USCBC THE US-CHINA BUSINESS COUNCIL
美中贸易全国委员会

OPTIMIZING CONNECTIVITY:
Recommendations for China's Information Technology Environment

November 2016

Information technology (IT) has created new channels for growth and revolutionized how companies do business. With the largest number of Internet users in the world, China has become a global hub for innovation in mobile application development, smart devices, ecommerce, mobile payments, and other frontiers of technology that integrate big data with internet-based functions to enhance traditional business models.

At the same time, governments worldwide are faced with the challenge of regulating the development and growth of new technology in ways that are efficient and safe for all users, while balancing appropriate governmental requirements with the needs of businesses and individuals. Chinese policymakers, like their counterparts around the world, are developing measures to address data privacy and information security, as the growth of new technology challenges traditional regulatory frameworks to adapt.

Seventy-nine percent of US-China Business Council (USCBC) members cited concerns about China's approach to information flows and technology security in USCBC's 2016 member survey, largely due to the impact those policies have on companies' ability to conduct day-to-day business. China's current regulatory regime affects the operations of companies — both foreign and domestic — in ways unseen in other markets. Many policies in China make it unclear if companies may use their global best practices in innovation and technology security in the country. As a result, companies are restricted from using many technology solutions that combine operational efficiency with globally-proven technological safeguards – including the exchange of information used to combat security threats - creating vulnerabilities in an increasingly global digital economy.

USCBC's recommendations explore some of the specific obstacles companies face when using information technology in China, are based on extensive interviews with company technology officers, and provide potential solutions that balance operating and security needs. They are proposed to provide constructive solutions to address the concerns of all sides in a practical manner. USCBC appreciates the opportunity to provide these recommendations and would welcome the opportunity to discuss them with Chinese regulators.

Challenge 1: DATA FLOWS AND LOCALIZATION

China's data policies disrupt communications between a company's China and its other global operations, stifle cross-border innovation, and increase the cost of business by requiring the installation of duplicative IT infrastructure. These policies also affect China's development plans such as Internet+ and the National Big Data Strategy by discouraging the use of companies' global expertise and technology. These restrictions impact foreign and domestic Chinese companies' ability to operate global platforms, carry out ecommerce and do cutting edge research and development (R&D).

Two types of data policies affect company operations:

- Data localization policies require the storage of certain types of data in China. These policies may require the use of local infrastructure for data hosting and processing, separate from what may be used globally in the rest of a company's operations.
- Data flow policies limit the movement of information across borders. Data flows are a critical component of a modern, international, digital economy that allow Chinese and foreign companies to maximize efficiencies among the countries in which they operate or ensure the integrity of financial transactions. Chinese regulations in financial services, healthcare, and other industries prohibit the flow of certain data across China's borders. In addition, China's current regulations make it unclear what types of data may be considered "state secrets," raising the risk that information may be transferred that unintentionally violates the law.

During interviews conducted by the US-China Business Council (USCBC) for a related report on information and communications technology (ICT) best practices in China, company technology executives said that China's data flows and localization policies make it difficult to use big data analytics in China for product support, security, or innovation. For example, energy companies that operate wind turbines in China need their fleets to be in constant communication with global headquarters, so their global teams can respond to power outages and prevent accidents. Companies that provide high-tech, internet-connected equipment used in "smart manufacturing" facilities require access to data from these devices so that they can remotely maintain or repair them. Companies that engage in international ecommerce rely on information flows to prevent international identity theft by tracking suspicious activity across borders. Financial services companies analyze data across borders to predict consumer trends, provide targeted services to customers, and identify potentially illegal transactions. Overly restrictive data regimes impede these types of activities and unnecessarily hinder the potential for companies to use global best practices.

While the goal of these types of policies might be to safeguard the security of citizens' personal information, regulations mandating data localization or forbidding cross-border flows do little to achieve that goal. The strongest international standards to protect data privacy are determined by industry consensus, draw on global best practices, and are largely blind to where data is stored or transferred. Cybersecurity experts agree that the type of technology used, expertise of users, and institutional good practice determine security, not the geographic location of data.

Ensuring the free flow of data across borders is an essential part of an innovative digital economy, the development of which China has made a priority. Chinese initiatives like the 13th Five-Year Plan, Made in China 2025, and Internet+ emphasize the development of smart- and internet-based technology. Speeches by senior officials regularly emphasize the importance of an open and interconnected internet both within China and under the G20 framework. These efforts can be strengthened by using the best practices and expertise offered by international companies, which have experience in integrating traditional business practices with global information networks. Allowing this information to be globally accessed by companies, support teams, and interactive products is a key component of "smart technology" — a goal of the 13th Five-Year Plan — and is necessary for successful high-level policy plans across sectors, such as Internet+, the Big Data Promotion Plan, and development plans for greater energy efficiency via smart cities or China's financial industry.

