CENTER FOR DEMOCRACY & TECHNOLOGY

Comments of the Center for Democracy & Technology to the Regulatory Policy Division, Bureau of Industry and Security, U.S. Department of Commerce on the Review of Controls for Certain Emerging Technologies (Docket 180712626-8840-01 (RIN 0694-AH61))

January 10, 2019

The Center for Democracy & Technology (CDT) is a nonprofit public interest advocacy organization that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communication technologies. With expertise in law, technology, and policy, CDT promotes policies that protect and respect users' fundamental rights to privacy and freedom of expression, and enhance their ability to use communications technologies in empowering ways.

We appreciate the Bureau of Industry and Security (BIS) of the Department of Commerce taking the time to solicit public comments on the criteria for identifying emerging technologies that are essential to U.S. national security through an advanced notice of proposed rulemaking (ANPRM) on the review of controls for certain emerging technologies (Docket No. 180712626-8840-01 (RIN 0694-AH61)). We hope this initial opportunity for public input helps BIS to better understand how the proposal will impact the the numerous companies and institutions in the commercial and academic sectors developing emerging technologies, as well as the related technical communities with a vested interest in the impacts of emerging technologies on security and human rights. Further, we anticipate BIS benefiting greatly from additional, more in-depth responses to a proposed rule from a broader range of interested parties on specific regulatory wording of an emerging technologies control regime.

CDT is active in evaluating the beneficial and detrimental impacts resulting from the myriad of uses of emerging technologies domestically and abroad, and we believe that the digital information technologies on the ANPRM's emerging technologies list should remain unencumbered for the free exchange and cross-pollination of advancements across borders. The United States has been a key incubator of technological innovation for decades as evidenced by the sheer number of technologies created and advanced by its domestic industry-leading companies and world-class academic institutions. Our academic and corporate research and development centers are of the highest caliber and benefit from easy flow of data, information, and ideas about emerging technologies both within the United States and beyond, often with diverse research teams including individuals that are not US

citizens or permanent residents (implicating "deemed exports"[1]). Many of these emerging technologies have nascent or immediate consumer benefits. Unreasonably restricting these technologies for export to limit their proliferation in foreign countries at the expense of benefits to those outside of the U.S. national security sphere must be carefully considered. With that in mind, we are providing comments that specifically address the following:

- The problems with **defining** emerging technologies;
- Criteria to consider when assessing whether there are specific technologies within these general categories that are **important** to U.S. national security; and
- The impact specific emerging technology controls would have on U.S. technological **leadership**

Our expertise is specific to digital information technologies, and accordingly we confine our comments to elements of the ANPRM list specific to those technologies (i.e., unless otherwise stated, we don't specifically discuss the following categories: (1) Biotechnology, (8) Logistics Technology, (12) Hypersonics, and (13) Advanced Materials.)

The Problems with Defining Emerging Technology

Many of the categories and their specific emerging technologies identified by BIS have been under research and development for decades[2] and have mass-market applications, rendering them far from "emerging" technologies. Further, mass-market applications in many of these areas would be stymied if burdened with export control obligations and numerous markets would be negatively impacted given the broad-reaching applicability of such technologies.

---

[1] 15 C.F.R. § 734.13(b). Note that deemed exports are considered by some to be the primary compliance-related issue in university research, *see:* "What is a deemed export?", University at Buffalo Office of Research and Economic Development, *available at:* http://www.buffalo.edu/research/research-services/compliance/export/frequently-asked-questions/what-is-meant-by-a-deemed-export-and-why-is-this-important-.html (last visited 9-Jan-2019).

[2] As the Center for Data Innovation's comment points out, technologies like expert systems have been in active deployment for almost 40 years and components of artificial intelligence such as natural language processing go back even further to the 1950s, *see:* Center for Data Innovation, *Comment Letter on BIS's ANPRM on Review of Controls for Certain Emerging Technologies*, (December 6, 2018), https://www.regulations.gov/document?D=BIS-2018-0024-0038 (last visited 10-Jan-2019). Similarly, the digital information technology fields of PNT technologies, microprocessors, advanced computing technologies, quantum information and sensing, additive manufacturing, robotics, brain-computer interfaces, advanced materials, and advanced surveillance technologies are quite mature. An exhaustive historical examination of maturity of each of these fields is beyond the scope of our comment for this ANPRM. As a few illustrative examples, 3D-printing was an emerging technology in the 1980s, the first commercial robot was available in 1956, *see:* Kodama, H. (1981). Automatic method for fabricating a three-dimensional plastic model with photo-hardening polymer. *Review of scientific instruments*, *52*(11), 1770-1773; Waurzyniak, P. (2006). "Masters of Manufacturing: Joseph F. Engelberger". *Society of Manufacturing Engineers*. 137(1), *available at:* https://web.archive.org/web/20111109053615/http://www.sme.org/cgi-bin/find-articles.pl?&ME06ART39&ME&20060709 (last visited 10-Jan-2018).

