foundation in multilateralism and concerns about military preparedness. Both the ITAR and EAR generally control exports to allies—including NATO Member States—more permissively. In addition, both regimes include license exceptions and exemptions that specifically facilitate NATO-related trade, including special ITAR exemptions for trade with Australia, Canada, and the United Kingdom, which were implemented pursuant to different bilateral agreements with those nations.[23]

II. Recent Developments: Export Control Reform Act and Recent Changes to U.S. Law

With that general understanding of U.S. export controls in mind, it is important for members of the NATO community to understand how U.S. export controls have recently changed and will soon evolve.

The John S. McCain National Defense Authorization Act for Fiscal Year 2019,[24] which became law on August 13, 2018, contained two pieces of legislation that will have a significant impact on investment and technology transfers in the U.S. defence sector for decades to come. First, the bill contained the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA"),[25] which significantly expands the scope of inbound foreign investments subject to review by CFIUS. Second, the bill also included the Export Control Reform Act of 2018 ("ECRA"),[26] which gives the President, acting through the U.S. Secretary of Commerce, a mandate and new authorities to restrict the outbound transfer of "emerging and foundational technologies" and requires the Secretary of Commerce to include the health of the U.S. national defence industrial base as a factor when evaluating export control license applications. Both measures are likely to have significant effects on the NATO community going forward by, among other things, re-routing investment flows and restricting cross-border collaboration in defence-related technologies. In other words, depending on the strength of the controls and the technologies to which they apply, the human and financial capital necessary to develop these critical technologies—rather than flowing easily across borders—may become concentrated in particular

[23] *See e.g.*, 15 C.F.R. § 740.11; 22 C.F.R. §§ 123.15, 126.5, and 126.14-.17.

[24] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, 132 Stat. 1636 (2018).

[25] Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, §§ 1701-28, 132 Stat. 2174.

[26] Export Control Reform Act of 2018, Pub. L. No. 115-232, §§ 1741-81, 132 Stat. 2208.

allied (or adversary) states.

Recent changes to U.S. foreign investment restrictions and export controls have been driven by concerns about sensitive U.S.-origin technology falling into the wrong hands, including especially companies owned or subject to control by the Chinese state. Part of the impetus behind FIRRMA were studies which showed how non-U.S. companies, and especially Chinese firms, have been participating in a range of venture capital investments in early-stage, innovative technology companies.[27] The U.S. Congress was particularly concerned that China was using national investment policies and private sector commercial arrangements to force U.S. companies to provide their Chinese counterparts with access to basic and advanced technologies that would enable China to leapfrog decades of technological development and pose an even larger economic and strategic threat to the United States and its allies. Indeed, these policies and arrangements, such as technology transfer for market access arrangements, have been critical to the development of China's defence sector.[28]

Congress also heard from observers who sounded an alarm noting that, over time, certain foreign investors have modified their investment strategies in emerging technologies to include venture capital and green field investments,[29] which CFIUS lacked jurisdiction to review and block. The realisation that foreign technology transfers involving critical technologies were being insufficiently monitored and regulated prompted Congress to give the U.S. Government new authorities under ECRA to control outbound flows of technology.

To help regulate these transfers, ECRA requires the President to establish, in coordination with the U.S. Secretaries of Commerce, Defense, Energy and State, a "regular, ongoing interagency process to identify emerging and foundational technologies" that are essential to national

[27] *See, e.g.*, MICHAEL BROWN & PAVNEET SINGH, CHINA'S TECHNOLOGY TRANSFER STRATEGY: HOW CHINESE INVESTMENTS IN EMERGING TECHNOLOGY ENABLE A STRATEGIC COMPETITOR TO ACCESS THE CROWN JEWELS OF U.S. INNOVATION (Defense Innovation Unit Experimental, Jan. 2018).

[28] *Id.*; Bradley Perrett & Michael Bruno, *Changing the Rules*, AVIATION WEEK, Vol. 180, No. 21, at 52-54 (Sept. 2018); OFFICE OF U.S. TRADE REPRESENTATIVE, FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974 (Mar. 22, 2018).

[29] "A green field investment is a type of foreign direct investment (FDI) where a parent company creates a subsidiary in a different country, building its operations from the ground up." James Chen, 'Green Field Investment' (INVESTOPEDIA, May 31, 2019).

security but not yet captured by any other critical technology list.[30] As these emerging and foundational technologies are identified, the Secretary of Commerce is to establish controls on the export, re-export, or in-country transfer of such technology, including requirements for licenses or other authorisations.[31]

ECRA does not offer a precise definition of the "emerging technologies" or the "foundational technologies" to be controlled by BIS. Instead, it offers criteria for BIS to consider when determining what technologies will fall within this area of BIS control.[32] BIS is then responsible for developing implementing regulations.

