Disrupting Export Controls: "Emerging and Foundational Technologies" and Next Generation Controls

SCOTT JONES[1]

Abstract

The U.S. export control system underwent a major reform beginning in 2010 in response to rapidly changing global political and economic dynamics. Although significant, the reform was administrative in effect only, as the underlying legal edifice, the Export Administration Act of 1979, was still formally lapsed. The recent and meteoric rise of China as a near-term technology competitor galvanized Congress to enact a new export control law and complementary foreign direct investment amendments. The focus of these efforts concern developing controls over so-called "emerging and foundational technologies," that confer and advance U.S. military superiority and vouchsafe national security. The U.S. has launched similar campaigns before in response to perceived risks to its technological preeminence. In 1979, the U.S. government created the Military Critical Technologies Program (MCTP), the goal of which was to identify and develop control strategies for emerging technology. By all accounts, the MCTP failed on conceptual and, therefore, practical grounds. This article reviews the MCTP in light of the current definitional and practical challenges posed by emerging and foundational technologies.

Keywords

Export controls, emerging technologies, technology, governance, trade, innovation, technonationalism, geoeconomics

Introduction

After nearly twenty years in legal abeyance, the Export Administration Act of 1979 (EAA, as amended) was repealed and permanently replaced by the National Defense Authorization

1 Dr. Scott Jones is a Non-Resident Fellow at the Henry L. Stimson Center, Affiliated Expert at CRDF Global, and Principal at TradeSecure, LLC.

Act of 2018 (NDAA) – specifically by the Export Control Reform Act (ECRA). During that twenty-year period, Congress was unable to effectively orient and calibrate U.S. dual-use export controls against a diverse array of threats – terrorism, "rogue states," and emerging powers – and ensure economic vitality through robust exports through revised legislation. The EAA lapsed in 2001, a momentous year for both trade and security, the same year Al Qaeda spectacularly attacked the United States and China joined the World Trade Organization (WTO).

The EAA was designed to address the Soviet and associated communist world military threat. The events of 9/11 and increasing concern with the proliferation of Weapons of Mass Destruction (WMD) taxed both worldviews and the associated mechanisms of technology control, the effect of which was conceptual paralysis. Described very simply, rising China, a technologically-empowered China specifically, crystallized and consolidated the new rationale for U.S. export controls and, as a novel development, foreign direct investment (FDI). The specific nexus linking export controls and FDI is the bourgeoning effort to identify and control "emerging and foundational technologies (EFT)." While the legacy export control concerns and controls remain intact (e.g., WMD and military items), the U.S. technology control complex is now charged with defining and expanding the scope of controls.[2]

The unique characteristics of the current technology control effort are unprecedented insofar as the vague unease over EFT acquisition is not predicated upon an unambiguously defined weapons taxonomy. In other words, EFT control list entries are in want of a weapon(s) and not the other way around. The current U.S. and multilateral military and dual-use control lists are based either on weapons systems or the components thereof. Artificial intelligence (AI) is neither a weapon nor a clearly defined component in current WMD or military stocks. AI military applications are, at this time, purely speculative or, if in beta, hypothetical and part of the associated technology hype cycle.[3] The proposed terms of art are likewise ambiguous and, as presented in the NDAA of 2018, essentially meaningless.

As during the Cold War, the U.S. struggled internally and with its allies on scoping control lists. This time, however, the undertaking is different in form and context. China is not the Soviet Union, however aggressively the current strategic narrative contends otherwise. While always concerned about the Peoples Liberation Army (PLA) reaching or surpassing strategic parity with the U.S. military, the United States is now equally, if not more so, alarmed by China's "innovative capabilities" of deploying new technologies not otherwise already incorporated

---

2 The Technology Control Complex is here used to refer to the collection of regulations and associated agencies tasked with identifying and protecting U.S.-origin critical technology from unlawful acquisition. A representative list of programs can be found in General Accountability Office (GAO), "Critical Technologies: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed," GAO-15-288, February 2015, pp. 4-5. See also, GAO, "High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas," March 2019.

3 In a recent report on Chinese innovation, the authors note, "China is making more rapid progress in innovation and advanced technology industries than the United States. There is no reason to believe this progress will slack over the next decade, particularly if China continues its commitment to Made in China 2025." See Robert D. Atkinson and Caleb Foote, "Is China Catching Up to the United States in Innovation?," Information Technology and Innovation Foundation, April 8, 2019, p. 50. See also Lee Yuan, "ZTE's Near Collapse May Be China's Sputnik Moment," *The New York Times*, June 10, 2018.

into existing or new defense systems.[4] The announcement of Made in China 2025 resulted in a paradigm shift in how war-planners and security officials define military superiority.

In historical context, the current conceptual crisis is not unique. Since the enactment of the Export Control Act of 1949, the U.S. TCC has witnessed similar inflection points. The last major reckoning occurred in 1976 culminating in the passage of the 1979 EAA, the recent termination of which seeded the EFT issue. The debates and resulting policies of that period can shed light on the current framing and definitional efforts. They can also reveal the necessary limits of traditional control approaches, particularly at the multilateral level.

This article will review the strategic environment that led to the creation of the Military Critical Technology Program (MCTP) in 1979, giving rise to the Critical Technology Approach to defining export control parameters. The subsequent sections will analyze the impact of this approach on how the United States managed rapid and globalizing technological changes. The concluding section speculates on possible lessons to be drawn from earlier efforts to delineate boundary conditions for "new" technologies and associated control mechanisms.

"The Release of Know-How is an Irreversible Decision:" The Bucy Report and EAA of 1979[5]

The modern U.S. export control system began with the enactment of the *Export Control Act of 1949* (ECA) and the establishment of the Coordinating Committee on Multilateral Export Controls (COCOM) that same year.[6] The singular focus of both systems was to curtail Soviet and Chinese Communist acquisition of military, nuclear, and dual-use items and technologies

4 In a recent report on Chinese innovation, the authors note, "China is making more rapid progress in innovation and advanced technology industries than the United States. There is no reason to believe this progress will slack over the next decade, particularly if China continues its commitment to Made in China 2025." See, Robert D. Atkinson and Caleb Foote, "Is China Catching Up to the United States in Innovation?" Information Technology and Innovation Foundation, April 8, 2019, p. 50. See also Lee Yuan, "ZTE's Near Collapse May Be China's Sputnik Moment," *The New York Time*s, June 10, 2018.

5 Defense Technical Information Center, A Report of the Defense Science Board Task Force on Export of U.S. Technology, "An Analysis of Export Control of U.S. Technology - A DOD Perspective," February 4, 1976, p. vi.

