Cybersecurity Coalition

January 10, 2019

Submitted via https://www.regulations.gov

U.S. Department of Commerce,
Bureau of Industry and Security, Regulatory Policy Division
14th Street and Pennsylvania Avenue NW, Room 2099B
Washington, DC 20230
RIN: 0694-AH61

RE: Comments on Proposed Rule "Review of Controls for Certain Emerging Technologies"

The Cybersecurity Coalition ("Coalition") submits this comment in response to the Advance notice of proposed rulemaking (ANPRM) FR Doc. 2018-25221 issued by the Bureau of Industry and Security, Commerce ("BIS") on November 19, 2018 regarding the Review of Controls for Certain Emerging Technologies.[1] The Coalition appreciates the opportunity to comment on the status of development of these technologies in the United States and other countries, and the impact specific emerging technology controls would have on U.S. technological leadership.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[2] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community.

The Coalition appreciates the opportunity to provide these comments and participate in this important discussion. Specifically, the Coalition notes that because of the global availability of cybersecurity tools, attempts to regulate U.S. companies with export controls on the emerging technologies under consideration puts U.S.-based cybersecurity companies at a significant competitive disadvantage. In particular, introducing barriers will hinder U.S. cybersecurity companies' ability to keep pace with foreign countries who have made substantial advancements in several of the Representative Technology Categories listed, including artificial intelligence

[1] https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

[2] The views expressed in this comment reflect the consensus views of the Coalition and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org.

(AI), quantum information and sensing technology, and data analytics (including automated analysis algorithms and data visualization). Lastly, because cybersecurity tools increasingly rely on new technologies, and government and critical infrastructure increasingly rely on these tools, the introduction of export controls may inadvertently harm U.S. national security by weakening U.S. companies' ability to innovate within the technologies under consideration.

The Coalition recognizes the government's concern in addressing the national security implications of emerging technologies, but we strongly emphasize caution in introducing new controls that would have significant negative effects on U.S. cybersecurity interests. In particular, the Coalition recommends the following: First, technologies that are today available in the market and have defensive or preventative uses in cybersecurity should not be controlled. Second, additional special consideration should be taken to avoid hindering the development of cybersecurity technologies that are needed to secure U.S. infrastructure, or infrastructure abroad that advances U.S. interests. Third, to mitigate negative impacts on U.S. companies due to lack of clarity, controlled emerging technologies should be defined consistent with recognized industry standards. Fourth, as part of its analysis of the effectiveness of export controls in limiting foreign proliferation of emerging technologies, BIS should consider viable technical and legal alternatives to export controls to achieve U.S. goals, such as increased measures to protect intellectual property and prevent espionage.

The Coalition's views are more thoroughly outlined below and account for the three process points BIS identified as needing consideration; the development of emerging and foundational technologies in foreign countries; the effect export controls may have on the development of such technologies in the United States; and the effectiveness of export controls on limiting the proliferation of emerging and foundational technologies in foreign countries. In addition, we welcome the opportunity for BIS to provide industry with the means to provide confidential/non-public feedback in further rule making since the absence of a confidential channel of industry feedback limits the ability of industry to provide substantive feedback due to competitive and intellectual property reasons.

Negative Impacts on U.S. Companies, Domestic Development, and Technological Leadership

While many of the largest and best cybersecurity companies, products and services are currently based or produced within the United States, many other countries have made significant strides in being able to produce products and services that are becoming comparable in quality. Given the global availability of these products and services, adding new controls on emerging technologies in the United States will undermine the position of U.S. cybersecurity companies in the marketplace relative to key foreign competitors. Some such competitors, such as Israel and China, are also not subject to multilateral regimes like the Wassenaar Arrangement, and the new addition of separate controls on U.S. companies will confer a greater advantage on those competitors. The introduction of any additional barriers to U.S. companies in the form of restrictive export controls is likely to result in market losses, while boosting the prominence and market share of foreign competitors at a time when the cybersecurity market is projected to grow significantly.