To begin the process of identifying emerging and foundational technologies, BIS issued an Advance Notice of Proposed Rule Making ("ANPRM") in November 2018, seeking public comments on how to identify emerging technologies.[33] BIS will also consider the development of emerging technologies abroad, the effect of unilateral export restrictions on U.S. technological development and the ability of export controls to limit the spread of these emerging technologies in foreign countries.[34]

BIS broadly describes emerging technologies as those technologies "essential to the national security of the United States" that are not already subject to export controls under the EAR or ITAR.[35] The ANPRM suggests that technologies will be considered "essential to the national security of the United States" if they "have potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications or could

[30]Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(a)(1), 132 Stat. 2208, 2218. For example, FIRRMA expands the scope of transactions subject to CFIUS review to include not only transactions resulting in the ownership or control of U.S. businesses by foreign persons (as has traditionally been the case), but also *non-controlling* investments in any U.S. business that produces, designs, tests, manufactures, fabricates or develops one or more "critical technologies." For CFIUS purposes, the term "critical technologies" includes: the defense articles and services described on the International Traffic in Arms Regulations ("ITAR") United States Munitions List ("USML"); certain technologies identified on the Export Administration Regulations ("EAR") Commerce Control List ("CCL"); nuclear facilities and equipment identified in 10 C.F.R. Part 110; and select agents and toxins. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1703(a)(6)(A), 132 Stat. 2174, 2182.

[31]Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(b), 132 Stat. 2208, 2219.

[32]*See* Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(a)-(b), 132 Stat. 2208, 2218-21.

[33]Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (advance notice of proposed rulemaking Nov. 19, 2018) [hereinafter ANPRM].

[34]ANPRM at 58,201. Given the express limitations provided in ECRA, technologies produced outside the United States are unlikely to be targeted by the new controls, as unilateral U.S. export controls would do little to restrict the flow of these technologies.

[35]ANPRM at 58,201.

provide the United States with a qualitative military or intelligence advantage."[36] Although the ANPRM does not provide concrete examples of "emerging technologies," BIS provided a list of fourteen broad areas of technology[37] it viewed as subject to limited controls that could potentially be considered "emerging" and therefore subject to new, broader controls under ECRA once specific technologies are identified.

Meanwhile, the process for developing controls on "foundational technologies" will operate along a separate, but parallel, track.[38] While BIS has not yet issued a second ANPRM that identifies possible candidates for "foundational technology" controls, the agency is widely expected to do so in the coming months.

Once BIS has arrived at a definition for "emerging technologies" and "foundational technologies," respectively, along with a set of potential controls for each, BIS will likely publish a proposed rule (or rules) providing this information for a period of public comment. Those comments will undergo a process of interagency review, and BIS should then announce its final rule (or rules) providing the new controls on the export of emerging and foundational technologies.

Once specific emerging and foundational technologies are identified in the final rule(s), companies can expect that their proposed exports of these technologies will be subject to greater scrutiny, and at least for some countries, subject to a licensing policy of denial. This is because ECRA also obligates the U.S. Department of Commerce to gather and consider the kinds of information on foreign ownership that would normally be included in CFIUS submissions prior to its grant of an export license for emerging and foundational technologies. For example, if a proposed export transaction involves a joint venture, joint development agreement, or similar collaborative arrangement involving emerging and foundational technologies, the Department of Commerce is to "require the applicant to identify, in addition to any foreign person participating in the arrangement, any foreign person

[36]ANPRM at 58,201.

[37]These broad areas include: (1) Biotechnology; (2) Artificial intelligence and machine learning technology; (3) Position, navigation and timing technology; (4) Microprocessor technology; (5) Advanced computing technology; (6) Data analytics technology; (7) Quantum information and sensing technology; (8) Logistics technology; (9) Additive manufacturing (e.g., 3D printing); (10) Robotics; (11) Brain-computer interfaces; (12) Hypersonics; (13) Advanced materials; and (14) Advanced surveillance technologies. ANPRM at 58,202.

[38]*See* ANPRM at 58,202 ("Commerce will issue a separate ANPRM regarding identification of foundational technologies that may be important to U.S. national security").

with significant ownership interest in a foreign person participating in the arrangement."[39]

While it is unclear how the Department of Commerce will specifically implement these new policy and licensing directives, we predict that many companies seeking to export emerging and foundational technologies will find it more difficult going forward. Not only will they be required to provide more information regarding their proposed counterparties in their export license applications, such as information on their counterparties' ultimate ownership and their role in the U.S. defence industrial base, but the Department of Commerce will likely deny applications when key strategic competitors of the United States, such as China, are involved.

Moreover, any technologies that BIS identifies as emerging or foundational through this rulemaking process will be considered "critical technologies" for the purposes of determining CFIUS jurisdiction.[40] FIRRMA now requires that certain foreign investments in U.S. companies that deal in these critical technologies receive CFIUS review and approval. Under CFIUS's new regulations implementing FIRRMA, CFIUS must receive advance notice of certain types of non-controlling foreign investments in U.S. companies that design, test, manufacture, fabricate or develop critical technologies—including emerging and foundational technologies identified by BIS—for use in one of several listed industries.[41] In this regard, BIS's final determination regarding what constitutes "emerging and foundational technologies" will also impact the scope of CFIUS's expanded jurisdiction.

III. Factors Affecting the Impact of Export Controls on Emerging Technologies

The impact of new export controls on the further development of emerging technologies identified for new export and foreign investment controls, even among NATO Member States, is likely to vary based on several different attributes.