6 The ECA was preceded by the *Export Control Act of 1940* which authorized the President to license or prohibit the export of "essential defense materials." The ECA of 1949, however, was the first peacetime export control regime and amended in 1951, 1953, 1956, 1958, 1960, 1962, and 1965. While the short supply ethos of the earlier Act animated the 1949 Act, national security became the dominant rationale. As regards the ECA of 1949, "[p]robably no single piece of legislation gives more power to the President to control American commerce." Harold J. Berman and John R. Garson, "United States Export Controls—Past, Present, and Future," *Columbia Law Review,* Vol. 67, No. 5 (May 1967), pp. 791–890 as quoted in Richard T. Cupitt, *Reluctant Champions: U.S. Presidential Policy and Strategic Export Controls* (Routledge: New York, 2000).

that could be used to advance their respective military capabilities.[7] The initial list structure for both U.S. and multilateral systems was exact, save for the inclusion of additional items on the lists (e.g., unilateral controls). The size and content of the control lists were subjects of constant debate within the U.S. and between NATO allies, a characteristic that persists into current export control deliberations.[8] Arguably, the less complicated and relatively static parts of the lists – nuclear and directly military-related items – were uncontroversial. The bourgeoning dual-use list, by its very nature, roiled consensus-building efforts on establishing control parameters.[9]

During the late 1960s, a number of factors dramatically affected the scope and practice of U.S. export controls. U.S. Soviet bloc policy underwent a period of moderation, resulting in closer economic and political ties with the Warsaw Pact states. For example, in May 1972, President Richard Nixon visited Secretary General of the Soviet Communist party, Leonid I. Brezhnev, in Moscow, becoming the first U.S. president to do so. A few months earlier, Nixon met with Mao Zedong in Beijing. At the same time, Washington recognized and fostered the increasing importance of trade to the U.S. economy.[10] Lastly, with the rapid economic development of European and East Asian economies, the U.S. lost much of its enforcement leverage over the practice of multilateral export controls through the Mutual Defense Assistance Control Act (the Battle Act).[11]

In response to these strategic and technological changes, the U.S. revised its dual-use export control system in 1969 with the authorization of the *Export Administration Act* (EAA), which

---

7 As an adjunct to COCOM and in response to Chinese involvement in the Korean War, the United State petitioned for the creation of a separate committee, CHINCOM, to multilaterally control exports to communist China in 1952. Export controls by CHINCOM were considerably more restrictive and corresponding lists more expansive than controls by COCOM, which became known as the "China Differential." In 1957, however, the U.S. allies formally incorporated CHINCOM into COCOM. For more information on CHINCOM, see, among others, Frank Cain, "The US-Led Trade Embargo on China: The Origins of CHINCOM, 1947–1952," *Journal of Strategic Studies*, Vol. 18 (1995), pp. 33–54 and Hugo Meijer, *Trading with the Enemy: The Making of U.S. Export Control Policy toward the People's Republic of China* (Oxford: Oxford University Press, 2016).

8 The dynamic nature of export controls figured prominently in policy tensions between the U.S. Executive and Legislative branches. The complex policy interplay between control list parameters and associated policy guidelines also extended to debates within and between Executive agencies. The canonical review of this export control "policy entrepreneurism" can be found in Richard T. Cupitt, *Reluctant Champions: U.S. Presidential Policy and Strategic Export Controls* (Routledge: New York, 2000).

9 Michael Mastanduno, "*Economic Containment: CoCom and the Politics of East-West Trade*," (Ithaca: Cornell University Press, 1992). See also Major Rand Lewis, "COCOM: An International Attempt to Control Technology," *Defense Institute of Security Assistance Management (DISAM) Journal*, Vol. 13, Issue 1 (Fall 1990), pp.66-73

10 See, for example, William Branson and Helen Junz, "Trends in U.S. Trade and Comparative Advantage," Board of Governors of the Federal Reserve System Brookings Papers on Economic Activity, Number 2, 1971.

11 The Battle Act was designed to ensure a U.S.-centric interpretation of COCOM through the denial of foreign aid to countries that exported strategic items to the communist bloc.

was significantly amended in 1979.[12] The EAA of 1969 was a significant departure from the earlier system, one largely based on an "economic warfare" model.[13] The 1969 Act authorized the Secretary of Commerce to fundamentally restructure and reduce the control list (Commodity Control List) and streamline associated licensing procedures. Regarding the former, the list pruning was predicated on retaining only items of "military significance."[14] In addition, the EAA of 1969 included the first statutory provisions requiring that foreign availability be taken into account in licensing determinations.[15]

In 1977, the EAA was further amended to capture the increasing nuance in U.S. foreign policy with the Communist Bloc countries.[16] The erstwhile binary Communist/Non-Communist export control distinction was discarded for a policy comity model in which, for example, states like Yugoslavia were treated differently from the Soviet Union in terms of export control policy.[17] In 1981, China would be accorded this dispensation.

The various EAA amendments throughout the 1970s culminated in the passage of a new export control act, the EAA of 1979.[18] Like the 1969 Act, the EAA continued to emphasize the importance of trade noting that export controls should only be imposed "to the extent necessary...to restrict the export of goods and technology which would make a significant contribution to the military potential of any other country or combination of countries which

---

12 As is evident in the titular change from the Export Control Act of 1949, the control footing was shifting from control to administration, a deliberate alteration to reflect the increasing commercial pressures of détente, a stalling U.S. economy, and declining leverage of the earlier Battle Act approach to ensuring allied consensus on East-West trade controls. Prior the 1979 revision, the EAA was amended in 1972, 1974, and 1977. See Stuart Macdonald, *Technology and the Tyranny of Export Controls: Whisper Who Dares* (London: Macmillan, 1990) and Ed Zschau, "Export Controls and America's Competitive Challenge," *High Technology Law Journal*, Vol. 1, No. 1 (1986), pp. 1-25.

13 Richard T. Cupitt, *Reluctant Champions: U.S. Presidential Policy and Strategic Export Controls, Truman, Eisenhower, Bush, and Clinton* (Routledge: New York, 2000), p. 117.

14 See "Trade and Technology: Hearing before the Subcommittee on International Finance of the Committee on Banking, Housing, and Urban Affairs," Ninety-Sixth Congress, United States Senate. First session. United States Committee on Banking, Housing, and Urban Affairs, Subcommittee on International Finance, January 1, 1980.

15 Export Administration Act of 1969, Pub. L. No. 91-184 at § 2(1), 4(b), 83 Stat. at 841, 842-43. The foreign availability concept as a matter of law was further articulated in the 1972 Equal Export Opportunity Act (EEOO). The EEOA also provided a means by which to assess foreign availability by the creation of various Technological Advisory Committees (TACs).

