GEORGETOWN UNIVERSITY

10 January 2019

Matthew S. Borman
Deputy Assistant Secretary of Commerce for Export Controls
Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Re: ANPRM on *Review of Controls for Certain Emerging Technologies* (BIS-2018-0024)

Mr. Borman,

The Center for Security and Emerging Technology (CSET) at Georgetown University has an ongoing project studying the exports of artificial intelligence (AI) technologies. AI is projected to contribute at least $13 trillion to global economic activity by 2030.[1] Beyond their economic importance, AI technologies have a range of applications to national security, including intelligence and cybersecurity.[2] There are substantial risks to national and global security if democratic nations lose their current lead in AI. Below we review options for export controls on AI software, chips, chip design, and chip manufacturing equipment. To summarize our findings:

- *AI software is unlikely to be an effective point of export control.* Export controls on software are likely to undermine US competitiveness and damage the US Government's relationship with leading US AI firms.
- *Microprocessors for AI systems ("AI chips") are not currently desirable points of export control.* While AI chips are increasingly important to US competitiveness and security, export controls are likely to prompt other states to invest in domestic manufacturing capacity, achieve import substitution, and erode a US supply chain advantage.
- *Equipment for manufacturing AI chips is likely to be an effective point of export control.* Controls on this equipment provide important leverage on future AI chip production. The design and production of such equipment requires advanced capabilities and rare expertise, and existing firms are based in a small number of democratic countries.

As these conclusions are part of an ongoing project on AI exports, we we would be happy to provide additional information to BIS during its analysis.

Best regards,
Jason Matheny
Director, CSET
Jason.Matheny@georgetown.edu

---

[1] Bughin et al. (2018); Rao et al. (2017).
[2] Defense Innovation Board (2017).

Export controls on AI software are likely to be counter-productive

Export controls on AI software are likely to harm US industry R&D. The United States and other democratic countries hold a leading position in the development of AI technologies. With the world's strongest universities and technology companies drawing the brightest technical talent from around the world, this lead is likely to be sustained. While China plans to allocate billions of dollars to subsidize their development of AI technologies,[3] the US has historically made larger investments, with the largest contribution made by industry R&D. Industry funding for research depends on the continued profitability of AI technologies, which would be harmed by any actions that substantially reduce US exports. In addition, compliance with export controls is likely to disproportionately harm small businesses and start-ups whose innovation has been central to US industry's success.

Export controls on AI software are likely to reduce the US AI talent pool. In Silicon Valley, more than half of all technology workers are immigrants.[4] Among those immigrants are many of the world's top AI researchers, and many American-born researchers prize the opportunity to work with the best researchers from around the world. If export controls affect who can work on AI technologies in the US, and what American researchers can share and discuss with non-American colleagues, it will reduce the attractiveness of US research organizations and companies. Fewer world-class researchers will come to the US, and many will leave, weakening AI firms in the US while benefiting firms in competing nations.

Export controls on AI software are likely to damage US Government partnerships with industry. The US Government may damage its fragile relationship with US AI firms if it constrains their ability to share advances in AI research.[5] Many leading AI researchers are committed to sharing results, code, and data, even in cases of limited sharing by industry that don't meet the definition of "fundamental research." Constraints on sharing are likely to alienate a substantial fraction of the US AI research community.

Export controls on AI software are unlikely to stop the spread of software. Software is a poor target for export control, due to the ease of illicit transfer and theft, and due to the difficulty of crisp legal definition. It is impractical to list the set of principles, algorithms, models, architectures, parameter weights, and datasets that comprise the non-hardware components of AI research, development, and production. The ambiguity of "AI" would likely encourage both under- and over-compliance for an export control: conscientious researchers are likely to err on the side of safety and under-share research, reducing progress, while the brazen will exploit the ambiguity to avoid compliance.

Export controls on AI software are appropriate in rare cases. Important exceptions to the above are export controls narrowly targeting AI technologies that invite misuse by authoritarian states. These include controls on specific AI-related products designed for law enforcement and

[3] Ding (2018).
[4] Coren (2017).
[5] Fryer-Biggs (2018); Nix (2018); Zegart & Childs (2018).

national intelligence use,[6] and end-user controls on technologies that serve as component pieces for tools to automate censorship,[7] and biometric technologies that can be used for mass surveillance.[8] As well as furthering the human rights aims of the US, such controls, unlike others, have the potential to strengthen the US Government's relationship with the AI research community.

Export controls on AI chips and AI chip designs are likely to be counter-productive

Export controls on AI chips would erode an important supply chain advantage of the US and other democratic states. The computing power required for AI increasingly relies on specialized microprocessors, "AI chips," optimized for AI applications. While AI chips could be targeted by export controls, the vast majority of chips exported by US firms will not be used for purposes that threaten security or human rights. Even in cases of exports to non-democratic states, the US position in the supply chain preserves options for future influence.

Export controls on AI chips are likely to prompt import substitution. In 2016, when export controls prevented Intel from shipping Xeon processors to China for the Sunway TaihuLight supercomputer, China replaced the processors with locally designed Sunway SW26010 processors. Less than a year and half later, the TaihuLight was the fastest computer in the world,[9] a title it held for two years. The effect of the US export control was a substantial loss for Intel, costing hundreds of millions of dollars, and a substantial gain for the Chinese microprocessor industry, gaining hundreds of millions of dollars and significant technical experience.[10] Export controls on AI chips are likely to prompt similar import substitution.

