Statement Before the

House Energy and Commerce

Subcommittee on Communications and Technology

"Telecommunications, Global Competitiveness, and National Security"

A Testimony by:

Samm Sacks

Senior Fellow

Technology Policy Program

Center for Strategic and International Studies

May 16, 2018

2123 Rayburn House Office Building

Chairwoman Blackburn, Ranking Member Doyle, and Members of the Subcommittee, thank you for holding this hearing and for the opportunity to address these critical issues for U.S. economic and national security. My testimony today reflects my experience as an analyst of Chinese technology policy for more than a decade. I have not only worked with the U.S. government, but also in the commercial sector with leading multinational companies in China. The complex structural challenges posed by China's approach to technology and industrial policy require a deep understanding of both the commercial and strategic security dimensions of our trade and investment relationship.

The Challenge

The Chinese leadership is in the midst of building the most extensive governance system for cyberspace and information and communications technology (ICT) of any country in the world. A blend of national strategies, laws, regulations, and standards make up President Xi Jinping's vision of building China into a "cyber superpower" and "science and technology superpower."[1] Recognizing that technology has advanced more quickly than the government's ability to control it, Beijing has moved to rapidly to construct a policy and legal framework that will strengthen the Communist Party's hand not just over online content, but also the digital economy and the hardware and software that undergirds the internet.[2] President Xi has repeatedly stressed the need to bolster China's domestic ICT industry in order to reduce reliance on foreign core technologies.

The build-out of China's ICT governance system has implications for U.S. companies operating in China, as well as for Chinese investment flowing into the United States and globally. As this system takes shape, an accurate understanding of its elements and practical effects will be key for U.S. policymakers to calibrate the right response. There are substantial challenges from a national security and commercial perspective. Yet, U.S. and Chinese technology development, supply chains, and commercial

[1] https://www.csis.org/analysis/cyber-policy-and-19th-party-congress.
[2] https://www.csis.org/programs/technology-policy-program/technology-and-innovation/cybersecurity-and-governance/china.

markets are tightly intertwined in such a way that we risk undermining our own economic prosperity and our ability to maintain leadership in technology innovation without a targeted approach.

What Beijing Requires of ICT Companies in China

China's Cybersecurity Law (which took effect in June 2017) is the centerpiece of a much broader ICT regulatory system made up of dozens of interlocking parts. There are three main ICT regulatory concerns for U.S. companies operating in China: "black box" cybersecurity reviews, restrictions on cross-border data transfer, and an overall trend toward localization under the guise of security.

Cybersecurity Reviews

U.S. companies now face at least seven different ICT security reviews that can be used for political purposes to delay or block market access. These reviews will be conducted by different Chinese government agencies with unclear jurisdictions. There is even conflicting jurisdiction within individual reviews. Moreover, the specific criteria, metrics, and, in some cases, those conducting the evaluations are not known. As several U.S. industry representatives put it, the reviews are essentially a "black box" because we do not know what they entail and what is required to pass them. Some have lobbied the Chinese government to accept international security certifications (such as through ISO) as a basis for compliance, but so far it is not clear if Chinese authorities will recognize these certifications or still require their own reviews. Since there is no transparency into the process, these reviews can easily become political tools. The different cybersecurity reviews are discussed below:

1. The Multi-level Protection Scheme (MLPS): MLPS is managed by the Ministry of Public Security (MPS) and has existed since 2006. MLPS will likely undergo revisions as part of the new ICT legal regime, but coming changes, as well as how it will be coordinated with other similar security reviews, remain unknown. MLPS involves ranking networks by level of sensitivity, and then assigning certain compliance obligations.

2. Cybersecurity Review Regime: A key question is how MLPS will work in relation to a new review known as the Cybersecurity Review Regime (CRR) or Cybersecurity Review Measures of Network Products and Services. Issued in "interim" form in June 2017, the measures require network products and services used in critical information infrastructure (CII) to undergo a cybersecurity review administered by the Cyberspace Administration of China (CAC) and other sector-specific regulators. Some industry experts believe that the CRR will involve inspections of the backgrounds and supply chains of network and service providers. The final definition of CII is still pending, and the full criteria for assessments and list of those conducting them are unknown. Yet, without these pieces of the puzzle, the practical implications of this system remain murky.

   The Chinese government has begun to issue several other documents meant to provide more clarity on the scope of the new review regime. These include the "Public Announcement on Issuing Network Key Equipment and Cybersecurity Special Product List (First Batch)," which outlines a list of products and services subject to the review and certification. There are also at least three relevant standards that have not yet been officially published. Yet, the follow-on product list and standards do little to narrow the far-reaching scope of the CRR. That is because the "interim" document establishing the CRR states that the review will focus on "other risks that could harm national security"— essentially preserving government authority to interpret the scope of reviews however it wants. Again, this is a channel that opens the door for political whim to determine market access.