A. Relative Cost and Likelihood of Expected Payoff of Developmental Research

[39] Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(b)(3)(C), 132 Stat. 2208, 2220.
[40] Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1703(a)(6)(A)(vi), 132 Stat. 2174, 2182.
[41] 31 C.F.R. § 801.101 (2020).

Who may be willing to sponsor development research depends on the potential payoff relative to the investment. High-cost, risky investment in emerging technologies—made more expensive and riskier by the imposition of new export controls—may limit the number of entities willing and able to undertake research and development of these new critical technologies. In general, one would expect riskier, higher cost investments in developmental research to be pursued only by the best-resourced entities that can afford potential failure. In contrast, when there is a greater likelihood of returns on lower cost investments, more may be willing to make the initial investment required to bring products to market.

B. Cultures of Innovation

The relative impact of export controls on an emerging technology will also hinge in part on the cultural practices of technologists in the fields required to develop the technology, which may vary—even among close allies. For a range of reasons, technologists in a particular field may already share freely and frequently as innovations occur. Technologists in other fields, for example, in fields where more investment is required to generate new products, may be less inclined to share particular innovations or the results of attempts to apply them beyond the walls of their respective employers.

When a specific field of emerging technology has a more open culture of innovation, export controls that seek to channel innovation may be more disruptive and may be less effective in channelling further innovation when compared with fields with more closed innovation cultures.

C. Emerging Technology-Specific Drivers for Collaborative Innovation

Alongside the economics and cultures of innovation in particular fields of emerging technology, there may be inherent drivers in some fields that lead technologists to collaborate. Generally speaking, if there is an expectation that a particular emerging technology may lead to development of products that will be more ubiquitous in people's lives, technologists may work to throw open the development of security standards and functions for these technologies to ensure that their applications are better vetted and trusted by others. In contrast, if emerging technology products are more likely to be adopted by only a few actors and in limited applications, technologists are more likely to keep the development of security for their products proprietary. For example, researchers in both

quantum computing and AI may have strong public policy interests to collaborate with one another in the development of common security protocols.

Given the potential power of quantum computing to breach the encryption algorithms used to secure so many aspects of modern-day communications, finance, and privacy, researchers have strong incentives to collaborate with one another on the development of quantum-safe cryptography. Similarly, given the potential ubiquity of AI-enabled applications in people's everyday lives, researchers have strong public policy incentives to ensure that AI-enabled applications cannot be hacked.

Other related drivers are the potential for an emerging technology to become a platform technology—i.e., the basis upon which other technologies or applications are developed—or the need of emerging technology applications to share platforms with others. Technologists may have strong incentives to be the first movers in particular areas of technology and to open their technology to others that will use it to develop applications based on their technology and draw still others to the new platform. Similarly, when a technologist knows that they will, by necessity, need to share infrastructure with other competitors, they may be more inclined to participate in the development of common standards and functionality.

D. Existing Export Controls on Emerging Technologies and Associated Technologies

The impact of new export controls on the development and proliferation of technologies is also likely to vary depending on whether there are already existing controls on associated technologies. Not all fields of emerging technology draw from fields of research that are already subject to export controls. To the extent that they are, technologists are already subject to limits on the dissemination of development technology through pre-publication review and licensing and the impact of new export controls is more likely to be only incremental.

E. Pre-Existing Distribution of Innovation

Whether and how controls could impact the development and proliferation of an emerging technology are also dependent on the underlying distribution of research in the relevant fields. If researchers in only a single country or a small set of countries are currently pursuing research in a particular subject area, ring fencing around the perimeter of this innovation

could potentially be effective in limiting its further proliferation. In contrast, such controls may be less effective at controlling a technology's proliferation, or proliferation to specific actors, if there are many more centers of innovation. When innovation is multi-centered, however, export controls could lead to a reduction in cross-fertilisation of technological ideas and abet the development of multiple advanced but divergent forms of the technology.

F. Managed vs. Unmanaged Innovation

The impact of export controls on the development of an emerging technology will also hinge in part on whether subsequent innovation is being centrally managed. Although a government may invest in the fundamental research required to lay the groundwork for an emerging technology, how export controls may impact the development of the technology may depend in part on whether the investment that follows is managed or unmanaged. For example, if export controls cut off a particular country and its researchers from a required building block for product development, a centrally managed system is more likely to be able to channel investment to the development of replacements. While those pursuing innovation in less centrally managed systems may also be able to identify a gap and channel research to fill it, they may not be able to do so as quickly or as effectively.

IV. Likely Impacts of New Export Controls on Two Types of Emerging Technologies

Finally, for a glimpse into how the forthcoming U.S. export controls on emerging technologies may play out in the real world, we offer two case studies. By applying the factors described in the previous section to a pair of technologies likely to be crucial to NATO's future military capabilities—hypersonics and artificial intelligence—it is possible to see how U.S. export controls, depending on how they are written, may cause innovation to become concentrated behind national borders.