16 The 1977 Amendment was also noteworthy in that, for the first time, companies engaging in the transfer of technological data were required to report their activities to the Department of Commerce. Export Administration Amendments of 1977, Pub. L. No. 95-52, § 103(a)(3), 91 Stat. 235, 236.

17 As noted in the Amendment, "In administering export controls for national security purposes ... United States policy toward individual countries shall not be determined exclusively on the basis of a country's communist or non-communist status but shall take into account such factors as the country's present and potential relationship to the United States..." Export Administration Amendments of 1977, Pub. L. No. 95-52, § 103(a)(3), 91 Stat. 235, 236 (amending 50 U.S.C. app. § 2403(b)(2)(A)).

18 Also during this period, the U.S. revised its defense export control system. The *Arms Export Control Act of 1979* (AECA) came into being under a different title, the *Foreign Military Sales Act of 1968* (FMSA). Before 1968, foreign military sales were conducted under the authority of the *Foreign Assistance Act of 1961* (FAA).

would prove detrimental to the national security of the United States."[19] The 1979 Act also introduced the concept of "critical technologies" into the law for the first time.

The "Critical Technology Approach"

The critical technology approach emerged from a 1976 Defense Science Board Task Force on Export of U.S. Technology report, "An Analysis of Export Control of U.S. Technology: A DOD Perspective," chaired by Fred Bucy, Chairman of Texas Instruments.[20] The so-called "Bucy Report" represented a radical departure from contemporary export control concepts which focused primarily on material control. In defining "critical technologies," the Bucy Report established guidelines that: (1) advocate the control of design and manufacturing know-how, as opposed to finished products; (2) concentrate on "active" transfers (e.g., transfers of technology in which the interaction between East and West may be most intense, as opposed to "passive" transfers); and (3) focus on technology that represents a "revolutionary" as opposed to an "evolutionary" advance to the receiving nation.

While the 1969 Act, for the first time, captured the intangible dimension of export controls by circumscribing "data and technical information" transfers, it was not until the Bucy Report that U.S. export control officials reckoned with "technology," and, more specifically, with technology that was "critical" to U.S. military superiority.[21] As Bucy noted, "The control of design and manufacturing know-how is absolutely vital to the maintenance of U.S. technological superiority. All other considerations are of secondary importance."[22]

Throughout the late 1960s and early 1970s, U.S. officials gradually recognized the decline in U.S. high technology dominance, as noted in the foreign availability provision in the EAA of

---

19 Export Administration Act of 1979, Pub. L. No. 96-72, 93 Stat. 503 (codified at 50 U.S.C. app. §§ 2401-2420 (1982)), § 2402(2).

20 A Report of the Defense Science Board Task Force on Export of U.S. Technology, "An Analysis of Export Control of U.S. Technology - A DOD Perspective" (1976) reprinted in Transfer of Technology and the Dresser Industries Export Licensing Actions: Hearing Before the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs, 95th Congress, 2nd Session, 1978, pp. 33-89. The task force was chaired by J. Fred Bucy, executive vice-president of Texas Instruments.

21 Stuart McDonald observed that "Now, to Fred Bucy, with his background in semiconductors, a field in which the intangible is infinitely more important in innovation than the tangible, the significance of information must have been so obvious as scarcely to warrant the assertion. Yet, it had never been terribly clear whether export controls did extend to know-how. Certainly the Export Administration Act of 1969 had bestowed authority to control data and technical information, but virtually all practical interest had been in the control of exports of equipment - and in the era of detente even this emphasis had been distinctly muted. In stating what is really no more than a truism from which there can be no convincing dissent, Bucy was unwittingly opening a can whose worms are wriggling furiously more than a decade later." Stuart McDonald, *Technology and the Tyranny of Export Controls: Whisper Who Dares* (London: Macmillan, 1990), p. 65.

22 A Report of the Defense Science Board Task Force on Export of U.S. Technology, "An Analysis of Export Control of U.S. Technology - A DOD Perspective" (1976) reprinted in Transfer of Technology and the Dresser Industries Export Licensing Actions: Hearing Before the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs, 95th Congress, 2nd Session, 1978, pp. 33-89.

1969. The Bucy Report, however, forcefully defined the nature of that erosion by differentiating between consequential ("revolutionary") and mundane ("evolutionary") technology and where the U.S. led in the former. The new terms of art – revolutionary and evolutionary technology – would be the basis upon which the Commodity Control List was organized and, correspondingly, licensing decisions determined.[23]

The ultimate recommendation of the Bucy Report concerned refocusing U.S. controls on "high-velocity strategic technologies" rather than on all but the most sensitive dual-use products. As noted by Assistant Secretary of Defense for Global Strategic Affairs, Richard Perle:

> *"The Bucy report made an important breakthrough in the U.S. approach to the problem. It placed the focus on the exporting of know-how and certain keystone technologies, not products. Bucy's approach reshaped American thinking about the definition of technology, and it has led to important revisions in the categories."*[24]

As further elaborated in the report, the identification, designations, and control of "critical technology" would be vested in the Department of Defense with "Knowledgeable individuals from both government and the private sector contributing to the development of the following information for selected technologies on an ongoing basis: identification of strategic technologies and their impact on strategic missions; identification of key elements of critical technologies; and tracking their rate of advance critical infrastructure requirements including key manufacturing."[25]

The unflattering portrait of the U.S. export control system presented by the Bucy Report suggested that the then current list-based embargo approach was both economically and strategically misaligned with the rapidly changing political and economic environment. The recommended solution would materialize in the enactment of the 1979 Export Administration Act in a form very much in line with Bucy's recommendation. Ironically, this same vehicle – created to identify "critical technologies" – would formally lapse with the authorization of the Export Control Reform Act of 2018 (ECRA).

---

23 For example, the Report argues that "to preserve strategic U.S. lead time, export should be denied if a technology represents a revolutionary advance to the receiving nation, but could be approved if it represents only an evolutionary advance," Ibid.

24 Richard Perle, "The Eastward Technology Flow: A Plan of Common Action," *Strategic Review* (Spring 1984), p. 29.

25 The Report was especially critical of the absence of control metrics, noting that the licensing process was thoughtlessly extreme: "Although the number of items on the list has been reduced over the past three years— it is still too long— and U.S. companies still encounter frustration in trying to obtain validated licenses for high-technology product shipments to Communist countries … Of special concern is that there does not appear to be selective prioritization of effort in screening the various classes of technology export. The administration of export control appears to place equal emphasis on all requests, whether they be for product sales or the more active mechanisms of technology transfer," in A Report of the Defense Science Board Task Force on Export of U.S. Technology, "An Analysis of Export Control of U.S. Technology - A DOD Perspective" (1976) reprinted in Transfer of Technology and the Dresser Industries Export Licensing Actions: Hearing Before the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs, 95th Congress, 2nd Session, 1978, p. 28.

