BRILL
NIJHOFF

SECURITY AND HUMAN RIGHTS (2021) 1-13

SECURITY AND
HUMAN RIGHTS
brill.com/shrs

Trading Emerging Technologies: Export Controls Meet Reality

Scott A. Jones
Non-Resident Fellow, The Stimson Center, Washington D.C., USA
qed747@gmail.com

Abstract

"Emerging technologies" and the growing inventory of their dual-use applications increasingly challenge policymakers with how to balance technological development, economic competitiveness, and national security priorities. While dual-use export control regulators have always struggled with balancing economic and security interests, emerging technologies are challenging controls systems ill-equipped to define or practically control them. As the most advanced case, the US export control effort is an instructive regarding the challenges of deploying conventional controls over defining and controlling rapidly developing technology sets. This article reviews the US case in light of the current challenges posed by emerging and foundational technologies.

Keywords

emerging technologies – dual-use – proliferation – security – innovation – disruption

1 Introduction

"Emerging technologies" and the growing inventory of their dual-use applications increasingly challenge policymakers with how to balance technological development, economic competitiveness, and national security priorities. Exponentially improved computing power, hyper-precise navigation systems, and mass amounts of stored personal data represent many of the key issues driving the need for effective emerging technology governance. However, many pivotal questions remain unanswered. What is the best approach to

regulate, if at all, the trade in emerging technology to ensure that these technologies do not threaten national security interests? Based on their current stages of advancement, how can trade control tools be effectively applied to specific emerging technology areas?

The disruptive nature and the uncertainty surrounding the military applications of emerging technologies increases the perceived risks associated with associated unregulated trade flows. Governments are beginning to address this challenge using traditional export control policies and procedures. In 2018, the US reformed its export control regulations to cover emerging technology exports. Other governments are following suit.[1] As the most advanced case, the US export control effort is an instructive case regarding the challenges of deploying conventional controls over defining and controlling rapidly developing technology sets.

This article will examine the US effort to control the trade in emerging technology. The first section examines the conceptual underpinnings of emerging technology. Section two includes an examination of various national policy developments regarding emerging technologies trade controls. The final section considers the US export control case regarding emerging technology and related implications for overall efforts to manage the trade in and, more explicitly, the prevention of the illicit acquisition of emerging technologies.

2 Emerging Technology: Dual-Use Considerations

The security implications of emerging technologies are based on their dual-use nature.[2] The term "dual-use" refers to materials, equipment, and technology that have both a civilian and military purpose.[3] States' security

1 See, Kolja Brockmann, "Drafting, Implementing, and Complying with Export Controls: The Challenge Presented by Emerging Technologies," *Strategic Trade Review*, Vol. 4, Issue 6, Spring/Summer 2018.

2 Arguably, the term "emerging technologies" subsumes the dual-use category, that the underlying technology can be applied simultaneously to commercial and military-defense effect. That said, definitions for emerging can vary. For example, Rotolo, Hicks, and Martin analyzed commonalities of existing definitions of "emerging technologies" and identified five main attributes: "(i) radical novelty, (ii) relatively fast growth, (iii) coherence, (iv) prominent impact, and (v) uncertainty and ambiguity." The UK's Defense Technology Plan defines emerging technologies as follows: "Emerging technologies can be characterized as: immature technologies in the early proof-of- principle stages; more mature technologies but where a novel defense application has been identified."

3 See, for example, "15 CFR § 730.3 – "Dual use" and other types of items subject to the EAR.," Cornell Law School, available at: https://www.law.cornell.edu/cfr/text/15/730.3.

objectives may be achieved through controls on the transfer, flow, and development of related technology. Increasingly, policy tools such as export controls, investment controls, private sector engagement, and government sanctions seek to manage the risks and threats posed by emerging technologies.