Artificial intelligence (AI) is a prime example. It is quickly becoming a standard feature in most modern software and digital services, especially forms of AI such as machine learning. From phones to thermostats to music services,[3] almost all modern software solutions use machine learning techniques to provide users with automated, tailored experiences that better anticipate their needs on a continual basis. Computer vision technologies allow users to search for semantic concepts like "bicycle" and have images returned that contain those kinds of objects. There are many other examples in AI alone.[4] Attempting to control the free-flow of openly-available AI technologies would be akin to placing export controls on essential commodities such as electricity.

We have had significant concerns with export control regulation in the past: first with cryptography and associated key sizes in the 1990s[5] and a just few years ago with network intrusion tools and zero-day vulnerabilities.[6] In the most recent process, the information security community was surprised that tools used by both defenders and attackers would be controlled; we and many others weighed in at the time asking BIS to narrowly tailor those controls so that they would not affect ongoing defensive activities. It took three years to arrive at (potential) rules that establish exemptions for defenders who are engaged in the international coordination of information about security vulnerabilities and malware.[7] Decontrolling mass-market and publicly available tools helped alleviate some of the concerns surrounding the potential impact of the proposed implementation on security researchers and professionals, thereby forestalling the insecurity that would result from such individuals no longer having easy access to such tools.

Stated simply, while regulations will change the behavior of law-abiding firms and individuals, it will not do so to those that act outside the law, exacerbating existing asymmetric adversarial relationships and resulting in increased leverage for entities from other nations. This balancing act is at the heart of export control regulations: how can they be designed in such a manner as to surgically restrict the flow of materials and information that must receive more careful control across the global market

---

[3] Bernard Marr, *27 Incredible Examples Of AI And Machine Learning In Practice*, Forbes (April 30, 2018), https://www.forbes.com/sites/bernardmarr/2018/04/30/27-incredible-examples-of-ai-and-machine-learning-in-practice/ (last visited 10-Jan-2019).

[4] National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee, *The National Artificial Intelligence Research and Development Strategic Plan*, (October 2016), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf (last visited 10-Jan-2019).

[5] CDT coordinated the original Risks to Key Recovery report in 1997 that raised concerns with export controls mandating backdoors, *see:* Hal Abelson et. al, Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, (27 May 1997), https://www.cdt.org/files/pdfs/paper-key-escrow.pdf (last visited 10-Jan-2019).

[6] CDT et al., *Comments to the U.S. Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements*, (July 20, 2015), https://cdt.org/files/2015/07/JointWassenaarComments-FINAL.pdf (last visited 10-Jan-2019).

[7] Tom Cross, *New Changes To Wassenaar Arrangement Export Controls Will Benefit Cybersecurity*, Forbes (January 16, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/01/16/new-changes-to-wassenaar-arrangement-export-controls-will-benefit-cybersecurity (last visited 10-Jan-2019).

without negatively impacting research and innovation. We build off of this notion in the next section to comment on factors that should be weighed when considering new export controls for emerging technologies.

Determining Specific Technologies Important to U.S. National Security and The Potential Effectiveness of Export Controls

As we have described, segregating specific technologies into general categories can be problematic. We suggest considering at least the following questions when assessing whether there are specific technologies within these general categories that are important to U.S. national security: is it already mainstream, open-source, and/or publicly-available; who has demonstrated capabilities; would international cooperation benefit U.S. interests, and; to what extent would export controls restrict domestic research and development?

The more a technology enjoys wide mainstream commercial use, the more likely controls will restrict those uses and the more likely the technology will easily escape reasonable control regimes.[8] Publicly-available technologies that can be purchased on the open market, and especially technologies that have open-source software and hardware components, will be difficult to control; effectively calibrating a control regime to cover these widely-available technologies will require onerous restrictions on those technology uses without clear benefits to national security.

Identifying the extent to which other countries have demonstrated capabilities with identified emerging technologies should also be included in the decision-making process. To the extent a number other countries have demonstrated capabilities in a given area, the less likely export controls are going to be effective as technical knowledge in these areas has already diffused. Progress in commercial markets and even in products made available to consumers can provide insight into the capabilities of an emerging technology that a foreign government has – or has ready-access to – through commercial partners. For example, consider the market dominance of China-based drone manufacturer DJI. The company has managed to combine expertise in computer vision, sensor arrays, flight control, wireless data transmission, and micro manufacturing to develop both consumer and commercial products. According to one analyst: “There is now a general acknowledgment from the industry that no competition exists to DJI.”[9] It would be be naive to expect that the Chinese government isn’t considering domestic unmanned aerial system (UAS) partnerships that match or

[8] This is one reason the EARs exempt certain mass-market technology from controls. 15 C.F.R. § 740.17 *et seq*.
[9] Dinakar Devireddy, *How is DJI ruling Drone marketplace with > 70% global market share?*, LinkedIn (September 16, 2018), https://www.linkedin.com/pulse/how-dji-ruling-drone-marketplace-70-global-market-share-devireddy (last visited 10-Jan-2019).

exceed those of the U.S. military currently available for export.[10] Export controls here would likely only hinder US development by limiting contact between US domestic firms and potentially more-advanced international partners.

