On "Smart Competition: Adapting U.S. Strategy toward China at 40 Years"

A Hearing Before the

House Foreign Affairs Committee

Testimony of Samm Sacks
Cybersecurity Policy and China Digital Economy Fellow, New America

May 8, 2019

Chairman Engel, Ranking Member McCaul, and Members of the Committee, thank you for the opportunity to testify today.

I am a Cybersecurity Policy and China Digital Economy Fellow at New America. My research focuses on information and communication technology (ICT) policies in China. I have worked on Chinese technology issues for over a decade, not only with the national security community, where I focused on technology transfer and dual-use technology, but also with the private sector, tracking China's cyber regulatory environment.

All eyes this week are on the potential for a trade agreement between the United States and China. To be sure, such an agreement would be a stabilizing force in what has been perhaps the most tumultuous period in the bilateral relationship in four decades. But even if we do get some kind of agreement, the two governments will continue to struggle with a much deeper, simmering conflict over technology. As my colleague Graham Webster wrote recently: "The two societies and their governments are only starting to reckon with the challenges that will come with emerging technologies and their deep integration with social and economic systems."[1]

[1] Graham Webster, "If the U.S. and China Make a Trade Deal, Then What?" *ChinaFile*, Asia Society, April 30, 2019, available at: http://www.chinafile.com/conversation/if-us-and-china-make-trade-deal-then-what.

The administration of President Xi Jinping is doubling down on aspirations for China to become a so-called "cyber superpower" and "science and technology superpower."[2] These aspirations manifest through a state-driven approach in which political and financial resources are directed toward cementing China's leadership in emerging technologies and the development of technical standards.[3] Artificial intelligence (AI) and the 5G wireless networks that will enable data-driven applications and connectivity are top priorities for the country's leadership.

As part of this vision, the leadership is seeking to reduce reliance on foreign suppliers in what are deemed "core technologies."[4] For a more detailed discussion of the challenges posed for market access of U.S. firms operating in China, I would like to refer the Committee to my earlier testimony from March before the Senate Commerce Subcommittee on Security, in which I spoke about issues such as source code review requirements, localization pressures, and restrictions on cross-border data flows.[5] I talked about how the risks created by China's domestic cybersecurity standards regime are not likely to go away, even if the Chinese government appears to make concessions in a trade deal, for instance by prohibiting technology transfer requirements or by removing caps on foreign ownership shares in certain sectors. I would be happy to take any questions on this topic during the hearing.

---

[2] Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster, "China's Strategic Thinking on Building Power in Cyberspace," *DigiChina*, New America, September 25, 2018, available at: https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

[3] Hilary McGeachy, "US-China Technology Competition: Impacting a Rules Based Order," United States Studies Centre, University of Sydney, May 2019, available at: https://www.ussc.edu.au/analysis/us-china-technology-competition-impacting-a-rules-based-order.

[4] Paul Triolo, Lorand Laskai, Graham Webster, and Katharin Tai, "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities," *DigiChina*, New America, May 19, 2018, available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

[5] Samm Sacks, Testimony before the Senate Commerce Subcommittee on Security on "China: Challenges to U.S. Commerce," March 7, 2019, available at: https://www.commerce.senate.gov/public/index.cfm/2019/3/china:%20challenges%20for%20u.s.%20commerce and Graham Webster, Samm Sacks, and Paul Triolo, "Three Digital Policies at Stake in US-China Trade Talks," *DigiChina*, New America, April 2, 2019, available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/three-chinese-digital-economy-policies-at-stake-in-the-uschina-talks/.

Beyond market access, there are also national security, supply chain, ideological, and human rights dimensions to this technology conflict with China. The decisions U.S. policymakers take at this juncture are likely to have implications for generations to come. So what should be done?

U.S. policy should be based on a "small yard, high fence" approach.

Borrowing a phrase from former Secretary of Defense Robert Gates, this means being selective about what technologies are vital to U.S. national security, but being aggressive in protecting them.[6] Overreach in the form of blanket bans, unwinding global supply chains, and discrimination against Chinese individuals based on national origin is not the answer.