A. Hypersonics

The term "hypersonics" describes technologies that enable aircraft, missiles, and other projectiles to travel at speeds of over Mach 5, or five times the speed of sound.[42] The technology has potential civil applications if it can

[42] *See, e.g.*, Congressional Research Service, 'Hypersonic Weapons: Background and Issues for Congress' R45811, (Mar. 17, 2020) 2.

be deployed in a manner safe enough to power commercial aircraft, but the primary application of hypersonics is military. For example, Russia claims to have now developed, tested, and deployed missiles that can travel as fast as Mach 27 and, if this claim is true, there is no defence system currently deployed anywhere in the world that would be able to intercept. Moreover, given the speed at which they would travel, hypersonic attacks would be more difficult to detect and would provide those targeted only a short period of time to respond.[43]

Fundamental research on hypersonics is occurring in multiple sites around the world, including China, the United States, Germany, France, Australia, and Russia, among other countries. According to a presentation count at the AIAA International Space Planes and Hypersonic Systems and Technologies Conference, China-based researchers have been the most prolific.[44] In contrast to China, which is managing a more integrated university research effort by placing large numbers of researchers focused on hypersonics in the same location, university research in the United States has been decentralized and less coordinated to date.[45]

Table 1: Top Ten Countries Presenting Papers at AIAA International Space Planes and Hypersonic Systems and Technologies Conference (2005-2017)[46]

Country	2005	2006	2008*	2009	2011	2012	2014	2015	2017	Total
China	7	17	4	15	18	31	3	42	260	397
U.S.	61	64	38	38	60	15	18	32	14	340
Germany	11	17	16	30	28	25	10	18	9	164
France	22	13	13	16	16	15	5	18	8	126
Australia	8	24	7	20	10	26	8	13	7	123
Japan	21	17	16	14	13	20	4	7	1	113
Italy	27	10	7	19	16	8	0	7	5	99
European groups[2]	6	6	6	8	9	5	1	8	6	55
Russia	14	5	6	4	3	6	0	5	5	48
U.K.	2	5	0	6	3	4	1	13	4	38
Total	**179**	**178**	**113**	**170**	**176**	**155**	**50**	**163**	**319**	**1,503**

Source: IDA Science and Technology Policy Institute
* International Space Planes and Hypersonics Systems and Technology Conference is not held every year.

[1] Other nations presenting papers at the 2017 conference were Algeria, Belgium, Brazil, Canada, Greece, Hungary, India, Iran, Netherlands, Norway, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan and Turkey.

[2] European organizations

[43] R. Jeffrey Smith, 'Hypersonic Missiles Are Unstoppable. And They're Starting a New Global Arms Race' *NY Times Magazine* (New York, June 19, 2019).
[44] K. Button, 'Hypersonics Weapons Race' *Aerospace America* (June 2018).
[45] *Id.*
[46] *Id.*

China, Russia, and the United States are on the shorter list of countries that have been able to move beyond fundamental research and into development, testing, and even deployment, in part because there are high barriers to entry in the further development of hypersonics and their associated technology. For example, hypersonic weapon testing in the United States relies in part on the prior existence of high velocity wind tunnels capable of simulating the wind speed and resistance that aircraft and projectiles traveling at higher than Mach 5 speeds would encounter. Moreover, the further development of hypersonic technology also requires innovation in several different fields, including ceramics, metallurgy, composite materials, and propulsion. Each of these associated technologies have their own high development costs and, as a result, tend to be pursued by larger private sector entities who are better able to afford research and development investment with more uncertain pay-offs.

The United States currently lags behind China and Russia in the development and field testing of hypersonic weapons and is now spending billions of dollars to catch up.[47] For example, the fiscal year 2019 U.S. Department of Defense budget included USD $2.6 billion for hypersonics development and the largest contract awarded went to Lockheed Martin to develop hypersonic missile systems for B-52 bombers and Air Force jets.[48] The fiscal year 2020 U.S. Department of Defense budget funded the creation of a university consortium to provide the Defense Department with increased access to foundational research, technology development, and workforce expertise. It also allocated over USD $500 million to support the rapid prototyping of hypersonics among other investments. Thus, while the United States currently lags both China and Russia in hypersonic development, it is investing significant sums now to catch up to and surpass its strategic competitors. Depending on how the United States opts to control the hypersonic technologies it is developing, NATO allies may or may not be involved in, or have opportunities to co-develop and use, hypersonic defensive and offensive weapons systems.

Although those conducting fundamental research into hypersonics are likely to continue publishing research papers, technologists working to develop and flight test hypersonic technology are less likely to freely share

[47] Anthony Capaccio, 'Pentagon to Test Hypersonic Missiles at Five Times the Speed of Sound' *Bloomberg* (Jan. 28, 2020).
[48] *Id.*

with others outside their particular sponsoring organizations. University researchers conducting applied projects are often subject to pre-publication review and clearance, and private sector engineers are typically precluded by their employment agreements from sharing their discoveries. Moreover, already-existing export controls, such as the ITAR, prohibit the public dissemination of technology associated with weapons systems without U.S. agency approval or licensing. Accordingly, even robust U.S. export controls on hypersonics are unlikely to alter the already closed and compartmentalized research landscape.