Governments manage the transfer of strategic items and technologies simultaneously through national and multilateral export controls. Multilateral export control regimes develop and maintain guidelines and control lists to regulate transfers of dual-use goods, and, after the United Nations (UN) Security Council Resolution 1540 was adopted in 2004, all UN member states have an international legal obligation to regulate the transfer of goods and technologies that could be used by non-state actors for weapons of mass destruction (WMD).[4] Technologies deemed relevant to WMD or conventional items are placed on control lists, thereby establishing a basis upon which to implement trade controls on those items. In the case of dual-use goods, military end-use as well as technical thresholds are specified on control lists. In addition, in most countries that implement export controls, so-called "catch-all" controls can apply in certain cases to exports of non-listed goods that have a WMD or military end-use.

The potentially revolutionary impact of so-called "disruptive technologies" such as artificial intelligence, additive manufacturing (i.e., 3-D printing), and quantum computing became part of the global national security repertoire as the revolutionary market effects of these technologies became apparent.[5] Disruptive or exponential technologies, albeit originally a business school concept, were soon adopted by national security strategists.[6] For example, in a

4 UN Security Council Resolution 1540, UN Doc. S/RES/1540 (28 April 2004).

5 For example, see Shawn Brimley, Ben FitzGerald, and Kelley Sayler, "Game Changers: Disruptive Technology and U.S. Defense Strategy", Washington, DC: Center for a New American Security, September 2013; and Michael E. Horowitz, "Coming Next in Military Tech," Bulletin of the Atomic Scientists, vol. 70, no. 1, January 2014, pp. 54–62. See also James D. Shields and James A. Tegnelia, Co-Chairmen, Defense Science Board Report on Technology and Innovation Enablers for Superiority in 2030, Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, October 2013.

6 The theory of disruptive innovation was first developed by Clayton Christensen, of Harvard Business School, in his book, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (1997). Dr. Christensen used the term to describe innovations that create new markets by discovering new categories of customers. They do this partly by harnessing new technologies, but also by developing new business models and exploiting old technologies in new ways. See, Clayton Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business Review Press, New Haven, 1997. See also, Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond," World Economic Forum, 14 January 2016; James Manyika et al, *Disruptive Technologies: Advances*

Center for a New American Security report, Ben FitzGerald and Shawn Brimley defined disruptive technology in the defense sector as "a technology or a set of technologies applied to a relevant problem in a manner that radically alters the symmetry of military power between competitors" which then "immediately outdates the policies, doctrines and organization of all actors."[7] The focus on "innovation" and emerging technologies animates, for example, the Pentagon's current, third, Offset Strategy, as a means to "assure U.S. military superiority."[8]

The increasing association of emerging technologies with national and, for that matter, international security is evident in even a cursory review of the relevant policy and academic literature.[9] The two primary themes animating recent studies include: 1. Reviews of possible weapons applications of, for example, artificial intelligence and autonomous systems; and 2. Technology denial or control strategies. In the case of the latter, most studies are ambiguous with respect to the ability of applying export controls effectively, often noting that investment controls should also be part of a country's technology control strategy.[10] In the case of the former, the risk of technology determinism threatens to undermine an international consensus of what and how emerging technologies pose security challenges.[11]

That Will Transform Life, Business, and the Global Economy, McKinsey Global Institute, May 2013, p. 6.

7 Ben FitzGerald and Shawn Brimley, *Game Changers: Disruptive Technology and U.S. Defense Strategy*, CNAS Publication, September 2013, p. 11. See also, Jennifer J. Snow, "Entering the Matrix: The Challenge of Regulating Radical Leveling Technologies," Monterey: Naval Post Graduate School, 2015, p. 5.

8 See, Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence, Office of the Secretary of Defense, 31 October 2016. See also, Paul McLeary, "The Pentagon's Third Offset May Be Dead, But No One Knows What Comes Next Experts say the U.S. advantage over China and Russia is eroding," Foreign Affairs, 18 December 2017.

9 See, for example, "Artificial Intelligence and National Security," Congressional Research Service, Updated 26 August 2020; Stephen Hummel, and John Burpo, "Small Groups, Big Weapons: The Nexus of Emerging Technologies and Weapons of Mass Destruction Terrorism," April 2020, United States Military Academy; and Natasha E. Bajema and Diane DiEuliis, "Peril and Promise: Emerging Technologies and WMD," Emergence and Convergence Workshop Report, National Defense University, October 2016 (Washington, D.C.: National Defense University Press, May 2017).