"It has Become More and More Difficult to Distinguish Dual-use Technology From Single-use Technology": The Military Technology Control Program (MTCP)[26]

The EAA of 1979 formally introduced the concept of "critical technologies" into the export control lexicon. The critical technologies approach, which grew out of the Bucy Report of 1976, focuses on controlling the export of dual-use technologies rather than end products. The EAA of 1979 required that the Secretary of Defense develop a list of "militarily critical technologies" and that the Secretaries of Commerce and Defense would "integrate items on the list of militarily critical technologies into the control list (Commerce Control List)."[27] The resulting streamlined dual-use list would have the simultaneous virtue of economic and national security efficacy by reorienting U.S. controls on, and only on, strategic technology and "keystone equipment" unique to the U.S. The EAA further instructed that the truncated list should inform multilateral controls.[28]

In response to the EAA provision, the Department of Defense (DOD) established the Militarily Critical Technologies Program in 1980.[29] The MCTP sought to provide an ongoing and systematic identification, assessment, and analysis of goods and technologies that: 1) are mature and critical to the U.S. military (the Militarily Critical Technologies List (MCTL)); and 2) are developing and could improve military capabilities once mature (the Developing Science and Technologies List (DSTL)). The MCTP delegated list development to the Institute for Defense Analyses (IDA), which created a Technical Working Group (TWG) system to generate and update the lists. The average yearly budget for the MCTP was approximately $2 million USD.[30]

The lists were based on a common set of 20 categories, the difference between lists designated in terms of timeframe (see Table 1 and Figure 1).[31] Each TWG, composed of academic, defense,

---

26 The quote continues: "There are almost no militarily significant technologies which do not also have important peaceful uses. Indeed, in the highly industrialized modern world, while arms and ammunition can still be identified, the distinction between implements of war and peaceful goods as well as the technologies for their manufacture has become so blurred that whether an item is a sword or a plowshare depends today not so much on how it is made but on how and by whom it is used ... So common is this dual-use characteristic that it is almost impossible to draw up a list of items, whether goods or technology, whose embargo will inhibit weapons development without including some items whose embargo will also inhibit (the) peaceful trade activity." in "East-West Technology Transfer: A Congressional Dialog with the Reagan Administration," A Dialog Prepared for the Use of the Joint Economic Committee of the United States 39-387, December 19, 1984, p. 83.

27 The Export Administration Amendments Act of 1985, Pub. L. No. 99-64, § 106(a)(2), 99 Stat. 120, pp. 128-29 (amending 50 U.S.C. app. § 2404(d)), amended the procedures for integrating the two lists. The Act requires that a foreign availability test be applied to items restricted by the MCTL before it is integrated into the CCL.

28 The Export Administration Amendments Act of 1985, Pub. L. No. 99-64, § 106(a)(2), 99 Stat. 120, p. 15.

29 Program oversight is provided by Office of International Technology Security.

30 "Defense Technology: DOD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions," July 2006, GAO-06-793, p. 4.

31 The MCTL was divided into three parts: Parts One and Two addressed weapon system technologies and Weapons of Mass Destruction, while Part Three focused on Critical Development Technologies (CDT).

and industry experts, identifies militarily *critical technologies* and the parameters at which they are critical, based on definitions of what is militarily critical established by the Export Administration Act.[32] As defined by the MCTL, "critical technologies" are those which "when fully developed and incorporated into a military system will produce increasingly superior performance or maintain a superior capability more affordably."[33] Since 1980, the MCTL and DSTL were truncated and select categories combined.

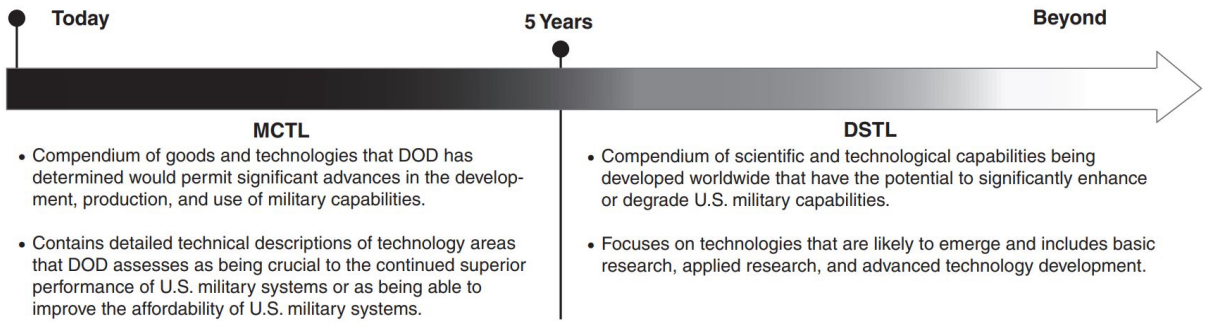

Figure 1. MCTL and DSTL Schematic (Source: Government Accountability Office)

Aeronautics technology	Lasers and optics technology
Armament and energetic technology	Manufacturing and fabrication technology
Biological technology	Marine systems technology
Biomedical technology	Materials and processes
Chemical technology	Nuclear technology
Directed and kinetic energy technology	Positioning, navigation, and time technology
Energy systems technology	Information security
Electronics technology	Signature control technology
Ground combat systems technology	Space systems technology
Information systems technology	Weapons effects technology

Figure 2. MCTL and DSTL Categories

32 The EAA established a process for the Secretary of Defense to identify "militarily critical goods"and technologies that should be considered by the Secretary of Commerce for inclusion on the Commerce Control List. To identify critical technologies, the DOD is required to consider (1) arrays of design and manufacturing knowhow; (2) keystone manufacturing, inspection, and test equipment; (3) goods accompanied by sophisticated operation, application, or maintenance know-how; and (4) keystone equipment which would reveal or give insight into the design and manufacture of a U.S. military system. See, "Defense Technology: DOD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions," July 2006, GAO-06-793, p. 5.

33 Office of the Under Secretary of Defense for Acquisition and Technology, The Militarily Critical Technologies List, February 1998, accessed at The Federation of American Scientists, <https://fas.org/irp/threat/mctl98-2/mctl98-2.pdf>.