B. Artificial Intelligence

AI is not a single technology but a set of related technologies that aim to mimic different aspects of human intelligence. While the development of AI powerful enough to mimic general human intelligence is viewed by many as several decades away, there are a plethora of narrow AI applications that perform defined tasks such as strategic game play, natural language processing and translations, and image recognition. Narrow AI applications are typically developed using large data sets and specific algorithms to make increasingly robust predictions about the future.[49] The data used for machine learning can be either supervised (i.e., data that is already associated with other facts, such as labels) or unsupervised (i.e., raw data that requires the AI application to identify data patterns without prior prompting). This includes reinforcement learning—where machine-learning algorithms actively choose and even generate their own training data.[50]

Research into AI is global, with significant centers of innovation in the United States, Europe (particularly the United Kingdom and Germany), Japan, and China.[51] In the United States, AI is being pursued across universities, in the military, and throughout the private sector, with the most significant amount of money being spent in the commercial sector. A McKinsey Global Institute study estimates that the commercial sector invested between USD $20 to 30 billion in AI research in 2016 and estimates that this number will increase to USD $126 billion by 2025.[52] In contrast, U.S. Department of Defense unclassified

[49]Joshua Meltzer, 'The Impact of Artificial Intelligence on International Trade' *Brookings Institution* (Dec. 13, 2018).
[50]*Id.*
[51]Bruno Jacobson, 'Five Countries Leading the Way in AI' *Future Trends* (Jan. 8, 2018).
[52]McKinsey Global Institute, 'Artificial Intelligence, The Next Digital Frontier?' (June 2017) 4-6.

expenditures on AI totalled only USD $600 million in 2016.[53] Given the order of magnitude difference between commercial and military investment in AI technologies in the United States, some observers have suggested that the Defense Department partner with the private sector to further develop military applications. However, there is strong scepticism of such partnerships among commercial leaders in the field, making the management of further innovation in AI decentralized and uncoordinated. In contrast, AI innovation in China is reported to be more centralized and intentional, and few boundaries exist between Chinese companies, university research laboratories, the military, and the central government.[54] To the extent the Chinese government identifies promising fundamental or applied AI research, it has a more direct way to guide further development.

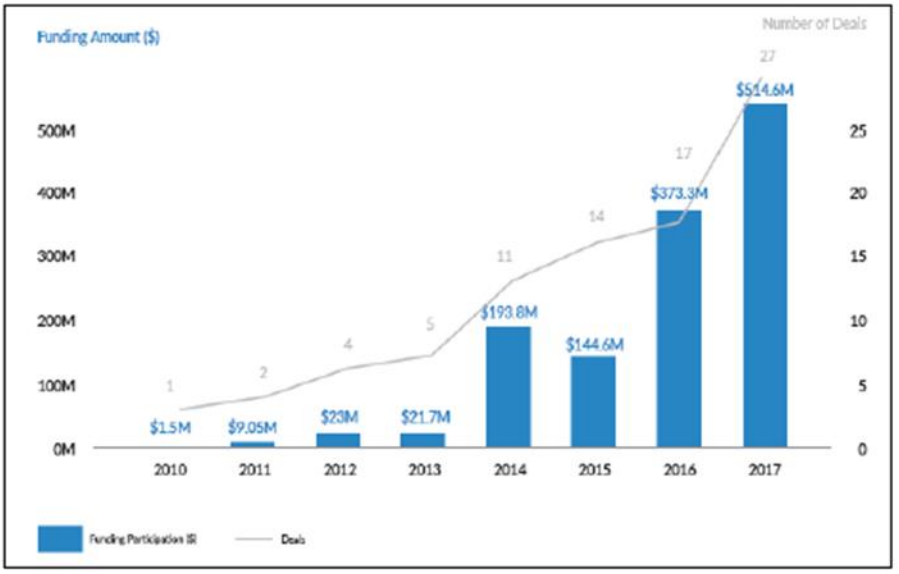
In contrast to other kinds of emerging technologies, AI has relatively low barriers to entry, at least with respect to AI software development. Although finding programmers with the requisite talent can be costly, many centers of AI research make training courses on AI available for free online and host environments, libraries, and data sets for those learning AI coding to train, program, and test AI applications. In addition to the relatively low level of investment required to learn AI programming, robust computing power and AI training software are also now available to customers through cloud-based services that can be rented from global providers like Microsoft Azure, Amazon Web Services, Google Cloud, and Alibaba Cloud.

In contrast to AI software development, there are higher barriers to entry to the design of AI-capable chips and their fabrication, barriers that largely replicate those that already exist for other areas of semiconductor manufacture, in which only a small number of companies compete to etch more and more computing power and efficiency onto smaller and smaller wafers. The life cycle for design, development, and production of new chips often spans several years, and there is only a small handful of companies in the United States, Taiwan, Japan, and South Korea that are capable of fabricating the most advanced semiconductors once designed.[55] Another key limit on AI development is the availability of bias-free, error-free and labelled data sets that readily can be used to train and test AI and machine

[53]Congressional Research Service, 'Artificial Intelligence and National Security' R45178, (Jan. 30, 2019) 6.
[54]Gregory C. Allen, 'Understanding China's AI Strategy' *Center for New American Security* (Feb. 6, 2019).
[55]*See generally*, Deloitte, 'Semiconductors – The Next Wave' (April 2019).

learning applications.[56]

Figure 2. Chinese Investment in U.S. AI Companies, 2010-2017



Source: Michael Brown and Pavneet Singh, China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation, Defense Innovation Unit Experimental, January 2018, https://www.diux.mil/download/datasets/1758/DIUx%20Study%20on%20China's%20Technology%20Transfer%20Strategy%20-%20Jan%202018.pdf, p. 29.