10 See, for example, Kolja Brockmann and Robert Kelley, The Challenge of Emerging Technologies to Non-Proliferation Efforts: Controlling Additive Manufacturing and Intangible Transfers of Technology, SIPRI Research Paper, Stockholm International Peace Research Institute (SIPRI), April 2018 and "Securitizing trade and investment: franchising CFIUS," *Trade Security Journal*, Issue 6, March 2018.

11 The idea that emergence of a new technology leads inevitably to change and that technology is necessary and sufficient to drive innovation in military capability has been widely discredited by those who study innovation. The study of military innovation

3 Emerging Technologies and Worldwide Policy Developments

The international community's heightened attention to security threats posed by technological advances has led to a number of policy developments. In the US, the Export Control Reform Act (ECRA), passed in 2018, establishes a process to identify emerging critical technologies currently not identified in any list of items controlled for export.[12] The technology areas identified pursuant to ECRA are listed in the Advanced Notice of Proposed Rulemaking (ANPRM) published by the Bureau of Industry and Security (BIS) within the Department of Commerce in 2018.[13] The ANPRM sought public comment from the private sector on criteria for identifying and potentially controlling fourteen broad representative categories of technology:

1. Biotechnology
2. Artificial intelligence (AI) and machine learning
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
14. Advanced surveillance technologies

In addition, the ANPRM includes a list of illustrative examples of the technologies for each of the above categories (e.g., computer vision and national language processing within the AI and machine learning category). The ANPRM also notes that the definitional process will be ongoing through the interagency

---

emphasizes the critical role of political and bureaucratic politics among both military and civilian actors in selecting (or not selecting) particular technologies. See, Andrew D. James, "Emerging Technologies and Military Capability," in Richard Bitzinger, ed., *Emerging Critical Technologies and Security in the Asia-Pacific*, Palgrave Macmillan, New York, 2016, p. 11.

12 Export Control Reform Act, 2018, H.R 5040, available at: https://www.congress.gov/bill/115th-congress/house-bill/5040/text.

13 "Review of Controls for Certain Emerging Technologies," Advanced Notice of Proposed Rulemaking, United States Department of Commerce, Bureau of Industry and Security, 2018, available at: https://www.federalregister.gov/documents/2018/11/19/2018–25221/review-of-controls-for-certain-emerging-technologies.

process, private sector outreach, the Emerging Technology Technical Advisory Committee, and the Committee on Foreign Investment in the United States (CFIUS).

In addition, the US in 2018 passed the Foreign Investment Risk Review Modernization Act (FIRMMA), which in part expands the scope of covered transactions that fall under the purview of CFIUS. FIRMMA expands the scope of transactions to businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies (including emerging and foundational technologies) in relation to a designated industry. Designated industries are listed in the Annex of the regulation. Importantly, in the case that technologies, including those specified in the ANPRM, become controlled pursuant to ECRA, they will automatically be covered under FIRRMA's definition of "critical technologies." Therefore, the decision on how emerging technologies listed in the ANPRM will be controlled has significant repercussions for both export and investment, with an even greater potential to affect the private sector and worldwide technology flows and development. Other jurisdictions are likewise linking export controls and FDI reviews over emerging technologies.[14]

Outside of the US, policymaking to manage advancing technologies has begun in the context of investment controls but is slowly progressing to the realm of export controls. The European Union (EU), in May 2019, adopted Regulation 2019/452 establishing a framework for the screening of foreign direct investments (FDI) and subsequent guidance on implementation of the regulation in March 2020.[15] In November 2019, the Japanese Diet passed an amendment to their Foreign Exchange and Foreign Trade Act (FEFTA) introducing new, more stringent controls on foreign investment.[16] While most countries already have some form of controls on FDI, many have chosen to tighten these laws over the last several years. For years, the EU, individual EU member states, and other countries have also been analyzing groups of technologies to determine whether there is a basis for control in the multilateral export control regimes or on a state-level basis.[17]

14 See, for example, "EU Set to Tighten Rules on Foreign Investment to Fend Off China," *Bloomberg*, 19 November 2019.

15 "Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 Establishing a Framework for the Screening of Foreign Direct Investments into the Union," available at: https://eur-lex.europa.eu/eli/reg/2019/452/oj.