Recommendations

- Before releasing overly strict regulations, China should conduct a detailed analysis of the costs associated with restricting the efficient flow of data in an innovative and global digital economy, taking into account the associated costs for domestic industry, global commerce, research and development, and cyber-threat management. Based on that analysis, China should remove unnecessary security review regimes and data security licensing in order to allow its transfer across national borders. Chinese regulators should align data flow policies with internationallyproven cybersecurity best practices. This includes revising provisions in the Cybersecurity Law that unnecessarily restrict the efficient flow of information.

- China should provide a more detailed definition of the types of data that may be categorized as "state secrets" to ensure that companies do not unintentionally violate regulations on the storage and transfer of such information. This definition should be limited in scope so as to only include information that has a vital interest for national security.

- China should allow copies of data to be sent abroad for analysis and processing in order to ensure operational efficiency and encourage innovation by using big data. This would preserve territorial jurisdiction on the data while still allowing important business functions to be conducted.

- Chinese policymakers should consult with international industry on global best practices for secure data management. Such policies should be developed in a clear and transparent manner, pursuant to China's international obligations on regulatory transparency.

- China should engage in regular dialogue with other governments on cyber-related issues to ensure its policies use global best practices, understandings, and solutions to ensure an optimal regulatory regime. In addition, China should engage in bilateral and multilateral discussions regarding information exchange mechanisms related to law enforcement cases to ensure the resolution of international jurisdictional issues.

- China should promote a reliable and open internet to allow the flow of information necessary for companies to engage in innovation and international commerce. Chinese regulators should work with companies that operate internet-based businesses to develop solutions that will allow them to bring their services to Chinese users.

- China should become a party to the APEC Cross Border Privacy Rules System (CBPRS), which was developed to build consumer, business and regulator trust in cross border flows of personal information. Under CBPRS's framework, independent third-party accountability agents ensure that countries' and companies' data protection mechanisms are in line with the APEC Privacy Framework and meet a suitable and enforceable standard for citizens' privacy protection.

Challenge 2: MARKET ACCESS AND GLOBAL SOLUTIONS

Chinese and foreign companies are unable to use many innovative cloud computing solutions in China due to a lack of clarity in China's licensing regime. These policies complicate the cost, efficiency, and information security considerations for both foreign and domestic company operations in China.

For example, the 2015 Telecommunications Services Catalogue released by the Ministry of Industry and Information Technology (MIIT) set licensing requirements for basic telecommunications services (BTS) and value-added telecommunications services (VATS) for foreign and Chinese companies. While the Catalogue does not use the term "cloud computing," it does cover elements of cloud computing as part of VATS, an approach not used in other markets. As a consequence, to provide cloud solutions in China, companies must obtain three different certifications -- Internet Data Center (IDC), Internet Service Provider (ISP), and sometimes Internet Content Provider (ICP) licenses. Foreign companies are required to have partnerships with local players to obtain these licenses. While foreign companies may control up to 50 percent of such operations, some international companies have been unable to apply for or receive any of these licenses. As a consequence, many foreign cloud services are unavailable in China, forcing Chinese and foreign companies that use them outside of China for technical support and maintenance solutions to use different systems for their China operations.

Companies that purchase global cloud products have reasonable expectations of using them wherever they do business — one of the core purposes of cloud-based solutions. This affects the efficient communication between China-based and international teams, which in turn affects the use of cloud-based client-relationship management (CRM) software, the sharing of business documents between internal teams and with external clients, and the application of cloud technology used for hosting data and providing development platforms for R&D purposes.

While there are a number of local Chinese cloud solutions available, few of these solutions have a global presence, creating the same kind of impediment to the use of Chinese cloud technology around the world that China's policies create for the use of global cloud products in China. As a consequence, China's policies may create significant players in its domestic market, but fail to create global technology leaders – something competition with global industry leaders at home would remedy.

The inability to link global and China-based networks can also create security risks. Local software or local vendors may be unable to troubleshoot or communicate problems that come up in the use of global technology. When maintenance issues, technical problems, or criminal infiltration of networks occurs, a fractured global communications network limits companies' ability to rapidly respond.

Ultimately, these restrictions mean that the goals of policies such as Internet+ and the 13th Five-Year Plan, which seek to capitalize on cloud computing to upgrade China's economy, will not be met, as allowing other markets instead to benefit from the efficiencies and security of global IT networks.

