15 June 2015
Samm Sacks, China Analyst, Eurasia Group

Testimony before the U.S.-China Economic and Security Review Commission:
Regulatory Barriers to Digital Trade in China, and Costs to US Firms

Key take-aways

- The Chinese government will press forward with stricter scrutiny of US technology suppliers given a determination on the part of the Xi Jinping government to deliver on long-held national security and domestic industrial innovation goals.
- The counterterrorism law and banking sector information technology (IT) regulations both remain in play despite reports to the contrary.
- US technology companies face greater risks now that they will be required to undergo invasive security audits, turn over source code, build local data centers, and provide the Chinese government with encryption access under a number of laws and policy directives.
- The Central Leading Small Group for Network Security and Informatization set up in February 2014 and chaired by President Xi is emerging as one of the most powerful elements within the bureaucracy and will consolidate the leadership's power to push forward national policies.
- Although hardliners have been empowered to shape China's foreign technology policies, China's political system is not monolithic. Some groups think localization will expose Chinese government and financial institution networks to security risks, while added compliance costs will impede innovation for emerging Chinese companies.
- A lack of full consensus, added security and compliance costs to Chinese industry and banks, and technological barriers for implementation mean that US firms will not lose market share at the pace and to the degree that some fear.
- Over the past year the Xi administration has shown a serious commitment to indigenous technological development that is unprecedented in scale, high-levels of government backing, approach, and vision—suggesting that China could show more progress on this front than in the past.
- But US firms will have to weigh the benefits of market access with added local data storage requirements, IP risks surrounding new licensing approvals, security reviews especially in online data transmission, and other forms of "soft discrimination."
- US policymakers and regulators should convey to the Chinese government the ways in which a hardline approach undermines objectives of President Xi's economic policy agenda – and how such policies can hinder Chinese companies as well as US companies.
- The US government should seek dialogue with Beijing with the goal of US companies having space for maneuverability in the final policy language, rather than provoking Beijing to dig in deeper and leave US companies with limited options for operating in China's market.
- The US government should also cooperate with other countries on developing a common set of best practices and guidance for operating in the China market.

Beijing appears unlikely to back down on IT policies requirements despite US pressure

The Chinese government will press forward with stricter scrutiny of foreign technology suppliers given a determination on the part of the Xi Jinping government to deliver on long-held national security and domestic industry goals. While there could be some room for compromise about timing, the extent of implementation for new requirements, and perhaps some of the ways in which these initiatives are implemented, Beijing is not likely to back down on its push to have more rigorous oversight and control over technology and information security, an area that has important implications for foreign intellectual property (IP). These development are leading to a fundamental shift in the business climate for US companies in a range of technology sectors, particularly for information technology (IT) but also in finance, next generation manufacturing, and energy efficiency.

Recent initiatives reinforce three distinct, high-level objectives by the Xi leadership. First, the government has a genuine concern about national security vulnerabilities as exposed in the Edward Snowden revelations in 2013. Second, President Xi has signaled a new commitment to driving technology innovation among Chinese industry as the government seeks to shift toward high value-add growth and promote the competitiveness of Chinese companies. Third, the government is expanding efforts to strengthen data security in the face of a rapid explosion in e-commerce, big data, and information transmission over the internet more broadly as it consolidates power. The Chinese government also is critical of the US for having double standards, maintaining that requiring encryption access is consistent with global standards.

There has been speculation in recent months about how far Beijing will go with localization efforts and plans to increase control over foreign technology. In March the US media reported that the counterterrorism law under review had been suspended following concerns raised by President Obama to President Xi; in April Beijing announced it would temporarily halt rules that increased restrictions on banks and their IT suppliers. But both policies remain in play despite reports to the contrary. In fact, there are now credible rumors that government officials are facing pressure to accelerate passage of the counterterrorism law this year, and the banking sector regulations are likely to be revisited as well.

Formal and informal tools to gain more oversight and control over foreign technology

Even if some parts of the regulations are diluted, Beijing is pressing forward with a spate of formal and informal tools that taken together will allow the government to assert more control and increase security and regulatory scrutiny of US technology companies in the next one to two years. US technology companies face greater risks that they will be required to undergo invasive audits, turn over source code, and provide the Chinese government with encryption keys for surveillance. Key legislation and policy directives that have emerged, are in draft, or are widely rumored include:

- A purge of foreign firms from a government-sanctioned procurement lists
- Restrictions on foreign equipment in the banking sector requiring suppliers to meet "secure and controllable" standards
- A draft counterterrorism law compelling telecom and internet companies to provide encryption keys to enable government surveillance and store data on local Chinese servers
- A new national security law that will expand Beijing's regulatory powers under a broad and far-reaching definition of national security and calls for sovereignty in cyberspace