The MCTL and DSTL were expressly not intended to become *de facto* control lists, but, instead, were to inform licensing decisions, inform counterintelligence efforts, and contribute content to the Commerce Control List (CCL) and, at that time, to the COCOM lists.[34] Since its inception in 1980, the MCTP failed to generate consistently updated and, according to designated U.S. government consumers, relevant lists. In a series of assessments, the Government Accountability Office (GAO) determined that the MCTL and DSTL were essentially useless. For example, a 2013 GAO report noted, "The MCTL is not used to inform export decisions — its original purpose. Export control officials from DOD and the Departments of Commerce and State reiterated their longstanding concern that the MCTL is outdated and too broad to meet export control needs."[35]

Bequeathed by the Bucy Report, the MCTL process was intended to identify and therefore control only the most militarily significant items in terms of current and future inventories. After the establishment of the MCTP, it quickly became apparent that the resulting MCTL and DSTL could not meet their objectives for conceptual rather than technical reasons. For example, a 1987 National Academy of Sciences report on U.S. exports controls noted that "the Bucy criteria have strong theoretical appeal but have proven extremely difficult to put into operation. They rely on distinctions — "critical," "revolutionary," ''keystone"— on which opinions are widely variable and difficult to reconcile."[36] Similarly, the GAO highlighted the conceptual challenges inherent in the MTCL process: "[A]ccording to DOD and Institute for Defense Analyses officials, it is challenging to determine the parameter at which a particular technology becomes militarily critical and is therefore subject to interpretation by the working group."[37]

---

34 The MCTL was never integrated into the Commodity Control List (CCL) as directed by the EAA. The Export Administration Amendments Act of 1985, Pub. L. No. 99-64, § 106(a)(2), 99 Stat. 120, pp. 128-29 (amending 50 U.S.C. app. § 2404(d)), amended the procedures for integrating the two lists. The Act requires that a foreign availability test be applied to items restricted by the MCTL before it is integrated into the CCL.

35 Protecting Defense Technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List Report to Congressional Committees, January 2013, GAO-13-157, p. 1.

36 Committee on Science, Engineering, and Public Policy; National Academy of Sciences, National Academy of Engineering, Institute of Medicine; "Balancing the National Interest: U.S. National Security Export Controls and Global Economic Competition,"Panel on the Impact of National Security Controls on International Technology Transfer, 1987, p. 129. As noted in the GAO (2006) report, "Reviewers were unsure how to interpret "militarily critical" when reviewing the proposed updates and therefore did not know how to comment." The absence of a clearly delineated taxonomy and associated parameters was not due to a failure of leadership or dedicated resources, but to the inherently subjective nature of the identification process. "Defense Technology: DOD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions," July 2006, GAO-06-793, p. 7.

37 Ibid., p. 6. Interestingly, Bucy later criticized the MCTL effort as overly bureaucratic: "The MCTL is the size of the New York phone book and worth a lot less. It's a bastardization of the concept of critical technology. The bureaucrats have taken a clear concept and turned it into a two-inch document that's absolutely worthless." Fred Bucy as quoted in Willie Schatz, "The Hitch in High-Tech Trade," *Datamation*, Vol. 29 (October 1983,) pp. 148-59.

Over time, the MTCL categories were increasingly neglected and lapsed, largely in tandem with decreasing annual budgets for the MCTP.[38] The central challenge, identifying and circumscribing controls for emerging technology, proved insurmountable in practice. Until the MCTL, control lists were the only means by which items were identified and defined. Unlike the MCTL outside of the weapons systems categories (e.g., ground combat systems technology), the defense (i.e., the United State Munitions List) and dual-use (ie., CCL) lists were developed from pre-existing weapons systems. Nevertheless, the need to identify "emerging" critical technologies remained acute.[39]

Parallel to the MCTP, other agencies developed similar "emerging technologies" identification projects. In the mid-1980s, the Defense Technology Security Administration (DTSA) developed a "Top Ten" list in lieu of the DSTL designed to help the DOD identify "paradigm-shifting technologies" on or approaching the horizon to provide a basis for defense proposals on how these technologies should be controlled and to inform decisions on how they may benefit the military. Similarly, the U.S. Army and Navy maintain technology centers worldwide to monitor and assess research efforts of foreign governments and industries to both inform science and technology planning and identify "rapidly evolving" or "breakthrough" technologies.[40] Although informed by the MCTP lists, these associated efforts were siloed and suffered the same concept of operations limitations.

More recently, the Defense Security Service (DSS) developed the Industrial Base Technology List (IBTL), a 25-category compendium of the science and technology capabilities under development worldwide that have the potential to significantly enhance or degrade U.S. military capabilities in the future. The IBTL categories are "correlated with legacy Military Critical Technology List (MCTL) categories."[41] Specifically, the DSS uses the IBTL to assess

38 The MTCL was last revised in 2011, although the DOD was statutorily required to maintain the list. Paul Roberts, "Funding Cut, Military's List of Critical Defense Technologies Languishes," *The Security Ledger*, January 25, 2013.

39 See, Steven D. Overly, "Regulation of Critical Technologies under the Export Administration Act of 1979 and the Proposed Export Administration Amendments of 1983: American Business Versus National Security," *Journal of International Law and Commerce*, Vol. 423 (1985).

40 "Defense Technology: DOD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions," July 2006, GAO-06-793, p. 15.

41 "To organize its targeting analysis, DSS applies a system of categories and subcategories that identify and describe technologies. In FY13, DSS ceased analyzing foreign interest in U.S. defense technology in terms of the 20 sectors of the Militarily Critical Technologies List (MCTL), shifting instead to the 29 sectors of the Industrial Base Technology List (IBTL). The newer system updates the categorization scheme to incorporate emergent and cutting-edge technologies. "Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting," Defense Security Service, 2014, p. 6.

foreign acquisition efforts of key U.S. technologies.[42]

Materials, Raw & Processed	Ground Systems
Electronics	Armaments & Survivability
Manufacturing Equipment & Processes	Energy Systems & Energetics
Lasers	Nuclear
Directed Energy	Biological
Optics	Chemical
Sensors (Acoustic)	Emerging Technology
Positioning, Navigation, Timing	Agricultural
Radars	Medical
Signature Control	C4 Systems
Aeronautic Systems	Software
Space Systems	Services & Other Products
Marine Systems	

Figure 3. Industrial Base Technology List (IBTL)

Other agencies likewise developed new emerging technologies identification processes. For example, to address controls on emerging technologies, in 2012 the Department of Commerce Bureau of Industry and Security (BIS) developed the 0Y521 series, composed of 0A521 for hardware, 0B521 for test equipment, 0C521 for materials, 0D521 for software, and 0E521 for technology and is described in a supplement to the Commerce Control List (CCL). BIS will designate an item as included in ECCN 0Y521 based on whether the item has either (a) "significant military or intelligence advantage to the United States" or (b) for "foreign policy reasons." The determination will not be based on "a classification of the item's technical