16 Sakon Kuramoto, Benjamin Miller, Hiroki Sugita, "Amendment to Japanese Foreign Exchange and Foreign Trade Act Regulations Expands Scope of "Restricted Businesses" to Include Some Information and Communications Technology Businesses," JD Supra, June 22, 2019, available at: https://www.jdsupra.com/legalnews/amendment-to-japanese-foreign-exchange-68547/.

17 For a full list of FDI legislation worldwide, see the Investment Policy Hub's website: https://investmentpolicy.unctad.org/investment-laws.

Using trade controls to manage the spread and use of new technologies is not an original development. A number of less than successful attempts have been made in the past, in the US and in other countries, to explore ways in which controls can be administered to new technologies that are still "emerging" to the extent that their potential military end-uses and/or risks are not yet concretely established.[18] Given that attempts to implement unilateral controls on new technologies in the US are ostensibly rooted in the aim of establishing new entries in the control lists of multilateral export control regimes, so far attempts to in fact do so have largely failed with regards to "new" technologies whose conventional or WMD end-use is not clear or directly tied to a security threat.

In 2013, the United Kingdom and France succeeded in passing a proposal in the Wassenaar Arrangement (WA), the export control regime dedicated to controlling conventional arms and dual-use goods and technologies, to control "intrusion software" and "IP network communications surveillance systems." As the US tried to implement the new controls nationally, vehement industry opposition via comments on a public notice of the new rules, lobbying, and letters forced the US to withdraw the controls it had proposed and implemented in its national legislation. The US then renegotiated the controls within the WA in 2017 resulting in many more exemptions and narrower control of such technology. The final controls on intrusion software in the WA thus include broad exemptions and narrower language. Much of the disagreement in the regime arose over the broadly non-military application of the subject technology.[19]

The case of additive manufacturing (AM) is another useful example. While the WA introduced a control on a specific type of AM production equipment: "directional-solidification or single-crystal additive manufacturing equipment for the production of gas turbine engine blades, vanes and tip shrouds, as well as the associated software," the control was introduced more to "ensure coverage of equivalent technologies to prevent substitution for other already controlled production equipment," as noted by Kelley and Brockmann in 2018.[20] Other attempts to introduce controls on AM production equipment in the Missile Technology Control Regime (MTCR) in 2014, and in the Nuclear Suppliers Group (NSG) in 2016, did not succeed.[21] While discussions continue

18 See, for example, Scott Jones and Kevin Wolf, "0Y521 and Section 1758: Emerging technologies by any other name?", *World Export Control Review*, Issue 89, May 2020.

19 Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research, *Lawfare*, 5 January 2018.

20 Brockmann and Kelley, *op. cit.*

21 Grant Christopher, "3D Printing: A Challenge to Nuclear Export Controls," *Strategic Trade Review*, Volume 1, Issue 1, 2017 and Kolja Brockmann and Sibylle Bauer, "3D Printing and Missile Technology Controls," *SIPRI Background Paper* November 2017.

in the various multilateral export control regimes about whether to introduce separate, specific controls on, for example, feedstock for AM machines or controls on technology transfer, regime members have not adopted new controls.

These two examples highlight the difficulty with introducing new controls on "emerging technologies" in both the national and multilateral context. This issue is key to consider in more depth as the dilemma of controlling technologies whose military end-use is uncertain, nor security threat and risk clearly established, contends with the very concept of "threat" and "security"—concepts that are at the crux of why certain materials, equipment, and technology are controlled at the multilateral level to begin with. Considering the interplay between "emerging" technologies and strategic trade controls therefore may magnify deeper conceptual lacunae in the nature, objectives, and use of controls in the modern security environment.[22] Are these technologies being controlled, indeed, to keep certain conventional weapons and WMD out of the hands of "bad" actors? Or are they being controlled with the aim of developing a monopoly on the development and use of certain technologies? While the expected and rather banal answer would be both, the answer as it appears to be forming from recent policy decisions over the last few years, at least in the US, could be the latter, the focus of which is to maintain economic advantage.