Export controls on AI microprocessor designs are unlikely to be effective. Microprocessor designs rely on intellectual property that is relatively easy to transfer or steal, and require expertise that is widely distributed.[11]

Export controls on AI chip manufacturing equipment are likely to be effective

Democratic nations lead the global market in semiconductor manufacturing equipment. AI chips are produced using highly advanced semiconductor manufacturing equipment that is relatively easy to define, monitor, track, and control. The equipment is produced by a small number of firms located in the US and other democratic nations. Most of the world's semiconductor manufacturing equipment is produced by firms based in the US (47%), Japan (30%), the Netherlands (over 17%), South Korea (<3%), and Germany (<3%).[12] Export controls for the equipment already exist and have not prompted import substitution, due to the difficulty of production.

---

[6] Already covered by BIS under "Crime control and detection" (15 CFR 742.7).
[7] Cope et al. (2017); Knockel et al. (2018).
[8] Mozur (2018).
[9] Barrett (2016).
[10] Sun (2015).
[11] PwC (2017).
[12] US International Trade Administration (2016).

Semiconductor manufacturing equipment is costly. The latest generation of lithography equipment, necessary for just one part of the semiconductor manufacturing process, costs $120 million per set.[13] The entire cost of equipment in one semiconductor foundry is typically over $10 billion dollars. These costs are increasing with each generation. Moore's Second Law (also known as "Rock's Law") observes that the cost of semiconductor tools doubles about every four years.[14]

Semiconductor manufacturing equipment is difficult to replicate, transfer, or steal. Semiconductor manufacturing equipment requires highly specialized tools and expertise to build. These technologies have involved hundreds of billions of dollars in R&D, and decades of production experience. Due to the tools' size and fragility, it would be difficult for states to circumvent export controls through illicit transfer or theft. Given the financial stakes, such transfer or theft is unlikely to go unnoticed.

References

Barrett, Brian. "China's New Supercomputer Puts the US Even Further Behind." *Wired*, 21 June 2016, https://www.wired.com/2016/06/fastest-supercomputer-sunway-taihulight/.

Bughin, Jacques, Jeongmin Seong, James Manyika, Michael Chui, and Raoul Joshi. "Notes from the AI frontier: Modeling the impact of AI on the world economy." McKinsey, Sept 2018, https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy.

Cope, Sophia, Jillian York, Jeremy Gillula. "Industry Efforts to Censor Pro-Terrorism Online Content Pose Risks to Free Speech." Electronic Frontier Foundation, 12 July 2017, https://www.eff.org/deeplinks/2017/07/industry-efforts-censor-pro-terrorism-online-content-pose-risks-free-speech.

Coren, Michael J. "More Silicon Valley tech workers were born outside the US than in it." *Quartz*, 17 July 2017, https://qz.com/1029860/more-silicon-valley-tech-workers-were-born-outside-the-us-than-in-it/.

Defense Innovation Board. "Recommendations." Department of Defense, 2017, https://innovation.defense.gov/Recommendations.

Ding, Jeffrey. *Deciphering China's AI Dream: The context, components, capabilities, and consequences of China's strategy to lead the world in AI*. Future of Humanity Institute, University of Oxford, 2018, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf.

Fryer-Biggs, Zachary. "Inside the Pentagon's Plan to Win Over Silicon Valley's AI Experts." *Wired*, 21 Dec 2018, https://www.wired.com/story/inside-the-pentagons-plan-to-win-over-silicon-valleys-ai-experts/.

[13] Ting-Fang (2018).
[14] Ross (2003); Rupp & Selberherr (2011).

Knockel, Jeffrey, Lotus Ruan, Masashi Crete-Nishihata, and Ron Deibert. “ (Can’t} Picture This.” The Citizen Lab, 14 Aug 2018, https://citizenlab.ca/2018/08/cant-picture-this-an-analysis-of-image-filtering-on-wechat-moments

Mozur, Paul. "Inside China’s dystopian dreams: AI, shame and lots of cameras." *New York Times*, 1 July 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

Nix, Naomi. “Google Drops Out of Pentagon's $10 Billion Cloud Competition.” Bloomberg, 8 Oct 2018, https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition.

PwC. "China’s impact on the semiconductor industry: 2016 update." 2017, https://www.pwc.com/gx/en/technology/chinas-impact-on-semiconductor-industry/assets/china-impact-of-the-semiconductor-industry-2016-update.pdf

Rao, Anand, Gerard Verweij, and Euan Cameron. “Sizing the Prize.” PriceWaterhouseCoopers, 2017, https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.

Ross, Philip. “5 Commandments.” *IEEE Spectrum*, 1 Dec 2003. https://spectrum.ieee.org/semiconductors/materials/5-commandments/2

Rupp, Karl, and Siegfried Selberherr. "The economic limit to Moore's law." *IEEE Transactions on Semiconductor Manufacturing* 24.1 (2011): 1-4.

Sun, Leo. “The U.S. Government Crushes Intel Corporation's Chinese Supercomputer Chip Sales.” *The Motley Fool*, 15 Apr 2015, https://www.fool.com/investing/general/2015/04/15/the-us-government-crushes-intel-corporations-chine.aspx.

Ting-Fang, Cheng. “Chinese chipmaker takes on TSMC and Intel with cutting-edge tool.” *Nikkei Asian Review,* 15 May 2018, https://asia.nikkei.com/Business/Companies/Chinese-chip-maker-invests-in-next-gen-tool-to-close-gaps-with-Intel-TSMC-Samsung.

US International Trade Administration. *2016 Top Markets Report Semiconductors and Semiconductor Manufacturing Equipment*. 2016, https://www.trade.gov/topmarkets/pdf/Semiconductors_Semiconductor_Manufacturing_Equipment.pdf.

Zegart, Amy, and Kevin Childs. “The Divide Between Silicon Valley and Washington Is a National-Security Threat.” *The Atlantic*, 13 Dec 2018, https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.