42 The GAO criticized DSS for developing another critical technologies list: "Faced with difficulty in finding a suitable alternative to the MCTL that sufficiently meets its needs, DSS now plans to develop its own technology reference. Such an undertaking will be time consuming and diverts resources from other missions." Protecting Defense Technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List Report to Congressional Committees, January 2013, GAO-13-157, p. 17. See also, Congressional Research Service, "Defense Primer: Emerging Technologies, October 23, 2019 and Christopher A. Bidwell, JD & Bruce W. MacDonald, "Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security," Federation of American Scientists, September 2018.

characteristics."[43] To date, only three 0Y521 entries have been registered.[44]

Maintaining the Technological Edge

As understood during the Cold War, "military superiority" was a concept relative to the Communist Bloc countries and to the Soviet Union in particular. Military superiority was also predicated on conventional weapons as opposed to Weapons of Mass Destruction (WMD), a distinction codified in law and in conceptual practice.[45] Indeed, with the exception of the Atomic List, COCOM controls were almost entirely focused on conventional weapons items and technologies.[46] With the end of the Cold War, the primacy of military superiority as the *raison d'etre* of export control policy became diffuse and subordinate to nonproliferation. As Richard Cupitt observes:

> *"In the summer of 1990, the United States finally appeared ready to abandon anti-Soviet containment as the basis for export controls. Critics pestered the Bush administration to formulate a new rationale for export controls, but none emerged. As some pundits pondered "the end of history," concerns about another military threat, the proliferation of Weapons of Mass Destruction and their means of delivery, became ever more prominent."*[47]

In tandem with the collapse of the Soviet threat, the U.S. national security establishment became acutely aware of the rapid rate of "technology-leveling" occurring throughout the global

---

43 Since enactment in 2012, the 0Y521 listings are for biosensors, XBS epoxy systems, and targets for the production of tritium. See BIS Federal Register Notices, <https://www.bis.doc.gov/index.php/all-articles/17-regulations?start=15>. More recently, BIS added a 0Y521 designation for artificial intelligence (AI), or, more formally, geospatial imagery software "specially designed" for training a Deep Convolutional Neural Network to automate the analysis of geospatial imagery and point clouds. See,"Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series," Federal Register, January 6, 2020 < is.gd/qgkeAx>.

44 The new ECCNs are 0A521 (biosensor), 0C521 (XBS epoxy system), and 1A231 (Targets for the Production of Tritium). See BIS Federal Register Notices <https://www.bis.doc.gov/index.php/all-articles/17-regulations?start=15>.

45 See for example, Michael T. Klare, "Endless Military Superiority," *The Nation*, June 27, 2002.

46 As noted by Evans, "Throughout CoCom's existence, the lists of controlled items was modified at least every few years, both to reflect new technological advances and the political/economic balance participating states—mainly the U.S.—were trying to reach. Most of these changes were made to the Industrial List." Samuel Weiss Evans, "Revising Control Lists," Flemish Peace Research Institute, March 2014, pp. 17-18.

47 Richard T. Cupitt, *Reluctant Champions: U.S. Presidential Policy and Strategic Export Controls* (Routledge: New York, 2000).p. 121.

economy as a technology-trade-investment virtuous cycle restructured international markets.[48] As noted in a 1999 Defense Science Board study on globalization and U.S. technological superiority, "The strategic significance of global military-technological leveling cannot be overstated. It presents a direct challenge to perhaps *the* (emphasis in original) fundamental, if subliminal, assumption underlying the modern—and certainly post-Cold War—concept of U.S. military superiority: that the United States enjoys disproportionately greater access to advanced technology than its potential adversaries."[49]

The rapid economic and, by extension, military rise of China throughout the early 2000s resuscitated the earlier Soviet-era concept of conventional military superiority.[50] As during the Cold War, the logic of deterrence constrained bilateral nuclear threat dynamics. PLA modernization, therefore, is the central threat, complicated by a bourgeoning awareness of the potentially revolutionary impact of so-called "disruptive technologies" such as artificial intelligence, additive manufacturing (i.e., 3-D printing), and quantum computing.[51] Originally a business school concept, disruptive or exponential technologies were soon adopted by national security strategists. For example, in a Center for a New American Security report, Ben FitzGerald and Shawn Brimley define 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

48 For example, as economist Richard Baldwin notes: "Managerial and technical know-how became more internationally mobile. After all, the offshored stages of production had to mesh seamlessly and evolve in tandem with the rest of the production network. This 'technology lending' – which is very different from the 1970s 'technology transfer' – could create advanced manufacturing activity in a developing nation in a matter of months. Developing nations no longer had to follow Korea's decade-long slog up the value chain (a feat that dozens of developing nations tried and failed before the 2nd unbundling)." Richard Baldwin, "Trade and Industrialization After Globalization's 2nd Unbundling: How Building And Joining A Supply Chain Are Different And Why It Matters," NBER Working Paper, No. 17716, Issued in December 2011, Revised in January 2013, p. 6.

49 "Final Report of the Defense Science Board Task Force on Globalization and Security," Office of the Under Secretary of Defense for Acquisition and Technology, December 1999, p. 29.

50 The re-emergence of "great power competition" with Russia and, more pointedly, China has impacted the national security narrative regarding export controls, which had earlier focused on WMD and anti-terrorism. For example, a recent Congressional Research Service report contends that: "The shift to renewed great power competition has profoundly changed the conversation about U.S. defense issues from what it was prior to 2014, leading to a reduced relative emphasis in the conversation on counterterrorist operations (although such operations continue), and to a new or renewed emphasis in the conversation on …. maintaining U.S. technological superiority in conventional weapons…" See "Renewed Great Power Competition: Implications for Defense—Issues for Congress," Congressional Research Service, R43838, November 7, 2019, p. 6.

51 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* (New Haven: Harvard Business Review Press, 1997). See also Klaus Schwab, "The Fourth Industrial Revolution: What it Means, How to Respond," World Economic Forum, January 14, 2016 and James Manyika et al, Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy," McKinsey Global Institte, May 2013, p. 6.

policies, doctrines, and organization of all actors."[52] The focus on "innovation" and emerging technologies animates the Pentagon's current, third, Offset Strategy, as a means to "assure U.S. military superiority." [53] Since the creation of the MCTP, the "military superiority" imperative remains intact and, as in earlier identification efforts, underspecified.

Emerging and Foundational Technologies: The MCTP by Any Other Name

The National Defense Authorization Act for Fiscal Year 2019 repealed the portion of the Export Administration Act of 1979 that mandated the creation and maintenance of the Military Critical Technologies List (MCTL). In December 2018, the U.S. Department of Defense cancelled the related DOD Instruction 3020.46, thereby officially terminating the MCTP.[54] As part of the NDAA, Congress enacted the Export Control Reform Act of 2018 (ECRA). 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 technologies 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

---

52 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.