In contrast to those working in hypersonics and other emerging technologies, AI technologists freely share the results of their work in research publications and through a range of online platforms such as GitHub, arXive.org, and H2O.ai. Many of the algorithms used in AI today are publicly available, and university and even applied AI researchers working with these algorithms will often move to quickly publish their work both to demonstrate proof of concept for their implementation and also to help accelerate the review and vetting of innovations by peer technologists. Moreover, similar to making operating system source code freely available to encourage programmers to develop new applications, several of those providing AI services frameworks also make them open source to help accelerate the further development of new applications and the wider adoption of particular AI service provider platforms.[57]

Another key contrast with hypersonics research is the relative lack of

[56] *See e.g.*, 'Almost 80% of AI and ML Projects Have Stalled, Survey Says' *Robotics Business Review* (May 23, 2019).
[57] Patrick Shafto, 'Why Big Tech Companies are Open-Sourcing Their AI Systems' *The Conversation* (Feb. 22, 2016).

export controls on AI today. While there exist certain controls on software and semiconductor design and fabrication technology, with only one exception, U.S. export controls have not been framed around AI-enabled applications, and neither machine learning nor smarter kinds of AI are themselves objects of control under either the EAR, the ITAR, or international regimes such as the Wassenaar Arrangement. On January 6, 2020, the U.S. Department of Commerce imposed new controls on software that uses AI to automate the analysis of geospatial imagery and point cloud data.[58] As a result, when new, application-specific AI controls are imposed, many researchers in AI will experience new and significant impacts on their ability to freely share and collaborate on that specific application and any iterations that rely or build on it.

C. Probable Impacts of New Export Controls on Technology Development and Interoperability

Given the foregoing development characteristics of hypersonics and AI, we can make reasonable predictions of how different types of U.S. export controls are likely to be applied and how they are likely to impact both U.S. and international technological development in each field.

1. Impact of New Emerging Technology Controls on Hypersonic Development

First, because many of the fields required to advance hypersonics are already subject to multilateral export controls, the applied research communities working in the United States on hypersonics will likely be able to continue cross-border collaborations in much the same way as they have performed to date: under specific export licenses authorising only certain collaborations with counterparties outside of the United States. Second, because of the high barriers to entry, further development of hypersonics, especially hypersonic vehicles that integrate research and development from hypersonics' associated fields, will continue to be a limited pursuit of only large defence contractors, who are best placed to make and receive the kinds of investments necessary to further develop and apply advancements in the several different areas of fundamental research required for hypersonics. Third, further development of hypersonics is likely to result in divergent development with multiple, different proprietary designs being

[58] Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series, 85 Fed. Reg. 459 (Jan. 6, 2020).

pursued by researchers who have not engaged in the kind of open-source collaboration that has characterized development in fields like AI. Fourth, because only a few private sector entities and applied research centers will be in a position to develop hypersonic offensive and defensive capabilities, there will not be the same incentive to develop open and widely-shared security protocols to protect access to hypersonic technologies as there would be for technologies that are expected to be more widely adopted in civil applications. Taken together, these factors will likely act together to cluster hypersonics development into only a small number of companies and government-funded research institutes in the United States, Europe, Russia, and China, with each developing independently from one another unless national export authorities allow, and multilateral institutions like NATO and its membership sponsor the integration of research and development, application, and production. While the United States' new export controls on hypersonics and associated technologies will almost certainly restrict the flow of these technologies and resulting weapons systems to strategic competitors like Russia and China, the already existing NATO and NATO member investment in the development (including co-development) of hypersonics could provide the United States with an incentive to fashion controls that include NATO and NATO Member States in U.S. development efforts.

New deemed export licensing requirements, which hinge on item-based controls, are less likely to have a significant impact on hypersonics development because many U.S.-based defence contractors are already accustomed to the kinds of hiring and technology controls required to implement these restrictive measures, and have likely already obtained licensing for any non-U.S. person technologists working in the several areas of technology required to further develop and test hypersonics research.

U.S. and multilateral export controls on end-uses and end-users are also likely to intensify the clustered and divergent development of hypersonics. In addition to item-based U.S. export controls, the contributions that hypersonics can make to both ballistic and nuclear weapon proliferation also makes applied hypersonics potentially subject to end-use and end-user licensing requirements. These kinds of export controls have the effect of ensuring that only authorised persons and entities outside of the United States receive technology and other items controlled for these purposes, further reinforcing collaboration channels with specific end-users and also making it less likely that hypersonics technology will be shared with those considered to be adversaries of the United States. The recent expansion of CFIUS's jurisdiction to

review certain non-controlling, as well as controlling, investments in U.S. businesses is also unlikely to have a significant impact on the development of hypersonics. Given the sector's high barriers to entry and the substantial role played by large defence contractors in developing such technology, there are already limited avenues for foreign investors to acquire a significant interest in one of the handful of U.S. businesses capable of developing hypersonics. As FIRRMA is fully implemented, opportunities for non-U.S. persons to invest in such technology are likely to remain similarly constricted.