The United States is no longer the clear frontrunner in the production or development of several of the listed emerging technologies that have become integral to innovation in cybersecurity, while at the same time many competitors in these areas are unburdened by export control regimes. Specifically, the uptick in the automation of cyber offense and cybercrime can only be effectively countered by the integration of AI and machine learning into defensive measures, an area in which many U.S. companies are currently focusing. There are strong non-U.S. competitors doing research and development in AI- and machine learning-related cybersecurity. If U.S. companies' emerging technologies are controlled, this will cede the market to non-U.S. competitors. Customers globally are demanding this kind of defensive automation in response to automated cyberattacks and will buy it from a non-U.S. company if needed.

Export controls on emerging technologies that are essential to cybersecurity could also hinder U.S. cybersecurity companies' ability to protect organizations worldwide – including U.S. government agencies and organizations that are U.S. companies with international branches, partners, customers, and supply chains- weakening these organizations' ability to defend their information and networks against cyber adversaries (who do not have controls on innovation and who will remain steps ahead). This will in turn inflict damage throughout the U.S. economy and be an unintended consequence of U.S. export controls on these emerging technologies.

Overly broad export controls may further damage U.S. companies, hinder domestic development, and damage the cybersecurity environment in numerous additional ways. First, security research and information sharing, which is critical to maintaining the health of the cyber ecosystem by ensuring threats and vulnerabilities are quickly identified, analyzed, and patched in a timely manner, may be hampered. Because the entire global digital infrastructure is interconnected—data as well as cyber threats flow across borders—controlling cybersecurity technology in this manner could also have the unintended but counterproductive consequence of slowing the discovery and disclosure of critical vulnerabilities, as well as the tools needed to patch them - this could in turn harm the U.S. critical infrastructure. Second, if any new controls apply to back-end data sets, which are necessary for AI, machine learning, and their subcategories such as deep learning and natural language processing, this could significantly increase the cost and lower the efficacy of research needed for U.S. firms to stay competitive globally. Third, overly broad restrictions may create ambiguity in terms of coverage, which could lead to companies to refrain from innovating in emerging technologies or step back from certain key technologies to avoid compliance issues. Lastly, the effects of any new restrictions that hinder U.S. cybersecurity companies' ability to innovate and remain on the cutting edge of technology development will reduce the desirability of relocating companies or recruiting individuals to the United States, a factor that has been important in retaining elite talent and maintaining robust research and development.

All of the above will greatly impact the standing of the United States' global technological leadership in cybersecurity. It would be prudent to adopt the posture that, if an emerging technology is used for defensive and preventive purposes with benefits for the U.S. economy generally it should NOT be controlled.

Development in Foreign Countries

Cybersecurity Coalition

Export controls are unlikely to significantly hinder the foreign development of these emerging technologies. Many states already possess detailed policy plans for developing areas of expertise within them, including Russia, France, China, and the UK. Specifically, China has made dramatic progress with evidence to suggest that they are quickly closing the gap with the United States in many of the emerging technology categories such as quantum, AI, and data analytics.

In quantum computing: China already has the first satellite capable of intercontinental quantum cryptography; has made quantum research a designated "mega project"; reportedly set aside $10 billion for the National Laboratory for Quantum Information Sciences; and reportedly has surpassed the United States in quantum related patents.[3,4,5] Chinese development of AI for security purposes follows a similar trajectory.