- The creation of a cyberspace review body to evaluate security for all internet and IT products
- A new cybersecurity law or framework
- A 13th Five Year Plan for Software and Big data focused on boosting data security for SOEs, financial institutions, and government agencies

Among the laws currently under consideration, the counterterrorism law is perhaps the focus of the most high-level political attention right now that will increase the likelihood of its passage in the coming year. It is possible that Beijing could walk back the encryption access and localization requirements in the final version of the law, and use broad language that leaves space for discretion when it comes to implementation. However this alone would not mitigate risks to foreign firms given the overall policy environment and inclinations of the top leadership.

A second draft of the national security law came out in early May and is likely to be passed next year. Once enacted, this law will serve as the legal framework to bolster security across all sectors of the economy, including but not limited to internet and information technologies. While the final content of the law is not yet known, draft language reveal two worrisome developments. First, the provision of the law calling for cyberspace sovereignty suggests that the Chinese government is pursuing a policy strategy that could eventually over the long-term lead to fragmentation of the US-led global internet. Beijing is seeking to have a greater ability to control internet content as a tool to maintain stability. Second, this law is likely to serve as the legal basis for national security reviews of inbound investment—also proposed in the draft foreign investment law still under review—and could also lead to the creation of new bodies nationwide, akin to the Committee on Foreign Investment in the United States (CFIUS). Currently these security review bodies only exist within China's four free trade zones (FTZs) in Fujian, Tianjin, Guangdong, and Shanghai under a new pilot announced just in April. But initial content readings of the draft law suggest that these new bodies will take a more expansive approach to national security than CFIUS, providing justification for restricting foreign investment across sectors on the basis of strategic, economic, social, moral, ideological, and technical readings of national security.

The pace of cybersecurity policymaking is also accelerating in ways that suggest Beijing will look to assert greater sovereignty in cyberspace. Although drafting of the cybersecurity law or guiding framework is not as far along as that of the counterterrorism and national security law, Premier Li Keqiang indicated at the National People's Congress in March that completing a first draft would be a priority for 2015. In May the Ministry of Industry and Information Technology announced it will draft a five year plan for the ICT sector focused on improving network security, innovation, and global competitiveness. That same month the Shanghai Academy of Social Sciences (SASS) released its annual report on cybersecurity expressing concern that the US has too much influence over global cyber space and seeks to contain China's technology development. The SASS report—a full book length volume—provides a detailed compendium with research on topics including: security risks with next generation IT systems, developing policies and laws in cyberspace, online cultural security, development of the information security industry in an era of big data, and global internet governance.

Outside of formal policy channels, the government will take a more assertive approach to requiring companies to submit technology and IP for inspection. Purchasers may also face more pressure to

buy domestic. State and quasi-state sponsored hacking methods will also be used to help Beijing achieve these goals. Government officials are also pressuring banks, SOEs, private and quasi-private companies, and public institutions to purchase from local suppliers regardless of official policy.

The government will also treat banking IT as infrastructure slated for increased state support as the economy slows. There are a growing number of Chinese banks that will require significant investment in IT systems (both hardware and software), providing an attractive venue for the government to achieve these goals. These banks will help to generate increased demand for equipment as the government focuses on redirecting state resources to build up the domestic IT sector. Chinese IT companies geared toward financial systems stand to gain from more policy support and incentives.

Hardliners on localization and cyber sovereignty empowered within bureaucracy

These latest developments reflect the growing influence of hardliners on China's industrial and foreign technology policies. Within the Chinese bureaucracy, proponents of greater data localization, import substitution, sovereignty in cyberspace, and encryption access are exerting increasing influence over the policy agenda. Hardline policies on these issues are not new to Chinese policy landscape and have in the past been walked back by Beijing—for example in 2007 the Ministry of Public Security introduced a "Multi-Level Protection Scheme" prohibiting foreign companies from supplying core products for government, banks, and other critical infrastructure companies; a 2010 "Compulsory Certification for Information Security Scheme" required foreign companies to submit security product IP to the government. But what is different now is that direction is coming from the highest levels in the Chinese system under the direction of President Xi himself.

The Central Leading Small Group for Network Security and Informatization set up in February 2014 and chaired by President Xi is emerging as one of the most powerful elements within the bureaucracy and will consolidate the leadership's power to push forward national policies. Contrary to popular perception, China's cyber policy environment had been fragmented among military, civilian, industrial, and other state actors at both regional and central levels, leading to gridlock and inconsistent implementation. This group is more powerful than its equivalent under the Hu administration. Xi himself is the chair while the earlier group was chaired by Premier Wen Jiabao. Elevating the group from the State Council level to the Party level will enable better coordination among the State Council, National People's Congress, and the People's Liberation Army.