3. Reviews of Cross-border Data Transfer: There will also be separate security review of data that companies seek to transfer outside of mainland China. The government is in the process of refining the process and conditions under which data would undergo a security assessment under two draft regulations: Personal Information and Important Data Cross Border Transfer Security

Evaluation Measures and Guidelines for Data Cross-Border Transfer Security Assessment. The specific scope is not yet clear, but according to industry sources inside China, it is likely that Chinese authorities will take a broad and ambiguous approach to enforcement of this particular review. (See following section on "Data Localization.")

4. Cross-border Communications: Although not a security review per se, companies operating in China must have authorization from the Ministry of Industry and Information Technology (MIIT) for using internal company VPN (virtual private network) services. In practical terms, this means that the government reviews and approves the channels that companies use for all of their international connectivity. Requirements issued by MIIT in 2017 mandate that companies only use internal VPN services from licensed providers, which are the three state-owned telecommunications carriers. Cloud service platforms must route communications with their overseas facilities through channels approved by MIIT.

5. Internet Technologies and Apps: New technologies and apps used in internet news/information services also have a new security review process. Service providers must conduct security evaluations before the introduction of new technologies or applications on their platforms, but details are also murky.

6. A Possible Chinese Version of CFIUS: Much less is known about another possible kind of security review of foreign investment that has yet to emerge. China's National Security Law (released in 2015) suggested in broad language there could be a new body perhaps akin to CFIUS. There has yet to been further clarification. New legislation expanding the scope of CFIUS could trigger Beijing to move forward setting up this new mechanism.

Data Localization

Many U.S. firms in China already assume that data localization requirements will become the de facto reality for their China operations. The specific scope of data localization requirements is still in flux; yet, some Chinese companies have even stopped sending their data to foreign companies that had the ability to store and process data within mainland China, despite there being no set requirement for them to do so. There are provisions still in draft form that would require certain kinds of data to be stored within mainland China and require approvals for cross-border data transfer. Below are the relevant laws, measures, and standards on the issue:[3]

According to article 37 of China's cybersecurity law: "Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." The government is still defining "personal information and other important data" or what sectors fall under "critical information infrastructure" under separate measures and guidelines, but early indications suggest even follow-on directives will be vast and ambiguous. This also underscores the fact that China's ICT legal framework is best understood as a matrix of overlapping parts. Recently, Chinese officials have been asking U.S. government and business leaders for advice on how to define critical information infrastructure, suggesting the parameters are still in flux and open to interpretation.

Following on the Cybersecurity Law, the Chinese government issued a measure and standard meant to clarify the scope of how restrictions on cross-border data transfers will be implemented. The problem is that these follow-on directives are equally vague and leave issues unresolved as different stakeholders within the Chinese system debate their meaning. First is the "Measures on Security Assessment of Cross-border Transfer of Personal Information & Important Data (Draft for comment)." Companies have until December 2018 to comply. Several internal versions of the draft have been quietly circulated in the past few months. According to the latest publicly available draft, all "network operators" will be subject to

[3] https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

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. In addition, the National Information Security Standardization Committee (TC260)—China's cybersecurity standards body—issued a standard to flesh out technical guidelines assessing cross-border data transfers.

Yet, the language even of this technical standard is extremely vague and far-reaching. The May 27, 2017 version gives a sweeping definition of "important data" that echoes the National Security Law, spanning that which can "influence or harm the government, state, military, economy, culture, society, technology, information . . . and other national security matters." "Network operators" could mean anyone who owns and manages an IT network, raising the possibility that e-commerce could be deemed CII given all the personal data held by companies like Alibaba and Tencent. Depending on how CII is ultimately defined, many companies that are not in ICT sectors could potentially fall in scope. Chinese regulators are now studying how countries like the United States define CII through numerous Track 1.5 dialogues. While regulators are showing a willingness to engage and dialogue, it is not clear how these exchanges will ultimately impact Beijing's policy trajectory, particularly since Beijing views this as primarily a national security rather than trade issue.

While China's regulatory regime for data flows looks bleak, it is important to keep in mind that there are also competing voices in China advocating for more alignment with international practices. These voices should not be disregarded by U.S. policymakers. Key players in China think that cutting off cross-border data flows will hurt the country's global economic goals. From national tech champions like Alibaba seeking global markets, to Chinese financial institutions facilitating global transactions, cross-border data flows are a core operational reality. These voices also exist within the Chinese government. For example, Hong Yanqing, who leads the personal data protection project for TC260, writes: "A fundamental consensus has emerged today that data naturally flows across national borders, that data flows produce

value, and that data flows can lead to flows of technology, capital, and talent." These players could be important allies for the United States.