The United States and China belong to an interconnected system when it comes to research, development, manufacturing, and talent. Innovation by American companies is fueled by access to the Chinese market. The leading semiconductor manufacturers make substantial profits in China. They then plow a major portion of those profits back into R&D in order to stay competitive in emerging technologies like 5G. Unlike the Cold War space race with the Soviet Union, the line between U.S. and Chinese technological development is not as clear as the political border between the two countries. Efforts to segregate or "decouple" the two systems will come at a steep cost to U.S. innovation and technological leadership.

Moreover, not all Chinese students, researchers, and scientists are spies. Treating them as such is dangerous to U.S. national interests.

[6] Lorand Laskai and Samm Sacks, "The Right Way to Protect to American Innovation," *Foreign Affairs,* October 23, 2018, available at: https://www.foreignaffairs.com/articles/2018-10-23/right-way-protect-americas-innovation-advantage.

The question, then, is: How do we maintain the openness of the U.S. system in a way that is less vulnerable to exploitation? Is it possible to build a system that is both open and resilient? Yes, I believe we can and we must.

I'd like to talk about the different tools available to do this. First, export controls.

The Department of Commerce has issued a list of "emerging technologies" that may be subject to new export controls due to their importance for national security and has solicited feedback from industry. Updating the export control regime is an important step, but, as Kevin Wolf—who played a key role in creating these rules in his former role as Assistant Secretary of Commerce for Export Administration—has testified before this committee last year: "[they must be] properly calibrated, tailored controls to avoid collateral economic costs, unnecessary regulatory burdens, and misallocation of federal resources. Excessive controls harm the U.S. defense industrial base, which results in harm to our national security."[7]

I cannot identify today a list of emerging technologies that should be prioritized into the future. In fact, I would argue that we cannot know ahead of time the specific technologies that will be crucial to U.S. national security. So, instead of the open-ended and vague negative list that has been proposed, I'd like to offer a framework and a set of principles that can help us arrive at a specific list of technologies and applications.

In general, a technology should be subject to greater control if:

1) It is essential to military technology; however, the term "essential" should not be interpreted to encompass technology that is simply used or is usable by the military, since the defense industry

[7] Kevin Wolf, Testimony before the House Foreign Affairs Committee on "Modernizing Export Controls: Protecting Cutting-Edge Technology and U.S. National Security," March 14, 2018, available at: https://docs.house.gov/meetings/FA/FA00/20180314/107997/HHRG-115-FA00-Wstate-WolfK-20180314.pdf.

is increasingly reliant on commercial off-the-shelf technology. The International Traffic in Arms Regulations (ITARs) are designed to fulfill this purpose, but differentiating between essential military technology (often controlled by the United States Munitions List) and dual-use technology remains a challenge;

2) There is a scarcity of knowledge about the technology, except among a small group of experts located in the United States or like-minded countries; and
3) The United States is truly ahead of the curve, and that technology is developed exclusively in the United States or other countries that enforce similar export controls. Technical experts must be regularly consulted to evaluate incremental differences between our technology and that of other countries on this point. Not doing so risks the "designing out" of U.S.-made components from products for global markets, which would advantage foreign companies with similar products that are not subject to export controls.

Reviews of the list of emerging technologies should be conducted by both military and non-military stakeholders (including those from the commercial sector who are not regularly part of the export control system), and the findings must be regularly reevaluated and updated.[8] This should not be a one-off process. It is very important that industry provide specific feedback to the ongoing Commerce Department process.