Overall the make-up of the group suggests that development of the internet has become a focal point across the industrial, financial, and telecom space. Inclusion of departments such as the National Development and Reform Commission, People's Bank of China, Ministry of Finance, and Ministry of Industry and Information Technology mean that there is support for boosting internet technologies across all areas of the bureaucracy. Of the 22 members of the group (President Xi and Premier Li Keqiang are the two top officials), roughly half have a status as the most senior rank among Party, military, and government officials.

But even as President Xi centralizes and consolidates power, it is important to keep in mind that China's political landscape is not monolithic and there are domestic players that are not necessarily supportive of the leadership's recent policy approach. A number of domestic companies have already voiced concerns to regulators, suggesting Beijing is using a top-down approach with limited

consultation and input from industrial stakeholders. Chinese companies are concerned that local suppliers lag behind when it comes to securing infrastructure, and recognize that prioritizing localization rather than market competition around the most secure systems will expose Chinese networks to security risks. Huawei's rotating chief executive Eric Xu remarked in April that hampering competition will stifle innovation. Small start-ups also stand to lose from these policies since the new standards will demand more resources to be compliant.

IT policies also reflect an unprecedented effort to boost homegrown technology under President Xi

The Chinese government has talked about driving indigenous innovation and boosting homegrown technology industries for years, but has had limited success building competitive Chinese brands and shrinking the technology gap with foreign companies. Indigenous innovation policies under the administration of the former President Hu Jintao were largely ineffective, helping to maintain a status quo in which China's economy weighted heavily towards low-end manufacturing and energy and investment-intensive heavy industries, relying on foreign suppliers in value-add technology sectors.

But since coming to power in 2012, President Xi has made clear that China faces an imperative to shift the economy to a more sustainable and efficient mode of growth. A critical item on his reform agenda has been redirecting state resources toward high technology sectors seen as boosting consumer demand and upgrading Chinese industry to give value-add productivity a greater role in the economy. Over the past year the Xi administration has shown a serious commitment to technological development that is unprecedented in scale, high-levels of government backing, approach, and vision—suggesting that China could show more progress on this front than in the past.

Beijing is using the China Manufacturing 2025 Plan (unveiled on 19 May) together with the Internet Plus Strategy (introduced in March at the National People's Congress) as the main channels to promote local high value-add technology sectors as the economy slows. The aim is to drive economic growth by integrating internet and information technologies with traditional industries, strengthening global competiveness of Chinese companies, and reducing reliance on foreign technology. Under the Internet Plus strategy, Beijing will focus state funding and policy support on advancing smart technology, mobile internet, cloud computing, big data, the internet of things, and e-commerce. Traditional industries targeted for upgrades using internet technology include manufacturing, logistics, finance, and health. The Made in China plan targets ten key sectors for support such as next generation IT and intelligent manufacturing and robotics.

The scale of Beijing's ambitions are evident in specific industry support plans. There are also signs that recipients of this kind of state support will be selected based on potential for return on investment, consistent with reform goals to give market forces a greater role in the economy. For example, the State Council also announced in May that the government will invest over 1 trillion RMB over the next three years in building internet network infrastructure. In June 2014 the government announced it had set up a 120 billion RMB central government equity investment fund for the integrated circuits industry, which the Chinese government views as the critical bottleneck of China's domestic IT capabilities. Regions and municipalities are also setting up their own funds in addition. A national cloud-computing strategy released in January will encourage infrastructure

upgrading for broadband and data centers and support domestic small- and medium enterprises (via preferential tax policies, financing, venture capital).

Separate Internet Plus plans are also coming out for individual sectors, providing some indication of how the government will prioritize and focus state resources under this policy. Examples include smart cars and logistics, including a stated goal of building 200 e-commerce pilots in cities nationwide and growing e-commerce trade volume by $3.7 trillion by 2016.

The Xi government is also increasing its political capacity to deliver on these objectives by centralizing power over IT and internet technology policy. In March MIIT announced that the government will set up a leading small group for strengthening national manufacturing to advance implementation of the Made in China 2025 plan. Together with the Central Network Security and Informatization Leading Small Group this manufacturing group will help streamline policy support for technology development, overcoming bureaucratic fragmentation.