Localization Push under "Secure and Controllable"

U.S. companies face de facto localization pressures in China even in the absence of specific regulation. The Xi Jinping administration has emphasized through multiple channels that it seeks to bolster China's domestic ICT industry to reduce reliance on foreign core technologies.[4] A report by the National People's Congress in December underscored the need for China to develop "indigenous and controllable core cybersecurity technology by 2020." While there is official definition of what the government means by "core technologies," authoritative documents indicate that the government is doubling down on indigenous development in fields such as advanced semiconductors, operating systems, cloud system, and the hardware and algorithms behind artificial intelligence systems.[5]

For several years, the government has used the phrase "secure and controllable" or "indigenous and controllable" in national strategies and directives as a way to link localization with security. Chinese companies have a competitive advantage when it comes to meeting these new security standards. This puts foreign ICT companies in a weaker negotiating position, and adds to pressure that they cooperate with local partners, rather than attempting to go it alone in the market.

The phrase has appeared in separate rules and strategies for cyberspace and the ICT industry. The phrase appears in sector-specific insurance, medical devices, and the Internet Plus sectors (i.e., smart technology, cloud computing, mobile technology, and e-commerce). A requirement for banking-sector IT to be "secure and controllable" was technically suspended, but many report that it still has negatively impacted market share. The phrase is also sprinkled throughout national-level blueprints for ICT

[4] http://www.xinhuanet.com/2018-04/22/c_1122722221.htm.
[5] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

development. For example, the 13th Five Year Plan for Informatization calls for "building a secure and controllable IT industry ecosystem.

Because this standard has no single definition, the government and Chinese industry have broad discretionary authority to launch intrusive security audits or reject foreign suppliers altogether as not secure. And while many of these regulations are still pending, Chinese government and industry are already moving forward with informal implementation of the standard, by asking foreign vendors to certify that they are "secure and controllable."

Why the China Market Matters

Why do U.S. companies stay in such a high-risk and restrictive market? The answer is the size of the market—which accounted for $23 billion of U.S. ICT exports in 2017—and its importance in the global supply chain. In addition, if major U.S. companies cannot operate and offer services in China, then they cede ground to Chinese companies since customers need to operate globally.[6]

China is not closed to all U.S. ICT firms or those with a digital footprint in the market. But the costs required to operate in China are increasing, particularly in high-tech sectors. Issues include ICT infrastructure—from trouble using corporate VPNs to the need to build local data centers—and lack of transparency around new licensing and security certifications that can be used to delay or block market access. Taken together, these new regulatory risks are now leading companies to reassess the tradeoffs required to make it in this important market.

Recommendations

There are substantial national security and commercial risks to the United States posed by China's ICT policies and approach to developing its domestic industries. We are correct to address these issues and seek areas where we have substantial leverage with the Chinese government. After all, Beijing does not change its behavior absent external pressures.

[6] https://www.finance.senate.gov/imo/media/doc/11APR2018GARFIELDSTMNT.pdf.

The challenge is that U.S. and Chinese technology development, supply chains, and commercial markets are tightly intertwined. A unilateral approach that isolates the United States will undermine U.S. economic prosperity, our technological leadership, and capacity for innovation. In confronting China, we must have a clear understanding about the consequences of our actions, and where there will be costs to ourselves. I have three recommendations:

First, we should 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.[7]

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. Indeed, the Chinese government has drawn up retaliation lists of U.S. companies in China. U.S. companies with viable domestic competitors in China will be particularly vulnerable, and may see licenses canceled or denied under the umbrella of cybersecurity reviews and certifications, particularly of network products and services. This is not just a commercial issue, but also undermines security since many multinationals in China would be forced to rely on Chinese ICT companies for their business operations if US ICT companies left the market.

Second, we need channels to work with those Chinese private sector players whose interests are actually more aligned with ours than some may expect. There are examples in which Chinese industry has been an important ally to U.S. companies on pending regulatory issues. Companies like Alibaba looking to expand into global markets have an interest in allowing data to flow across borders. Since much of China's ICT regulatory system is still in draft form, now is an important window to work with Chinese industry to push Beijing toward alignment with international best practices. The government cannot meet its goal of

[7] https://www.finance.senate.gov/imo/media/doc/11APR2018GARFIELDSTMNT.pdf.

having "big and strong Chinese internet companies" that can compete globally[8] if these players are hindered by their own government. These local champions will become less helpful as trade tensions spill over to affect the broader bilateral relationship.

Third, we must play offense by investing in our own research and development (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 we must be able to compete through our own technological and economic leadership.[9]

[8] http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm.
[9] https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180126_Lewis_MeetingChinaChallenge_Web.pdf?ccS38O06FR8XG_yUn7GS1YrJXOTCZklM.