On "China: Challenges to U.S. Commerce"

A Hearing Before the

Senate Committee on Commerce, Science, and Transportation's Subcommittee on Security

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

March 7, 2019

Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee, I appreciate the opportunity to testify on the challenges China presents to U.S. commerce.

I am a Cybersecurity Policy and China Digital Economy Fellow at New America. New America is a nonpartisan think tank dedicated to the mission of realizing our nation's highest ideals through confronting challenges caused by rapid technological and social change.

My research focuses on information and communication technology (ICT) policies in China and the U.S.-China technology relationship. I have worked on Chinese technology and cyber issues for over a decade, not only with the U.S. government, where I focused on the national security implications of technology transfer and dual-use technology, but also with the private sector, looking at China's complex and rapidly evolving regulatory environment.

This hearing could not come at a more critical moment. The United States and China are locked in a deepening conflict with technology and cybersecurity at the center. It is arguably the most significant period in the bilateral trade and investment relationship in the last four decades. The decisions made by U.S. policymakers during this window will have consequences for U.S. national security, competitiveness, innovation, technological leadership, and norms for years to come.

China's Technology Challenge

In his testimony last week before the House Ways and Means Committee, Ambassador Lighthizer testified that technology transfer, failure to protect intellectual property (IP), large subsidies, and cyber theft of commercial secrets present major problems for the U.S.

economy.[1] While much attention is paid to the role played by joint ventures (JVs) and China's industrial policy, I will focus here on three related issues that get less attention than they deserve and where there is an opportunity right now for action: standards, data flows, and emerging technology norms and governance.

While I will focus my comments on the ICT space, these challenges are not limited to companies in the technology industry. They also matter for all sectors that rely on ICT infrastructure, data, and digital platforms—including manufacturing, finance, energy, retail, healthcare, etc.

1. Market Access, IP, and Technology Transfer

The administration of President Xi Jinping is doubling down on plans to reduce reliance on foreign suppliers in what are deemed "core technologies."[2] These efforts coincide with Beijing's rapid build-out of the most comprehensive cybersecurity legal and regulatory regime of any government in the world. An interlocking system of laws, regulations, and standards create a maze of rules spanning data, online content, and critical infrastructure. While the Cybersecurity Law is the centerpiece of this system, far less understood are the hundreds of cybersecurity standards accompanying it, which in practice are vital for actually doing business on the ground.

These standards contribute to making China an increasingly difficult market for foreign firms to operate in. There are three main challenges posed by the standards regime:[3]

- **First, the Chinese government can use standards to pressure companies to undergo invasive product reviews where sensitive information and source code (even if not explicitly required) may be exposed as part of verification and testing.** This includes, for example, the security assessment process for products such as central processing units, operating systems, and office software suites. As part of the assessment, suppliers need to submit verification materials including product IP, source code, and design and development documents. China's Standardization Law (which took effect in January 2018) may require public disclosure of what are called "enterprise standards," referring to a company's proprietary product and service specifications, according to BSA's Special 301 Submission.[4]

---

[1] Robert Lighthizer, "Opening Statement of USTR Robert Lighthizer to the House Ways and Means Committee," February 27, 2019, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/february/opening-statement-ustr-robert.

[2] Paul Triolo, Graham Webster, Lorand Laskai, and Katharin Tai, "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities," *DigiChina*, New America, May 2, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

[3] Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *CSIS Briefs*, Center for Strategic & International Studies, August 2 2018, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

[4] BSA | The Software Alliance, "Special 301 Submission," February 8, 2018, https://www.bsa.org/~/media/Files/Policy/Trade/BSA2018Special301.pdf.

- **Second, Chinese standards also create a competitive advantage for Chinese companies.** Chinese companies may not have the same concerns foreign companies do about providing sensitive information to the government as a condition of meeting the standards. Chinese regulators may also deem Chinese companies as being more secure under the vague criteria contained in the standards simply because they are local and therefore perceived to be more "secure and controllable" and without influence from foreign governments.