Over 150 outside technology and industry specialists provided input on the Made in China 2025 plan over a two and a half year drafting process, lending more credibility to the plan's content. Beijing is also looking to outside experts at universities such as Tsinghua and state research institutes such as the Chinese Academy of Sciences and China Academy of Engineering for strategic input on the Internet Plus Strategy.

While the main beneficiaries of the plan will be Chinese companies with increased regulatory and localization risks for foreign firms, Beijing will also seek to lower formal barriers for foreign investment where domestic technology levels are weak. The main risks to US firms will be more "soft discrimination," intense competition from Chinese firms, and stricter security reviews. When the national security law, counterterrorism law, and cybersecurity law are passed there will also be added compliance costs and risks to core IP.

U.S. firms will still have opportunities in China market as formal barriers to entry in technology sectors comes down

Counter to the conventional view, the government does not want to fully prohibit foreign firms from the IT market, and, in fact, is taking steps to create new market opportunities for foreign technology firms in sectors like e-commerce and value-added services for telecom. This underscores a basic recognition in Beijing that foreign technology will be needed to support economic restructuring and industrial development goals as the economy shifts to a model of more efficient and sustainable growth. Beijing's aim is also to gain reciprocal market access for Chinese technology companies in global markets.

Moreover, foreign firms will not lose market share at the pace and to the degree that some fear because the government will have difficulty with implementation. Financial IT systems are highly complex and integrated, creating significant cost and technological burdens for Chinese banks. Domestic IT suppliers will lag behind foreign counterparts in technological capabilities for the foreseeable future, particularly when it comes to data security. Bureaucratic fragmentation will also be an impediment; MIIT, CBRC, and the Ministry of Finance are each responsible for different aspects of banking information systems. Lack of full consensus among Chinese users who recognize local options are not the most secure will also impede implementation.

Even the Made in China 2025 plan and Internet Plus Strategies will open new opportunities to US companies despite being targeted primarily at boosting China's domestic industry. The Made in China Plan specifically encourages more joint research and development (R&D) and overseas mergers and acquisitions (M&A) to gain access to foreign expertise and capital especially where indigenous capabilities are weak.

But the costs to U.S. firms of market access are rising

Even as these formal barriers to market entry come down, the costs of market access in these sectors will increase. Recent state support measures in technology sectors such as cloud computing and integrated circuits will primarily benefit domestic firms, increasing competition for market share and driving down prices as the technology gap shrinks. Competition from Chinese companies that have acquired IP from foreign partners will also intensify. Data localization requirements will add costs associated with building new data centers. US firms will have to weigh the benefits of market access with added local data storage requirements, IP risks surrounding new licensing approvals, and security reviews especially in online data transmission.

Recommendations for US policymakers

Beijing is likely to be less receptive to pressure from US officials than in the past given the current policy climate. Reports that Beijing had backed down on the counterterrorism law following a conversation between President Obama and President Xi proved unfounded. As a result US industry and policymakers will need to take a more proactive approach and be forward-looking in navigating increasing risks in China's policy environment.

As a result, it will be important for US companies to have space for maneuverability regarding the extent of the enforcement when these policies and directives are finalized. The US government should seek dialogue with Beijing with the goal of having the final regulatory language be broad and discretionary, rather than provoking Beijing to dig in deeper and leave US companies with limited options for operating in China's market. US companies will benefit from having a spectrum when it comes to implementation.

US policymakers and regulators should convey to the Chinese government the ways in which a their hardline approach undermines core objectives of President Xi's economic policy agenda – and how such policies can hinder Chinese companies as well as foreign companies. Selecting technology suppliers based on localization rather than market competition around the most secure systems will expose Chinese government and financial institution networks to security risks. Added compliance costs on Chinese technology companies will weigh especially on emerging technology start-ups at a time when Beijing is seeking to promote innovative small and medium sized companies. Data localization laws will hurt Chinese companies seeking foreign investment by restricting their ability to export information about credit. US policymakers should also focus on areas of leverage such as access to US markets for Chinese companies.

There is also a growing risk that these disputes set a negative tone for ongoing negotiations of the US-China Bilateral Investment Treaty (BIT). China's unwillingness to cede on new IT policies and national security exemptions could impede progress, especially if US companies continue to face market access problems related to technology transfer and localization requirements. The non-

discriminatory treatment provision of the BIT would be helpful to US companies on these issues, but Beijing does appear willing to apply this provision to the IT sector despite pressure from the Obama administration as negotiations on the negative list move ahead this year.

The US government should also work with international partners to come up a common set of best practices and guidelines. Countries with more cooperative trade relationships with China such as Germany or Japan could send a powerful message to Beijing working alongside US stakeholders.