53 See "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence, Office of the Secretary of Defense," October 31, 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*, December 18, 2017.

54 "This Instruction, under the authority of DoD Directive 5134.01 (Reference (a)), establishes policy, assigns responsibilities, and prescribes procedures for developing and maintaining the MCTL as initially mandated by section 2401 et seq. of title 50, United States Code (also known as the Export Administration Act of 1979) (Reference (b)), and extended via section 1701 et seq. of Reference (b) (the International Economic Emergency Powers Act). This Instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Defense Agencies, the DoD Field Activities, and all other organizational entities of the Department of Defense." Source: <t.ly/zOwKN>.

military, nuclear, and dual-use controls.[55]

In the context of the passage of ECRA, it is noteworthy that Congress had been unable to reauthorize the lapsed EAA (2001) to enact new dual-use export control legislation for nearly twenty-years.[56] 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 U.S. export and foreign direct investment controls.[57] The addition of EFT strongly suggested that the extant military and dual-use lists were insufficient to safeguard U.S. "national security" and assure military superiority.[58] Although ECRA does not define "national security," a request for comment BIS published in November 2018 described the national security concerns to be addressed by the effort -- 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."

On November 19, 2018, BIS published an Advanced Notice on Proposed Rulemaking (ANPRM) seeking public comment on criteria for identifying "emerging technologies," with an ANPRM for "foundational technologies" expected at a future date. The ANPRM includes fourteen broad representative categories of technology from which BIS seeks to determine what kinds of emerging technologies are important to U.S. national security for which effective export controls should be implemented: The following technologies are listed in the ANPRM:

---

55 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."

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

57 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."

58 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 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 in 2016 and 2017, January 2018, p. 15.

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

The ANPRM also includes a list of illustrative examples of such 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 inter-agency process, private sector outreach, the Emerging Technology Technical Advisory Committee, and the Committee on Foreign Investment in the United States (CFIUS).[59]

EFT, as categories, are defined neither in the NDAA nor in the ANPRM. While definitions are the apparent goal of the Commerce-led interagency effort, EFT is fundamentally similar in form and broad conceptualization to the earlier MCTL and DSTL programs. "Emerging," as the name suggests, concerns technologies "that are likely to emerge and includes basic research, applied research, and advanced technology development," which describes the DSTL. "Foundational" would seem to imply coverage over "technology areas that DOD assesses as being crucial to the continued superior performance of U.S. military systems or as being able to improve the affordability of U.S. military systems," which characterize the purview of the MCTL.[60] Unlike the EAA of 1979, the NDAA does not establish a dedicated program, the MCTP, but designates a Technical Advisory Committee (TAC) platform.[61]

---

59 Interestingly, the MCTL was also intended to inform CFIUS decisions. However, according to DOD officials, the MCTL was not used to inform these decisions. Instead, the DOD relied on input from technical experts in the Directorate for Defense Research and Engineering on an ad hoc basis. See, GAO, "Defense Trade: Enhancements to the Implementation of Exon-Florio Could Strengthen the Law's Effectiveness," GAO-05-686, September 28, 2005, p. 22.

60 "Defense Technology: DOD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions," July 2006, GAO-06-793, p. 5.

61 As its bureaucratic height, the MCTP was composed of 20 working groups of government, academic, and industry representatives and a dedicated, full-time bureaucracy. See, Raymond V. Wick "Revitalized Militarily Critical Technologies Program," Proc. SPIE 5798, *Spaceborne Sensors II*, May 19, 2005. The Export Control Reform Act (ECRA) required Commerce to establish an Emerging Technology Technical Advisory Committee (ETTAC), which is composed of voluntary private sector advisors.

The public responses to the ANPRM have been predominantly negative, arguing that specific controls were not, in the main, practicable.[62] Complaints varied on a continuum regarding the USG 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 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."*[63]

In many respects, the MCTP labored under the same constraints: defining military significance in the absence of a clear connection to a weapons system. Even with considerable resources, institutions, and expertise, the earlier Congressional mandate foundered.[64] The current compendium of "emerging technologies" is similarly organized and delegated and, therefore, unlikely to result in significant additions to the CCL. Furthermore, the revolutionary and disbursed commercial nature of the ANPRM emerging technologies militates against wholesale or rapid additions. Non-U.S. sources of supply, for example, are increasingly ubiquitous.[65]

---

62 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, November 30, 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."

63 "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>.

64 Martin Chorzempa of the Peterson Institute for International Economics recently noted: "The new regulatory regime, however, will be hindered by a lack of resources. The Bureau of Industry and Security at Commerce, which will likely administer the rules, already has its hands full with designs for new export controls. Without enough staff or expertise, the import process may involve lengthy delays and leave the agency without sufficient ability to evaluate real security risks." Martin Chorzempa, "New U.S. Tech Import Controls are Unacceptably Broad: Proposed Regulations, Targeted at China, Would Threaten American Companies," *Nikkei Asian Review*, December 17, 2019.

65 For example, as noted in a recent Chamber of Commerce report: "A unilateral approach to export control is ineffective. Chinese consumers can source many blocked items from non-U.S. sources. Ironically, unilateral control may accelerate China's development of emerging technologies through nationalization and the strengthening of local industries in mainland China." The American Chamber of Commerce in Shanghai, "Reappraising Export Controls for a New Era of U.S.-China Relations," *Viewpoint*, September 2019, p. 3. See also, Ezell and Foote, "How Stringent Export Controls on Emerging Technologies Would Harm the U.S. Economy," Information Technology and Innovation Foundation, May 2019.

Unlike the EAA of 1979, the identification of EFT under ECRA requires "any technology identified pursuant to subsection (a) be added to the list of technologies controlled by the relevant multilateral export control regimes."[66] If the proposal is not accepted during a three-year period, then the proposing agency must justify the existence of unilateral controls. As explored in other sources, the current and future prospects of multilateral export control regime cohesion, sufficient to generate the necessary consensus on control list additions, is exceptinally unlikely.[67] Even under less political fraught times, consensus on control list and new member additions is challenging.[68]

This cycle of emerging technologies consideration has evolved to the extent that the national security establishment is more highly attuned to the off-the-shelf basis upon which current U.S. military preeminence is based.[69] Specifically, as noted in the ANPRM, BIS cautiously circumscribes the classification effort to only those "specific emerging technologies that are important to the national security of the United States for which effective controls can be implemented *that avoid negatively impacting U.S. leadership* in the science, technology, engineering, and manufacturing sectors."[70] Nevertheless, despite such attentiveness, artificial intelligence is still neither defined or currently used in a weapons system.