2. Impact of New Emerging Technology Controls on AI Development

Although the significant investments required to develop and fabricate new AI hardware will continue to limit the number of entities that can work on AI hardware, AI software has been and will continue to be widely distributed and pursued globally, wherever talent can be found. The relative lack of existing export controls on AI and the widespread practice of open sharing of innovation and collaborative work on common AI standards among software developers will make it difficult to impose new export controls that will not be significantly disruptive.

Item-based controls on AI, such as on AI software and technology applied to specific military and dual-use items, are likely to cause AI development to fragment in different ways. The United States would presumably impose item-based controls in ways that limit transfer of AI technology to strategic competitors such as China and Russia, but allow licensed transfers to strategic allies of the United States such as NATO members, plus Australia, Japan, New Zealand, Sweden, and South Korea, or some subset of these countries. However, given that China is already a leader in AI research, it is likely that these controls will cut off at least U.S. researchers from certain innovations occurring in China and in multinational collaborations that include China. This could lead to divergence between U.S. and Chinese AI innovations and could undermine efforts to develop global security standards for access to AI-controlled applications. While U.S. item-based controls on AI are likely to leave open the potential for continuing collaboration with U.S. allies in NATO and Asia, export licensing is likely, at least at the outset, to hinder many ongoing collaborations. Moreover, U.S. allies are likely to be subject to significant geopolitical pressure from countries on the outside of the U.S. export control ring fence, especially China, who will continue to develop AI applications that may rival and even surpass U.S.

technologies in specific applications. Individual NATO countries will therefore likely be placed in the difficult position of trying to choose between divergent U.S. and NATO-developed AI applications and Chinese ones, the latter of which are likely to be less costly.

New, item-based deemed export licensing requirements are likely to have significant, disruptive impacts on the development of AI technologies. U.S. AI start-ups and technology giants alike rely on large numbers of non-U.S. technologists, with some companies employing non-U.S. person technologists numbering in the many thousands. Because AI and AI applications have not historically been the subject of significant export controls, many technology companies have not yet developed the internal compliance architectures required to identify potential licensing requirements or to keep separate licensed and unlicensed technologists within their companies. Especially for AI researchers who, for reasons discussed above, are already strongly predisposed to collaboration, these AI start-ups and product development teams within larger technology companies are likely to be severely impacted by new controls. This disruption—including the potential that the U.S. Government will delay or deny licenses to support leading non-U.S. technologists in their work—may cause many of these highly specialized personnel to search for employment opportunities outside the United States.

To the extent more targeted end-use and end-user controls are applied to AI innovation,[59] such controls may be less disruptive to current patterns of innovation and may be less likely to lead to significant divergence across countries and innovation ecosystems. With end-use controls, only certain applications of AI would be targeted and export authorities would have the opportunity to review and channel technological exchange toward certain projects and research collaborations and away from others. Similarly, end-user controls would only prevent certain end users, such as the applied research institutes and other organizations of strategic competitors, from obtaining U.S. or NATO technology.

Moreover, the CFIUS review process is likely to significantly disrupt cross-border investments in AI technology. Currently, China and the United States are among the leading centers of AI innovation and are also the top destinations for venture capital investment in AI technologies—with Chinese AI companies raising USD $31.7 billion during the first half of 2018, out of a

[59] *See id.*

global total of USD $43.5 billion.[60] However, since the Trump administration came to office in 2017, Chinese foreign direct investment in the United States across all sectors has fallen by approximately 90 percent, driven in part by heightened CFIUS scrutiny of China-based deals.[61] Indeed, while China has historically been a significant source of inbound investment in the United States, most of the transactions that have been blocked by the Committee to date either involved a Chinese acquirer or were motivated by concerns regarding Chinese competitors. Although CFIUS continues to clear Chinese deals, CFIUS review may result in lengthy delays and the imposition of significant mitigation measures. Accordingly, the prospect that the U.S. Government may delay, condition, or reject Chinese investments in U.S.-based AI companies may further chill foreign investment in the sector and cause Chinese and other foreign investors to instead direct their investment dollars toward homegrown AI companies.

Conclusion

Since publishing its list of potential targets for the new emerging technology controls,[62] BIS has signalled that the new controls will be more narrowly tailored—perhaps focusing on specific applications of emerging technologies—rather than broad controls on all items falling within any of the categories listed in the ANPRM.[63] It is possible that the new controls may be structured similarly to the restrictions BIS imposed on AI-driven geospatial imagery software in January 2020, which used specific performance characteristics to target a specific application of AI.[64] Such narrow tailoring could help to limit the new controls' impact. However, BIS officials have also cautioned that there will likely be more than one round of new emerging technology controls, and restrictions on foundational technology are still forthcoming.[65] The combined effect of these new controls—or simply the anticipation of their impact—could restrict international collaboration and slow development of the targeted technologies.