- **Third, to comply with some standards, foreign firms may need to redesign products for the China market where they are not compatible with international standards.** This is not only costly, but also creates interoperability issues with global markets.

Beijing uses vague language in standards, like in many Chinese laws and regulations, to avoid issues, such as World Trade Organization (WTO) challenges, while allowing the government maximum flexibility and discretion to apply onerous provisions when it sees fit. Internationally Beijing must disclose required standards to the WTO. However, in 2017 the government downgraded over 1,000 Chinese standards submitted to the WTO from required national standards to recommendations.[5]

Although officially most standards are deemed "recommended," in practice many may often be required to do business in China. This is the case when standards are listed as procurement requirements for government or state-owned enterprises. Beyond government customers, some Chinese customers may not buy from vendors who lack a certification associated with certain standards. There have been cases in which customer deals do not go through because a product lacks a certain certification.

Many more standards are likely to come, as Beijing is still only in the early stages of a national effort to build out its cybersecurity standards regime. Many existing standards are still only in draft form.

For more details on China's cybersecurity standards regime, please see the report I wrote in my previous position at the Center for Strategic & International Studies.[6] The report includes our translation and analysis of more than 300 standards dating back to 2015, when the Cybersecurity Law drafting process began.

[5] "396-xiang Qiangzhixing Guojia Biaozhun Feizhi 1077-xiang Qiangzhixing Guojia Biaozhun Zhuanhua" [396 Mandatory National Standards Abolished, 1077 National Standards Transformed], Ministry of Commerce of the People's Republic of China, April 1, 2017, http://chinawto.mofcom.gov.cn/article/i/ac/201704/20170402545384.shtml.

[6] Sacks and Li, "How Chinese Cybersecurity Standards Impact Doing Business in China."

2. Data Localization

Restrictions on cross-border data flows represent one of the top problems for U.S. companies in China. According to Article 37 of China's Cybersecurity Law: "Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China."[7] Depending on how it is implemented, this provision could require certain kinds of data to be stored within mainland China and require security approvals for cross-border data transfer.

The Chinese government is still defining "personal information" and "important data," as well as what sectors fall under "critical information infrastructure" (CII), under separate measures still in draft form,[8] but there are concerns that the scope could be vast and ambiguous.[9]

As the government finalizes these draft requirements amid much internal debate, it is important to keep in mind that there are also competing voices in China advocating for more alignment with international practices. Key players in China's private sector have argued that cutting off cross-border data flows will hurt the country's global economic goals; in fact, one of the main reasons why Beijing has yet to finalize the cross-border data flow measures is that there has been so much pushback from Chinese industry seeking global markets.

3. Leadership in Technology Norms and Governance

Artificial intelligence (AI), the Internet of Things (IoT), and the collection and use of the data involved present new challenges when it comes to technology norms and governance. The rules do not yet exist when it comes to complex questions related to ethics, safety, privacy, and discrimination.

Chinese scholars, practitioners, and the government are beginning to grapple with these challenges in often positive ways. There is a growing field of public conversations and legal scholarship in China devoted to topics ranging from the right to contest algorithmic decisions to

---

[7] A translation of China's Cybersecurity Law is available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[8] "Measures on Security Assessment of Cross-border Transfer of Personal Information & Important Data (Draft for comment)" and separate standard Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (draft for comment) together are meant to flesh out technical guidelines assessing cross-border data transfers. LINK See also Samm Sacks, Paul Triolo, and Graham Webster, "Beyond the Worst-Case Assumptions on China's Cybersecurity Law,' *DigiChina*, New America, October 13, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/

[9] According to the latest publicly available draft, all "network operators" will be subject to assessments before exporting data out of China. In practice, this could mean anyone who owns and operates an IT network. Industry sources report the government may have walked this back recently to focus just on CII operators, but there is still tremendous regulatory uncertainty given that the definition of CII itself is up in the air. The May 27, 2017, version gives a sweeping definition of "important data," spanning that which can "influence or harm the government, state, military, economy, culture, society, technology, information ... and other national security matters."