Recommendations

- China should reconsider licensing requirements that categorize cloud computing services in the MIIT Telecommunications Services Catalogue, to ensure that foreign and domestic companies can provide these services. Such a change would align with how such services are treated in other international markets.

- As long as cloud computing services are defined as a VAT service under the 2015 MIIT Telecom Services Catalogue, Chinese regulators should issue Internet Content Provider (ICP) licenses and Internet Data Center (IDC) licenses to wholly-foreign owned enterprises (WFOEs) and Sino-Foreign JVs seeking to offer cloud computing services in China.

- China should enhance transparency within the IDC, ISP, and ICP licensing approval process so foreign companies can proactively work with regulators to address concerns about risks and security requirements.

- As products move to more connected solutions that provide information via the internet directly to customers, such as onboard display systems in vehicles, China should provide clear definitions of the types of services that qualify as internet content providers (ICPs).

Challenge 3: Secure and Controllable Technology & Overly Broad Cybersecurity Review Regimes

Companies challenged with protecting client data from criminals use global technology systems to ensure the highest level of security possible for their customers. To that end, policies mandating the adoption or use of unique "secure and controllable" technologies may in fact be counter-productive to security goals. The exact definition of the term has not yet been clarified, but appears to be based on the inaccurate assumption that domestic products are more secure than foreign products.

Companies note that local procurement tenders for IT products still call for the use of "secure and controllable" technology and are implemented in a way that gives preference to local products over foreign technology based solely on nationality, rather than on technical assessment. References to secure and controllable also appear in draft national policies on technology in the financial services sector and in draft regulations stipulating a target use rate of 75 percent domestic technology by 2019. In addition, certain draft regulations promoting "secure and controllable" technology contain requirements for the disclosure of source code, an intellectual property (IP) item that users of technology often do not have access to, or are legally barred from providing to third parties.

Over the past several years, China has quietly implemented cybersecurity review regimes for ICT products without necessary details regarding testing guidelines, product scopes, or required documentation, timelines, or other licensing procedures. As a consequence, it is unclear how these regimes will interact with existing review assessments such as the multi-level protection scheme (MLPS), other non-public review mechanisms, or the cybersecurity review mechanisms outlined in the draft Cybersecurity Law.

In addition, some draft and enacted regulations have called for the use of local encryption algorithms, an approach that is inconsistent with global best practices and raises security concerns. Multinational firms use international encryption standards, tested extensively by international experts for security vulnerabilities, to minimize problems and ensure client data is well-protected— something financial industry regulations in particular require. Adopting different encryption standards for Chinese and global networks, which may be incompatible with each other, could create vulnerabilities in China-specific networks. These risks work against China's overall goal of enhanced IT security.

Ultimately, the use of technology systems unique to China will limit the ability of companies to apply global solutions and best practices within China to the benefit of Chinese consumers. Furthermore, sourcing from local partners may mean the use of equipment that is incompatible or inferior to the security standards companies set for their global operations. Decisions to contract IT globally or locally should be determined by company risk assessment needs rather than government directive.

Recommendations

- The Cyberspace Administration of China (CAC) should ensure that the definition of secure and controllable technology, being developed in its national information security standardization technical committee (TC260), is non-discriminatory, developed in a transparent manner, and will not require or give preference to the procurement or use of Chinese-origin products, technologies, intellectual property, or standards.

- China should streamline its cybersecurity review mechanisms into a single, clear regime that sets narrow parameters for the types of products under the scope of its review, and provide details on licensing requirements, timelines, testing procedures, and other information to facilitate company compliance. This regime should be transparent and formulated in consultation with international industry, to ensure that China will benefit from the experience of existing security review mechanisms already utilized in other markets. Any cybersecurity review regime should also clarify its interaction with existing security mechanisms, such as MLPS. This would ensure more efficient processes, reduce business costs, and reduce international concerns regarding the potential for discrimination in such procedures.

- China should allow companies to use single, global technology platforms and to procure IT solutions and products that best fit their corporate and security needs, based on considerations such as global network integration, risk-based cybersecurity frameworks, and global security standards based on industry consensus practices.

- China should draft technology security standards, including those on secure and controllable technology, in consultation with foreign companies and industry associations to ensure that global best practices are being incorporated to integrate Chinese and global IT security regimes. Draft standards on technology security should not contain mandates for the disclosure of source code, use of local encryption standards, or otherwise impose other burdens that would compromise IP usage and protection.

- China should require that draft standards on technology security reflect its commitments at the 2015 Joint Commission on Commerce and Trade and the 2016 Strategic and Economic Dialogue that technology security should not inherently be linked to product nationality, and should be ascertained via technological assessment of security functions and processes.