Another consideration with respect to foreign state capabilities is to what extent industrial espionage may render export controls mere window dressing. For example, US Intellectual Property (IP) is targeted by foreign adversaries which makes the effectiveness of export controls difficult to maintain. Recently, alleged Chinese spies were indicted[11] on charges that they "targeted and 'stole hundreds of gigabytes of sensitive data' in aviation, space and satellite technology, manufacturing, pharmaceutical and oil and gas exploration, as well as from communications and computer processor firms and maritime technology companies."

International talent has been a meaningful and important element to American innovation. Students from nearly every country attend universities in the United States and present their findings at international conferences. Soft forms of restricting those exchanges such as more stringent immigration policies[12] and prohibiting security researchers from participating in global convenings[13] have the effective impact of imposing controls on intellectual capital. Moreover, to the extent an area of technical innovation, research, and development is subject to restrictions on "deemed exports" – which can be triggered by a mere communication about a controlled subject – compliance will require cumbersome procedures to be established in industry and academia to separate US persons (who can receive such communications unrestricted) and non-US persons (who cannot without a deemed export license in place). Further isolating the U.S. from such exchanges should be considered as part of determining if international cooperation would benefit U.S. interests.

Finally and closely related to international cooperation, BIS should consider to what extent a given control regime would restrict domestic research and development. This could be a market analysis that estimates the burden on typical market participants (manufacturers, consumers, academic researchers, etc.) of compliance with new control obligations. These should be published as part of the supporting material to a proposed rule (in the forthcoming NPRM, perhaps) so that public

---

[10] Stephen Carlson, *AeroVironment awarded contract for drone data links for Norway*, UPI (July 27, 2018), https://www.upi.com/AeroVironment-awarded-contract-for-drone-data-links-for-Norway/2651532695960/ (last visited 10-Jan-2019).
[11] Zack Whittaker, *Justice Department accuses Chinese spies of hacking into dozens of US tech and industry giants*, TechCrunch (December 20, 2018), https://techcrunch.com/2018/12/20/us-indictment-tech-hacks-chinese/ (last visited 10-Jan-2019).
[12] Yeganeh Torbati, *Fewer foreign students coming to United States for second year in row: survey*, Reuters (November 13, 2018), https://www.reuters.com/article/us-usa-immigration-students/fewer-foreign-students-coming-to-united-states-for-second-year-in-row-survey-idUSKCN1NI0EN (last visited 10-Jan-2019).
[13] Violet Blue, When China hoards its hackers everyone loses, Engadget.com (March 16, 2018), https://www.engadget.com/2018/03/16/chinese-hackers-pwn2own-no-go/ (last visited 10-Jan-2019).

commenters can give specific estimates of burdens they will face that might warrant particular attention or changes to the regime design.

Impact Specific Emerging Technology Controls Would Have On U.S. Technological Leadership

As Professor Susan Aaronson points out in her comment on the ANPRM,[14] the United States enjoys such competitive advantages in technical areas in great extent to our openness to new ideas and collaborations across borders. Controls over such a wide-ranging and mature set of technologies would have serious impacts to both industrial and academic competitiveness, reducing the flow of information about new research and development, and restricting the flow of global talent to industrial and academic research centers.

To be certain, other global players have chosen explicitly to restrict inputs and outputs of their industrial and academic research bases. For example, the U.S. does not hold a significant advantage in the areas of quantum computing and robotics compared to China. This is the result of a recent significant policy shift to reduce Chinese reliance on technology developments from Western countries. In 2016 China "launched a "megaproject" for quantum communications and computing, which aims to achieve major breakthroughs[15] in these technologies by 2030". Instead of benefiting naturally from the free flow of information, China has instead decided to offset the loss in flows of global information here by explicitly allocating a massive amount of money – over $1 Billion. Rather than emulate the Chinese strategy of isolation and drastically increasing tax-payer-funded research and development funding to offset the effects of isolation, the United States should continue to "attract investors, competition, and innovation"[16] through openness and welcoming foreign research and development.

Conclusion

Fostering an environment that creates and nourishes industry-leading companies and world-class academic institutions is key to the U.S. remaining competitive in specific areas and maintaining its general technological lead. The ability to exchange technologies, ideas, and information across borders is crucial to such an environment.

---

[14] Susan Aaronson, *Comment Letter on BIS's ANPRM on Review of Controls for Certain Emerging Technologies*, (December 14, 2018), https://www.regulations.gov/document?D=BIS-2018-0024-0031 (last visited 10-Jan-2019) (hereafter, "Aaronson Comment")
[15] Elsa B. Kania, *China's Quantum Future*, Foreign Affairs (September 26, 2018), https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future (last visited 10-Jan-2019)
[16] *Id.,* Aaronson Comment.

The digital information technologies on the ANPRM emerging technologies list should remain unencumbered for the free exchange and cross-pollination of advancements across borders. Overextending export controls will lead to the United States being isolated in the international community and overtaken in many important markets by nations without such controls. This will reduce the United States' ability to engage in cutting-edge academic and industrial research and development.

Please contact us if we can be of further assistance:

Joseph Lorenzo Hall, Chief Technologist, CDT (joe@cdt.org, +1-202-407-8825)
Maurice Turner, Senior Technologist, CDT (maurice@cdt.org, +1-202-407-8819)