---

66 ECRA, §1758. In many respects, parallel to the current EFT process, the Pentagon has recently further identified nine "Critical New Technologies:" hypersonics, directed-energy weapons, artificial intelligence (AI)/machine learning, quantum science, microelectronics, fully networked command and control, and communications, space, autonomy, and cyber. See Office of the Under Secretary of Defense for Acquisition and Sustainment and Office of the Deputy Assistant Secretary of Defense for Industrial Policy, Industrial Capabilities, "Annual Report to Congress Fiscal Year 2018," pp. 10-05.

67 Additionally, the Wassenaar Arrangement, for example, enumerates four criteria to be deployed in proposing additions to the control list: (1) foreign availability outside states participating in the regime; (2) the effective controllability of the goods; (3) the ability to make a clear and objective specification of the item; and (4) existing controls by other regimes. These criteria, combined with declining political cohesion, further diminishes the assimilation of U.S.-sponsored controls into the regimes. Michael D. Beck and Scott A. Jones, "The Once and Future Multilateral Export Control Regimes: Innovate or Die," *Strategic Trade Review*, Vol.5, Issue 08 (Winter/Spring 2019). The criteria are available at "Criteria for the Selection of Dual-Use Items," (agreed in 1994 and amended at the 2005 Plenary), the Wassenaar Arrangement, <is.gd/zx2j1a>.

68 As noted by Brockmann: "It is often difficult to find consensus on membership applications and entirely new control list items even among fairly like-minded states, such as the AG participants or the EU member states. Discussions on technical details, such as the definition and adjustment of control-list parameters, are usually shaped by scientific and industrial considerations, but these are difficult to decouple from economic and political interests. In addition, geopolitical competition and specific interstate issues can also break consensus among groups of generally like-minded states." See, Kolja Brockmann, "Challenges to Multilateral Export Controls: The Case for Inter-regime Dialogue and Coordination," Stockholm International Peace Research Institute, December 2019.

69 See Brian Holmes, "Strategic Latency, Technology Convergence, and the Importance of the Weapons Mix," in *Strategic Latency: Red, White, and Blue: Managing the National and International Security Consequences of Disruptive Technologies*, edited by Zachary S. Davis and Michael Nacht, Center for Global Security Research, Lawrence Livermore National Laboratory, February 2018.

70 Review of Controls for Certain Emerging Technologies: A Proposed Rule by the Industry and Security Bureau, Federal Register, November 19, 2018. See also Ashton Carter, "Shaping Disruptive Technological Change for Public Good," Belfer Center, Harvard University, August 2018.

Conclusion: *Rebus sic Stantibus*

Established in 1980, the MCTP was of limited practical utility. As revealed by GAO and other analyses, the MCTL and DSTL constructs were too broad and/or imprecise to be of direct use in controlling exports and investments and in conditioning control lists. These limitations notwithstanding, the extant military and dual-use control lists continued to operate seamlessly precisely because they are based on established weapons systems or platforms.[71]

As noted by former Assistant Secretary of Commerce for Export Administration Kevin Wolf in Congressional testimony on export control reform under the NDAA,

> *"Deciding what the right national security controls should be over commercial items that are not specific to military applications with respect to China (or any other country) ultimately boils down to how one defines "national security" …The process also includes identifying the commercial items that are required for the development, production, or use of WMD. Then, experts in each technology area work backwards from the identified threat to describe the technical characteristics of commercial items necessary for the development, production, or use of such items. Regulators, in a well-established interagency process, then work to add the items to the regulatory control lists of the United States and its multilateral regime allies. In sum, my main general point today is that the application of export controls in ways that are unclear, unpredictable, or unilateral generally ends up harming the very interests they were designed to protect."*[72]

With the exception of the closing of the so-called "dual-use gap" in the Nuclear Suppliers Group (NSG) in 1991, the nuclear control lists, for example, have changed little. WMD, as currently defined, are not rapidly developing technologies. The concern regarding emerging technologies has focused nearly entirely on those of "militarily significance." Insofar as specific categories have been identified, they cannot be operationalized from a control perspective precisely because they are disconnected from a clearly defined threat.[73] For example, in a report on the defense industrial base, the U.S. 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

---

71 As noted in a recent analysis of emerging technology and export controls, "The speed of development that characterizes most emerging technologies and the elusiveness of appropriate technical standards and parameters is an additional factor that can only be mitigated but is one of the general weaknesses of the list-based approach of the export control regimes and most national export control systems." 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), p. 25.

72 Kevin Wolf, "Testimony before the Senate Committee on Banking, Housing, and Urban Affairs "Confronting Threats from China: Assessing Controls on Technology and Investment" June 4, 2019, p. 3.

73 In many respects, the national security narrative regarding advanced technologies is developing in situ, in real-time. A useful construct for this process is found in Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder CO: Lynne Rienner Publishers, 1998), which outlines the process of *securitization*: "Securitization is the discursive and political process through which an intersubjective understanding is constructed within a political community to treat something as a threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat."

that deliver kinetic effects. Both aspects of the industrial base are needed for long term economic growth and national security"[74] AI, to take one representative genre technology, is currently and increasingly will fuel further innovations across all social domains. However, it is possible only to speculate as to *how* emerging technology will affect national security.[75] As such, by definition, it cannot be export controlled any more than the MCTL or DSTL contributed to the CCL.

In this context, the more meaningful question to pose concerns the process by which technology is managed as a function of and *defined* by national security. The conceptual challenges presented by the current illustrative EFT list 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).[76] 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.[77] The current "Revolution in Military Affairs" moment is narratively contiguous with its various predecessors, focused as they were on technology-driven military

74 "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.

75 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, R45178, November 21, 2019.

76 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, National Defense University, October 2018.

77 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*, July 15, 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.

disruptions.[78] The MCTP resulted from the associated anxiety regarding a possible Soviet military technology breakout.

The current MCTP approach is burdened with the same conceptual limitations and lacks the more considerable institutional heft afforded by a budget line and dedicated institutions.[79] More fundamentally, the present-day global commercial environment and R&D ecosystem is a profound countervailing force that radically undermines the proposed solution set: export controls.[80] As such, any meaningful control effort will require multilateral definitional and procedural support, a highly unlikely prospect given the current U.S. unilateral turn and important commercial applications of the concerned technologies. Indeed, the effective merging of investment and export controls in the FY19 NDAA suggests that controlling technology will require not only an institutional but also a conceptual restructuring of the concept "military superiority." Lastly, the control imperative will require need modes of technology governance. As one analyst recently observed, "Today'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."[81] 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 that do not adhere to the Westphalian model.

---

78 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."

79 In addition to the expiration of the MCTP with the passage of ECRA, the U.S. government also dismantled the Office of Technology Assessment (OTA) in 1995, further diminishing the government's dedicated ability to identify and assess rapidly developing technologies in a sustained and scientifically informed manner.

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

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