There are some technologies for which export controls may not be a suitable tool. Which brings me to the next question: **How should we think about U.S.-China collaboration on basic AI research?**

This is a very complex and difficult issue, and to date there is no rigorous, objective study that addresses the challenge. I recommend that the United States actively engage with international standards bodies

[8] Ibid.

such as ISO or Institute of Electronics and Electrical Engineers (IEEE) to guide the development of standards for collaboration on open AI research. This is not something that will be solved simply or quickly due to the interplay of three main challenges:

1) Many AI applications are inherently dual-use. As experts like MIT's R. David Edelman have commented, it may be impossible to distinguish between civilian and military uses of AI.[9] For example, facial recognition tools could be used to target drone strikes as well as to identify customers in a store.[10]
2) It is very difficult to prevent code from crossing borders. Many state-of-the-art AI systems like facial recognition are produced by industry and are then (in part or fully) published openly online. It would not be too difficult for a foreign military to pick up the technology and leverage it in a military application. In addition, research is often done collaboratively through networks of engineers around the world that do not conform neatly to national borders. Once code and other AI-related capabilities are published openly, it is virtually impossible to control their diffusion. Gaining control over end uses and users in global supply chains may be near impossible.
3) Lastly, the United States derives benefit from joint research with Chinese partners in the form of access to talent and to cutting-edge work in areas where U.S. and Chinese researchers are working to find answers to similar problems. Innovation now flows both ways across the Pacific. There are also national security risks to losing visibility and insight into the advancements of Chinese researchers and companies.

[9] Cade Metz, "Curbs on A.I. Exports? Silicon Valley Fears Losing Its Edge," *The New York Times*, January 1, 2019, available at: https://www.nytimes.com/2019/01/01/technology/artificial-intelligence-export-restrictions.html
[10] Justin Sherman, "U.S. Tech Needs Hard Lines on China," *Foreign Policy*, May 3, 2019, available at: https://foreignpolicy.com/2019/05/03/u-s-tech-needs-hard-lines-on-china-artificial-intelligence-technology-microsoft-google-defense/.

Despite these challenges, there may be more urgency now than ever for guidelines on the ethics of AI collaboration. As my colleague Justin Sherman recently wrote, "Collaboration on AI research gives far better insight into developing technology and its implementation than just reading a paper or downloading code online."[11] This matters because right now in Xinjiang, the Chinese government is detaining large numbers of ethnic Muslims and using a range of technologies in the process. Biometric scans, facial recognition, devices that scan smartphones for encrypted chats, and high-tech big data monitoring systems are enabling the mass surveillance and incarceration of Uighurs and other citizens, with estimates ranging from hundreds of thousands to more than one million people affected. Recent reports indicate that the Chinese government may be using AI for racial profiling to identify and track Uighur faces.[12]

International standards are one option for assessing AI collaborations with Chinese partner organizations. The idea would be to put in place a process to systematically consider the ethics of new projects, including the potential harm that can result from seemingly benign research like computer vision. When considering AI collaborations, factors to consider include: the possibility that the Chinese government may co-opt private sector or academic projects; whether the technology has already diffused and where it is on the spectrum of theoretical research to application; the nature of the collaboration; etc. Many U.S. companies are already having these discussions internally, so the aim of a standard would be to provide a more comprehensive framework and resources for thinking through the issue, potentially including third-party audits.

Relying on standards is not a complete or perfect way to address national security or human rights implications of AI collaboration, but the extreme positions—pretending these issues do not exist in this sprawling and changing field of research, or pushing to sever all AI research ties with China, regardless of

[11] Ibid.
[12] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *The New York Times*, April 14, 2019, available at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

the specifics or the downsides—do not serve U.S. interests and values. I hope that this can be the start of a candid and clear-eyed conversation among U.S. policymakers, companies, and research organizations.

My third and final recommendation is that the United States **must play offense by investing in its own R&D, infrastructure, and STEM education.** Ezekiel Emanuel, Amy Gadsden, and Scott Moore of the University of Pennsylvania argued in a recent op-ed that the United States must "fix the mismatch between its declared national technology priorities and the deployment of research funding." They argue for doubling funding in basic and applied research in the areas identified by the U.S. intelligence community such as AI, 5G, and quantum computing.[13]

The bottom line is that China will not abandon its technological ambitions, so we must be able to compete in our own right.

Thank you. I look forward to your questions.

[13] Ezekiel Emanuel, Amy Gadsden, and Scott Moore, "How the US Surrendered to China on Scientific Research," *The Wall Street Journal*, April 19, 2019, available at: https://www.wsj.com/articles/how-the-u-s-surrendered-to-china-on-scientific-research-11555666200.