4 Emerging Technologies and the US Technology Control Regime

As part of the National Defense Authorization Act (NDAA) for Fiscal Year 2019, Congress enacted the ECRA of 2018. Section 1758 of ECRA instructs that:

> The President shall establish and, in coordination with the Secretary, the Secretary of Defense, the Secretary of Energy, the Secretary of State, and the heads of other Federal agencies as appropriate, lead, a regular, ongoing interagency process to identify *emerging* and *foundational* technolo-

22 The conceptual ambiguity surround emerging technologies is consistent with previous policy treatments of technology in general. Grissom summarizes the literature on social shaping of technology and its emphasis on the nature of technologies as: ultimately ideas that are shaped by discourse and competition with different views on the potential of a given technology . . . these interest groups (such as research teams, policymakers and investors) vie to superimpose their own vision on a developing technology by building a coalition around their vision, engaging in bureaucratic maneuvers to exclude other groups, and ensuring that important design and engineering choices reflect their vision for the technology." Grissom, A. (2006) "The future of military innovation studies," *Journal of Strategic Studies*, Vol. 29 (5), pp. 905–934.

> gies that—(A) are essential to the national security of the United States; and (B) are not critical technologies described in clauses (i) through (v) of section 721(a)(6)(A) of the Defense Production Act of 1950, as amended by section 1703.

The "critical technologies" not otherwise captured in the new designations include current military, nuclear and dual-use controls.[23]

In the context of the passage of ECRA, it is noteworthy that Congress had been unable to reauthorize the lapsed Export Administration Act (2001) to enact new dual-use export control legislation for nearly twenty-years.[24] The rapid techno-industrial rise of China—particularly its Made in China 2025 industrial policy—galvanized and concentrated collective Congressional attention sufficiently to dramatically reorient and merge US export and foreign direct investment controls.[25] The addition of emerging and foundational technologies strongly suggested that the extant military and dual-use lists were insufficient to safeguard US "national security" and assure military superiority.[26] Although ECRA does not define "national security," a request for

---

23 As defined in the NDAA, critical technologies consist of the following: "(a) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120–130). (b) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations (EAR) (15 CFR parts 730–774) and controlled: (1) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or (2) For reasons relating to regional stability or surreptitious listening. (c) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by 10 CFR part 810 (relating to assistance to foreign atomic energy activities). (d) Nuclear facilities, equipment, and material covered by 10 CFR part 110 (relating to export and import of nuclear equipment and material). (e) Select agents and toxins covered by 7 CFR part 331, 9 CFR part 121, or 42 CFR part 73. (f) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018."

24 See, Ian Fergusson and Paul Kerr, The U.S. Export Control System and the Export Control Reform Initiative, Congressional Research Service, March 2019, R41916.

25 In terms of investment controls, The NDAA included the Foreign Investment Risk Review Modernization Act (FIRRMA). FIRRMA reforms the Committee on Foreign Investment in the United States (CFIUS) process currently used to evaluate and address national security-related concerns related to foreign investment into the United States. FIRRMA's most substantial change was to the scope of "covered transaction," which defines much of CFIUS's jurisdiction, to include "critical technologies." As defined in ECRA, critical technologies include "emerging and foundational technologies."

26 The catalyzing effect of Chinese "Civil-Military Fusion" efforts cannot be underestimated. In particular, a seminal study, the "DIUx Report," analyzed the rapid rate at which the Chinese government sought to acquire and invest in "emerging technologies," while at the same

comment BIS published in November 2018 described the national security concerns to be addressed by the effort, i.e., to identify now uncontrolled items that "have potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications, or [that] could provide the United States with a qualitative military or intelligence advantage."[27] Nevertheless, emerging and foundational technologies, as categories, are defined neither in the NDAA, nor ANPRM.