bias and discrimination in AI—similar questions under discussion among leading AI thinkers in the United States.[10]

Last year, China took a major step in asserting leadership in AI governance by hosting a major international AI standards meeting in Beijing and publishing an AI standards white paper that underlined the need for rules of the road when it comes to AI ethics, privacy, and safety.[11] Chinese authorities see this as a way to take a leading role in international governance, reflecting long-standing concerns that Chinese representatives were not at the table to help set the rules of the game for the global Internet. The Chinese government wants to make sure that this does not happen with the next generation of transformative technology, now that China has become a technology power with a sizeable market and leading technology companies.

With AI governance still in its early stages, it is too early to know what approach China will take; however, in some areas there are very troubling indications when it comes to the Communist Party's vision for the use of technology.

Reputable reports say that in Xinjiang, the government is detaining large numbers of 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 as many as one million people affected.[12]

It is not clear whether the Chinese government plans to expand the model for how technology is being used by security services in Xinjiang to other parts of China, but we cannot ignore that possibility that it could in the future.

There is tremendous uncertainty in China and the rest of the world about how to shape rules and norms around new technologies in ways that will bring benefits to humanity. China aspires to play a leading role in this conversation in ways that will have ramifications for U.S. companies doing business in China, and, more broadly, for the formation of global governance frameworks for the use of technology.

---

[10] I recently participated in a Track 2 dialogue on privacy with Berkeley Law and Peking University Law. The link to the public portion of the conference is available here: https://www.law.berkeley.edu/research/bclt/bcltevents/2019-privacy-and-cybersecurity-law-developments/agenda/.

[11] Jeff Ding, Paul Triolo, and Samm Sacks, "Chinese Interests Take a Big Seat at the AI Governance Table," *DigiChina*, New America, June 20, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/.

[12] Josh Chin and Clemente Burge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal*, December 19, 2018, https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355.

Recommendations for U.S. Policy Toward China

As Ambassador Lighthizer testified last week, the U.S. government is engaged in "very intense, extremely serious, and very specific negotiation with China on crucial structural issues."[13] This presents a window for achieving meaningful change that should not be squandered.

I have five recommendations:

1. **Adopt a "small yard, high fence" approach.** The question is how to address the challenges posed by China in a way that does not undermine ourselves in the process. In a recent article for *Foreign Affairs*, my colleague Lorand Laskai and I argue for an approach based on what the former Secretary of Defense Robert Gates called "small yard, high fence." This means being selective about what technologies are vital to U.S. national security, but being aggressive in protecting them.[14]

   Overreach in the form of blanket bans, unwinding global supply chains, and discrimination based on national origin is not the answer. Tools like the Committee on Foreign Investment in the United States (CFIUS), export controls, and law enforcement are designed to be used as scalpels, not blunt instruments.

   Overreach has costs for U.S. security, competitiveness, and innovation. As my New America colleague Graham Webster writes for *MIT Technology Review*, there may be greater harm to U.S. interests in viewing China's technological ambitions as an existential struggle between two competing blocs.[15] That is because the United States and China belong to an interconnected system when it comes to research, development, and manufacturing. 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. Today, government scientists have been replaced by international corporations and diffuse global networks of entrepreneurs, researchers, and venture capitalists.[16]

---

[13] Lighthizer, "Opening Statement of USTR Robert Lighthizer to the House Ways and Means Committee."
[14] Lorand Laskai and Samm Sacks, "The Right Way to Protect America's Innovation Advantage," *Foreign Affairs*, October 23, 2018, https://www.foreignaffairs.com/articles/2018-10-23/right-way-protect-americas-innovation-advantage.
[15] Graham Webster, "The U.S. and China Aren't in a Cold War, So Stop Calling it That," *MIT Technology Review*, December 19, 2018, https://www.technologyreview.com/s/612602/the-us-and-china-arent-in-a-cold-war-so-stop-calling-it-that/.
[16] Laskai and Sacks, "The Right Way to Protect America's Innovation Advantage."