As in quantum research, China surpassed the United States in AI related patents several years ago and they have also closed the gap with regards to academic publishing.[6] Much of that publishing came before China's comprehensive AI development plans for 2020 and 2030 were outlined in a 2017 paper that emphasized becoming the world leader in that area.[7] While AI has been implemented widely in Chinese surveillance programs for years, they broadened the scope considerably in their 2017 policy pronouncements to cover a wide range of security uses.[8] In Particular, Baidu, the largest internet search operator in China, has already offered AI driven facial recognition software for security purposes in multiple Chinese airports, including in Beijing.[9] Beyond facial recognition, Chinese AI companies like iFlyTek are among the global leaders in speech recognition and machine translation.[10]

---

[3] "Chinese Satellite Uses Quantum Cryptography For Secure Videoconference Between Continents". 2018. *MIT Technology Review*. https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/#.

[4] Decker, Susan, and Christopher Yasiejko. 2018. "Forget The Trade War. China Wants To Win Computing Arms Race". *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2018-04-08/forget-the-trade-war-china-wants-to-win-the-computing-arms-race.

[5] Katwala, Amit. 2018. "Why China's Perfectly Placed To Be Quantum Computing's Superpower". *Wired.Co.Uk*. https://www.wired.co.uk/article/quantum-computing-china-us.

[6] Huang, Echo. 2018. "China Has Shot Far Ahead Of The US On Deep-Learning Patents". Quartz. https://qz.com/1217798/china-has-shot-far-ahead-of-the-us-on-ai-patents/.

[7] Webster, Graham, Rogier Creemers, Paul Triolo, and Elsa Kania. 2017. "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)". *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

[8] Ibid

[9] Jing, Meng. 2017. "Beijing Airport Tests Baidu'S 'Face As Boarding Pass' Technology". *South China Morning Post*. https://www.scmp.com/tech/china-tech/article/2108163/baidu-offers-facial-recognition-technology-help-beijing-airport.

[10] Lee, Kai-Fu. 2018. *AI Super-Powers - China, Silicon Valley, and the New World Order*. 1st ed. New York: Houghton Mifflin Harcourt.

In an effort to further the AI development needed to implement these policies, China has outlined their plan to introduce reforms allowing better use of public data and tax incentives for companies engaging with AI.[11] AI research in China is further supported by the massive amounts of data available to train AI and machine learning. In summation, the regulatory permissiveness, enormous quantity of data created and available, and the opinion of some AI experts that China is better suited to implementing the AI advancements that originated in the West, has pushed China to the forefront of the technology and will continue to give China significant advantages moving forward.[12]

Conclusion

To reiterate, while the Coalition is cognizant of the government's desire to classify and control emerging technologies that may impact national security, it is the Coalition's view that restrictive export controls on a broad swath of emerging computing technologies, including a broad range of AI solutions, quantum computing, and data analytics will have significant negative impacts on U.S. cybersecurity companies and on the future development of many of those emerging technologies. Furthermore, the advanced development of these technologies, as they relate to cybersecurity, in other parts of the world is unlikely to be slowed by restrictive export controls in part due to their growing availability abroad.

The Coalition's recommendations are as follows. First, technologies that have defensive or preventative uses in cybersecurity should not be controlled. Second, that special consideration be given to support development of cybersecurity technologies that are needed to secure U.S. infrastructure, or infrastructure abroad that advances U.S. interests. Third, to mitigate negative impact on US companies due to lack of clarity and overbreadth, definitions for controlled emerging technologies should be based on internationally accepted standards. Fourth, as part of BIS' consideration of the effectiveness of export controls in limiting technology proliferation in foreign countries, BIS should consider viable alternatives to export control to achieve U.S. goals, such as technical and legal resources to prevent international hacking and espionage of emerging technologies.

The Coalition appreciates the opportunity comment on this important effort and looks forward to continued collaboration with the BIS as it engages in the interagency to identify and describe emerging technologies.

Respectfully Submitted,
The Cybersecurity Coalition

[11] Webster, Graham, Rogier Creemers, Paul Triolo, and Elsa Kania. 2017. "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)". *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

[12] Lee, Kai-Fu. 2018. *AI Super-Powers - China, Silicon Valley, and the New World Order*. 1st ed. New York: Houghton Mifflin Harcourt.