The public responses to the ANPRM were predominantly negative, arguing that specific controls were not, in the main, practicable.[28] Complaints varied on a continuum regarding the US government's approach to defining emerging technologies, arguing that the government should have started with very specific technologies rather than working from general categories. In other words, the onus should be on the government to establish why and how a technology is a national security threat *a priori*, not the other way around. One commentator succinctly captured this dilemma in the ANPRM process:

> The ANPRM notes that, "Certain technologies, however, may not yet be listed on the CCL or controlled multilaterally because they are emerging technologies. As such, they have not yet been evaluated for their national security impacts." These two sentences are at the heart of the problem of defining emerging technology within an export control framework. The

noting "DoD does not currently have agreed-upon emerging technologies the U.S. must protect although there has been extensive work on export controls to protect technology products from being shipped to U.S. adversaries." Defense Innovation Unit Experimental (DIUx), 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," Updated with 2016 and 2017, January 2018, p. 15.

27 From a strategic perspective, addressing emerging technologies is certainly not new. To ensure that emerging technologies of concern were captured and appropriately controlled, the so-called 0Y521 process was established in 2012 "[A]s a mechanism for situations in which an item that warrants control is not controlled yet—e.g., as with an emerging technology—this rule proposes the addition of a new, miscellaneous Export Control Classification Numbers (ECCN) to the Commerce Control List (CCL)." See, Proposed Revisions to the Export Administration Regulations (EAR): Control of Items the President Determines No Longer Warrant Control Under the United States Munitions List (USML) A Proposed Rule by the Industry and Security Bureau on 07/15/2011 t.ly/KB9yr.

28 Scott A. Jones, "Regulating the future: Concerns over defining 'emerging technologies'," *World Export Control Review*, Issue 79, May 2019. See also, Robert Williams, "Protecting sensitive technologies without constricting their development," Brookings Institute, 30 November 2018. Williams, in particular, notes: "[O]ngoing advances in artificial intelligence and next-generation technologies create enormous definitional challenges in determining whether an emerging or foundational technology is essential to U.S. national security."

> uncertainties and ambiguities around emerging technology make them difficult if not impossible to govern from an export control perspective, and yet this is exactly what the process to be established through this ANPRM is tasked to do.[29]

Unlike the majority of current control list entries, the notional emerging technologies categories are not directly linked to military or other weapons systems. The traditional list making process is predicated on identification of weapons system first, from which the component parts and technologies are then identified and listed.[30] The current proposed identification process is a transgression against established methods. As of October 2020, this approach may explain why the US has to date failed to list any emerging technologies.

5 Conclusion: Circumscribe First, Export Control Later

In a 2018 report on the defense industrial base, the US Department of Defense observes that "The next generation of weapons will require advanced software, artificial intelligence, and machine learning, but traditional manufacturing processes continues to build the systems, platforms, and munitions that deliver kinetic effects. Both aspects of the industrial base are needed for long term economic growth and national security".[31] AI, to take one representative genre technology, is currently and increasingly will fuel further innovations across all social domains. However, we can only speculate as to *how* emerging technology will affect national security.[32] As such, we, by definition, cannot export control it.

---

29 "Comment for the Department of Commerce ANPRM on "Review of Controls on Certain Emerging Technologies"," Samuel Evans, Research Fellow in the Program on Science, Technology, and Society at Harvard University's Kennedy School of Government. Source: <t.ly/DE95l>.

30 In the early 1990s, the United States determined the that extant lists were insufficient. Under the Enhanced Proliferation Control Initiative (EPCI). The resulting "catch-all" provision was designed to supplement list-based controls by licensing unlisted commodities destined for weapons of mass destruction (WMD) development. Although now firmly part of the export control canon, the practice of catch-all controls proved to be challenging for both government and industry. Bright, shining list entries were still the preferred medium.

31 Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806 September 2018, p. 26.