Innovation flows both ways across the Pacific. China is emerging as an AI powerhouse, with Chinese start-ups excelling in several areas, including computer vision, speech recognition, and machine translation. If U.S. companies are to have any chance of keeping up, they will need access to Chinese research, talent, and expertise.

2. **Targeted demands in China trade talks.** As U.S. and Chinese negotiators work to complete a trade deal, the U.S. side should structure its demands of Beijing to focus on the following issues which will have significant effect on the ability of U.S. companies to do business in China. By prioritizing the following three issues, the U.S. side may have a shot at achieving more than just a cosmetic deal with Beijing. These do not require that Beijing dismantle state capitalism or abandon its technological ambitions, but they could result in meaningful changes for doing business in China:

    a. **Standards:** Since China's standards regime is still taking shape, this is an area upon which the United States should press Beijing. The Chinese government should commit to revise regulations and standards that pressure U.S. companies to disclose source code, encryption keys, and other sensitive information such as proprietary product specifications in exchange for market access. Any government reviews should be conducted in a non-arbitrary and transparent manner, and include international third-party accredited bodies.[17]

    b. **Data Flows:** Beijing has yet to finalize the scope of what kind of data must be stored locally under the pending definition of critical information infrastructure. Beijing should commit to allow more commercial data to exit the country without undergoing opaque and arbitrary security audits. The final version of the relevant regulations on the issue should spell this scope out in clear terms. Beijing should also sign onto the Asia-Pacific Economic Cooperation's (APEC's) Cross Border Privacy Rules System (CBPRs)[18] to facilitate cross-border data transfers with the United States. Since Beijing is concerned with new U.S. restrictions on U.S. citizen data under the expanded CFIUS regime, the U.S. side should agree to its own security reviews involving access to U.S. citizen data in a narrow fashion.

    c. **IP Theft:** On IP theft, Beijing should commit to impose criminal penalties, including jail time (not just fines) against individuals as a deterrent against IP theft. It also should agree to put in place measures that protect confidential business information during government review processes, including a dispute channel to address conflicts of interest and the types of information requested, according to the U.S. China Business Council.[19]

---

[17] BSA | The Software Alliance, "Special 301 Submission."
[18] See: http://cbprs.org/.
[19] US-China Business Council, "US-China Business Council Statement on Section 301 Report," March 22, 2018, https://www.uschina.org/media/press/us-china-business-council-statement-section-301-report.

Robust verification measures should be put in place to backstop commitments made by Beijing. China did not live up to its commitments not to conduct cyber industrial espionage under the 2015 Xi-Obama cyber agreement. A compliance monitoring system focused specifically on IP and tech transfer should be used to scrutinize practices, procedures, and systems of violators.

3. **Work with China on setting norms for emerging technologies.** As governments around the world grapple with how to set norms and shape governance for emerging technologies, the United States benefits from cooperation and exchange with Chinese officials, companies, and policy thinkers. There are risks to losing visibility and insight into what China is doing on this front. It is in the U.S. interest to work with China to set rules on AI ethics and safety. Joint research and other partnerships provide this lens and channel.

4. **Coordinate with allies and partners to create international pressure on Beijing.** Multilateral pressure has proven successful in the past. For example, in 2009 a coalition including the United States, Japan, and Europe combined efforts to pressure the Chinese government to suspend a requirement that screening software ("Green Dam Youth Escort") with surveillance capabilities be installed on computers sold in China. The United States should build upon the alliance structures that have been successful since the end of World War II. Unilateral action will not only compel China to retaliate against U.S. companies; it will make Beijing double down on the very structural problems we want to address, feeding Beijing's own narrative about cybersecurity governance.

5. **The United States must play offense by investing in its own R&D, infrastructure, STEM education, and a capital market that rewards investment.** China will continue to invest in closing the technology gap with the United States regardless of our actions, so the United States must be able to compete through its own technological and economic leadership.