06

Beijing's Cyber Governance System

Samm Sacks

China is in the midst of building perhaps the most extensive governance system for cyberspace and information and communications technology (ICT) of any country around the world. Recognizing that technology has advanced more quickly than the government's ability to control it, Beijing has moved to rapidly to construct a policy framework spanning cybersecurity, the digital economy, and online media content—all under one mantel.

A matrix of national strategies, laws, measures, regulations, and standards together make up China's vision to become a "cyber superpower" and build a robust ICT governance system. These elements are mutually reinforcing, and lay out requirements that cover data transfer, data privacy, critical information infrastructure, internet content, and ICT industrial development.

The build-out of China's ICT governance system has implications both for U.S. companies operating in China, as well as for Chinese investment flowing into the United States and globally. For U.S. companies, regulatory uncertainties and costs for operating in China are rising, compelling many to reassess the tradeoffs required to be in China. At the same time, there are major national security and trade implications for the global expansion of Chinese firms and capital in ICT sectors. As this system takes shape, understanding the overall framework as well as its individual elements will be key for U.S. policymakers. Some parts are final, but many are still pending as stakeholders within the Chinese bureaucracy continue to debate their scope and implementation.

Understanding China's emerging cyber regulatory system will be critical in order to craft a precise and targeted U.S. policy response as U.S.-China trade risks grow. Calibrating the right approach to the challenges posed by China must begin with an accurate view of this complex system, one that is often misunderstood by outside observers.

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 foreign 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.

ICT Security Reviews

Foreign companies now face at least six different 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.

Coming actions to expand the scope of the Committee on Foreign Investment in the United States (CFIUS) could lead Beijing to likewise use these security reviews as channels to retaliate against U.S. companies operating in China. Since there is no transparency into the process, these reviews can easily become political tools, with U.S. companies on the frontlines as bilateral tensions increase.

The different cybersecurity reviews, and their practical implications, 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, 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 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:* In addition, 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. Again, 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:

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 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 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." Again, "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.

China vs. EU and APEC on data restrictions

These reviews are not comparable with requirements under international regimes such as the voluntary Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) or the EU's General Data Protection Regulation (GDPR). The EU views data protection primarily through the lens of user privacy. In contrast, passing one of the Chinese reviews for outbound data transfer is linked not merely to personal privacy or raw data security, but also to "national

security" and broader, more ambiguous concerns like "the people's livelihood" (Cybersecurity Law Article 31) or "economic development and social and public interests," according to the guidelines. Some industry groups are hoping that China might accept CBPR in place of their own data review system, but this looks unlikely given that China appears to want its own system.

Internal Debate within China over Data Flows

While China's regulatory regime for data flows looks bleak, 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"

Foreign 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. The most recent is a report by the National People's Congress in December underscoring the need for China to develop "indigenous and controllable core cybersecurity technology by 2020."

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 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."

Beijing's Vision for Making China a Global ICT Superpower

What makes China's cyber governance system so vast is that it does not just cover cybersecurity, but also establishes a top-down plan for advancing China's domestic ICT industry. Multiple overlapping strategy and planning directives all stress the need for China to be a global leader in advanced ICT, with Chinese companies at the forefront. These are not just empty slogans, but supported by detailed policy blueprints laying out the government's goals to reduce reliance on foreign technology to boost self-sufficiency in key fields, while increasing the global influence of China's national tech giants.

The "Made in China 2025" has received the most attention outside of China, but when it comes to ICT sectors there are other, more detailed policy directives spelling out what Beijing hopes to achieve. Three recent examples, summarized below, stand out as especially clear articulations of Beijing's objectives (there are many more):

- During President Xi Jinping's opening speech at the 19th Party Congress in October 2017, he called for the "deep integration of the Internet, big data, and artificial intelligence with the real economy" and for building a "science and technology superpower, quality superpower, aerospace superpower, cyber superpower . . . advancing the development of big data, cloud computing, and smart cities so as to turn them into a digital silk road of the 21st century." The speech marked the first time that an opening speech identified specific terms such as artificial intelligence (AI) and "digital China," suggesting these sectors will be priorities for Xi's second term.