32 The bourgeoning literature on national security and AI is voluminous. A sample reader with representative citations is found in *Artificial Intelligence and National Security*, Congressional Research Service, 21 November 2019, R45178.

In this context, the more meaningful question to pose concerns the process by which we manage technology as a function of, and *defined* by, national security. The conceptual challenges presented by the current illustrative emerging technologies lists concerns our erstwhile national security categories. The associated control mechanisms—primarily export controls—were predicated on clearly defined threats and, ideally, an attendant assessment on control viability (e.g., foreign availability analyses).[33] In particular, the current national security discourse is tendentiously fixated on a perceived "innovation gap," one that can be managed through the traditional technology control policies and procedures.[34] The current "Revolution in Military Affairs" moment is narratively contiguous with its various predecessors, focused as they were on technology-driven military disruptions.[35]

33 For example, a recent report on emerging technologies and WMD notes similarly: "In the absence of new ideas for governance to counter threats posed by the interaction of emerging technologies with WMD, it is tempting to apply the same types of governance or control mechanisms used in the past for preventing proliferation of WMD and other advanced military technologies. However, this strategy is not only doomed to fail, but it will also damage the U.S. position as a market leader and place significant restraints on what are vital engines of the future U.S. economy. For this reason, policymakers need to move beyond notions of control and consider a paradigm shift in how they view the threat of WMD, how they counter threats posed by WMD, and possibly how they define WMD itself." Natasha Bajema, "WMD in the Digital Age: Understanding the Impact of Emerging Technologies," *Research Paper No. 4*, Center for the Study of WMD, October 2018.

34 Military "gaps" have figured prominently in U.S. strategic thinking for decades. As one analyst recently observed, "As the defense community 60 years ago talked of a "bomber gap" followed by a "missile gap" between the United States and the Soviet Union, it 10 years ago discussed a "transformation gap" between America and European allies in NATO. Now it speaks of an "innovation gap" between the United States and its competitors, notably China. This gap exists because Chinese investments in technological innovation and manufacturing are catching up with American investments; in addition, Chinese investments are made much more strategically. In this way, the agendas on revolutionary technology and innovation join together." Laura Schousboe, "The Pitfalls of Writing About Revolutionary Defense Technology," *War on the Rocks*, 15 July 2019. See, also James Manyika and William H. McRaven, Chairs Adam Segal, "Keeping Our Edge: Innovation and National Security," Independent Task Force Report No. 77, Council on Foreign Relations, 2019.

35 Christian Brose, "The New Revolution in Military Affairs: War's Sci-Fi Future, *Foreign Affairs*, May/June 2019. See also, Department of Defense, "Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Advantage" (2018), p. 3. In particular, the strategy highlights rapid advances in advanced computing, big data analytics, artificial intelligence (AI), autonomy, robotics, directed energy, hypersonics, and biotechnology, which are characterized as "the very technologies that ensure we will be able to fight and win the wars of the future."

The present-day global commercial environment and R&D ecosystem is a profound countervailing force that radically undermines the proposed solution set: export controls.[36] As such, any meaningful control effort will require multilateral definitional and procedural support, a highly unlikely prospect given the current US unilateral turn and important commercial applications of the concerned technologies. Indeed, the current trend of merging of investment and export controls suggests that controlling technology will require not only an institutional but conceptual restructuring of the concept "national security." Lastly, the control imperative will require need modes of technology governance. As one analyst observed, "[t]oday's technological advances are deemed disruptive not only in market terms but also in the sense that they are provoking disruptions of legal and regulatory orders and have the potential to disturb the deep values upon which the legitimacy of existing social orders rests and on which accepted legal and regulatory frameworks draw."[37] The emerging governance model must necessarily reconcile the inherent limitations of export controls with the economic and political realities of accelerating technology diffusion and global supply chains.

36 See, for example, Stephen Ezell and Caleb Foote, "How Stringent Export Controls on Emerging Technologies Would Harm the U.S. Economy," 20 May 2019, Information Technology and Innovation Foundation.

37 Camino Kavanagh, "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?" Carnegie Endowment for International Peace, August 2019.