---

[60] Xiaomin Mou, 'Artificial Intelligence: Investment Trends and Selected Industry Uses' *IFC Emerging Markets Compass* (Sept. 2019) 2, Note 71.
[61] *See, e.g.*, Alan Rappeport, 'Chinese Money in the U.S. Dries Up as Trade War Drags On' *NY Times* (New York, July 21, 2019).
[62] *See* ANPRM.
[63] Ian Cohen, 'Companies, Trade Groups Concerned over Emerging Tech Controls' *Export Compliance Daily* (Nov. 8, 2019) [hereinafter Cohen, *Companies, Trade Groups Concerned*].
[64] Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series, 85 Fed. Reg. 459 (Jan. 6, 2020).
[65] Cohen, *Companies, Trade Groups Concerned*.

As described above, the effect of these new controls will also depend on several factors endogenous to the targeted industries. New export controls are likely to have a less significant impact for industries where the existing barriers to entry are already high or where the research and development culture is less collaborative. Current practices for sharing technology, existing export controls, and established distributions of capacity will all affect the extent to which new export controls shape the development of emerging and foundational technologies.

The impact of these new controls also depends on how they are implemented—whether they remain unilateral controls or are also adopted by U.S. allies. There are early indications that the United States hopes to make these new restrictions multilateral. Not only does ECRA require coordination with multilateral export control regimes, but BIS officials have also indicated that they plan to present the new controls on emerging technologies for adoption by the members of the Wassenaar Arrangement through the group's regular decision-making process.[66]

The United States has recently shown an interest in taking a multilateral approach in other areas of U.S. trade controls, encouraging international alignment by offering a reduced regulatory burden to those who adopt its policies and processes. New CFIUS regulations provide favourable treatment for businesses from countries that adopt a similar structure for national security review of inbound foreign investment.[67] Meanwhile, BIS has proposed removing license exceptions for re-exports from Wassenaar countries to jurisdictions of national security concern because of concerns BIS has about the different license review standards that the United States and its allies apply to such exports.[68] The implication of the proposed rule is that a realignment of those review standards by U.S. allies could mean the current license exception stays in place.

By first taking unilateral action and then pursuing multilateral adoption, the United States is indicating that—while it would prefer not to "go it alone"—the national security risks presented by the current regulatory landscape are sufficiently great that a unilateral response is preferable to no

[66]Export Control Reform Act of 2018, Pub. L. No. 115-232, § 1758(c), 132 Stat. 2208, 2221; Cohen, *Companies, Trade Groups Concerned*.

[67]*See* Provisions Pertaining to Certain Investment in the United States by Foreign Persons, 84 Fed. Reg. 50,174, 50,179 (Sept. 24, 2019) for an explanation of the new "excepted foreign state" status implemented in 31 C.F.R. §§ 800.218 and 800.1001.

[68]Modification of License Exception Additional Permissive Reexports (APR), 85 Fed. Reg. 23,496 (Apr. 28, 2020).

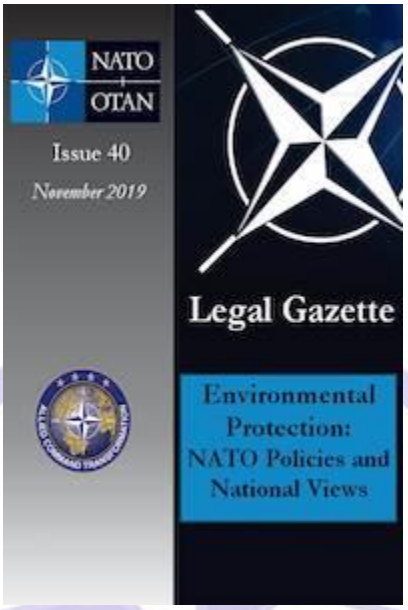
response at all.

In the short term, this control-now-cooperate-later approach could lead to a divergence in export controls that negatively affects the speed with which emerging technologies continue to develop and the interoperability of items made using these controls. If efforts to encourage international adoption of these restrictions fail, a fragmented regulatory environment could develop in the longer term—with separate controls adopted in the United States, EU, and China. Depending in part upon the factors described above, U.S. industry could suffer as revenue from restricted jurisdictions is lost and competitors gain market share. Development of important technologies could also move offshore in search of more favourable regulatory environments. Such shifts could also harm U.S. allies, as technical development slows or becomes inaccessible.

However, successful international coordination to control emerging and foundational technologies could expand the economic and security benefits of the current multilateral framework in the long term. Adoption of similar controls by U.S. allies in NATO would facilitate the development of those technologies and the interoperability of the cutting-edge items they will be necessary to produce. Just as Cold War collaboration on export controls helped to counter the threat of the Eastern Bloc and the Wassenaar Arrangement has helped to counter rogue states and international terrorism, multilateral adoption of controls on emerging and foundational technologies would help to ensure a coordinated approach by the United States and its NATO allies to address emerging threats to international security.

***

...of NOTE



The NATO Legal Gazette can be found at the official ACT web page:
http://www.act.nato.int/publications

and at LAWFAS