- China's 13th Five Year Plan for Informatization (2016–2020) states that China strives to "no longer [be] restrained by others for core technologies in strategically competitive fields," and identifies major projects slated for increased state support in "core electronic equipment, high-end universal chip, basic software, large-scale IC, next-gen wireless broadband mobile communication, quantum communication and quantum computing."

- Another example is language from an article published in September (just ahead of the 19th Party Congress) in a leading Party Journal by the Theoretical Studies Center Group under the Cyberspace Administration of China. The essay explains how to put into action President Xi's call for making China into a "cyber superpower." Among the many points in the essay, the authors write: "The global influence of Internet companies like Alibaba, Tencent, Baidu, Huawei, etc., is on the rise. . . . In 2016 on a global list of top 20 companies by market value, Chinese companies occupied seven slots."

Recommendations

China is certainly 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 be in the market.

There are real national security and commercial risks to the United States posed by China's ICT policies. In this context, it is understandable that U.S. policymakers are seeking a more confrontational policy stance, using a package of actions beyond just high-tech sectors, including: coming announcements about the 301 investigation, CFIUS reform, and a broader Trump administration China strategy.

The problem is that without a targeted approach, U.S. businesses are likely to become collateral damage in a trade war between the United States and China that does not benefit either side. U.S. companies in high-tech sectors are likely to bear the brunt of the damage. Here is what is likely to play out in 2018 depending on how both sides manage coming risks to the relationship:

First, in anticipation of coming announcements on the 301 investigation, the Chinese government is already drawing up retaliation lists of U.S. companies in China. U.S. companies with viable domestic competitors in China will be particularly vulnerable to retaliation. In the ICT sector specifically, U.S. companies with domestic Chinese counterparts may see licenses canceled or denied under the umbrella of various cybersecurity reviews and certifications. The various cybersecurity reviews (discussed in section one) could become political channels for the government to delay or block market access in sectors where network products and services are subject to black box reviews.

Second, if backed into a corner, Beijing is not likely to engage further in exchanges that have become an important channel for sorting out implementation of cyber policies and laws. There are informal and Track 1.5 or Track 2 channels that could come to a halt, leading to more hardline positions on still-unresolved ICT regulatory issues. To be sure, some have found the Chinese side to be less responsive in these channels, but there are in fact notable exceptions.

For example, in April 2017 the Chinese government faced significant backlash from foreign and domestic industry when it released the first draft of measures that all "important data" remain inside mainland China. In response, and after extensive back and forth with industry, Chinese authorities revised the scope to only require that data from critical information infrastructure (CII) operators be stored locally. They also moved back the date for compliance. Since the definition of CII is still unresolved, the issue remains problematic, but it shows that Beijing is willing to take a more nuanced position under certain circumstances. There are other examples in which Chinese domestic industry have been important allies to U.S. companies on pending regulatory issues, despite being competitors. These local champions will become less helpful to U.S. partners as trade tensions spill over to affect the broader bilateral relationship.

Looking ahead in 2018, Beijing has a draft encryption law in the legislative process. If enacted and enforced, the law could require only pre-approved domestic encryption products—a red line for many foreign companies in China. There are numerous other examples in which the U.S. tech sector stands the most to lose in a possible trade war between the United States and China.

U.S. and Chinese technology development, supply chains, and commercial markets are tightly intertwined in such a way that a sweeping approach to China's ICT policies will hurt U.S. economic prosperity and our ability to maintain our edge in technology innovation. U.S. policymakers need to tailor their reviews of Chinese commercial investments and punitive

damages in a way that does not further hinder U.S. companies operating in an already difficult Chinese market. The best approach is one that takes a more nuanced view of the U.S.-China trade and investment relationship to mitigate these downside risks.