



An internet bar in Chengdu on Jan 28, 2011. pcruciatti / Shutterstock.com

China's New Cybersecurity Law¹: Balancing International Expectations with Domestic Realities

February 5, 2017

Jing de Jong-Chen²

Almost all digitally-developed countries agree on the importance of cybersecurity regulations and the need for proper measures that enable protection of citizens and critical infrastructure. China, with over 700 million Internet users, has taken dramatic steps to establish a set of laws, regulations and standards to build a domestic cyber governance system, with government being firmly in control.

From a long term perspective, three core areas will shape the future of the global Internet economy. First, every nation must investment in both technology

innovation and public policies to support advances. This will support an accessible, unfragmented, and secure online ecosystem for continued economic growth. In this way, even with potential disruptions such as those caused by terrorism or economic turbulence, overall progress will continue and the Internet will remain open for business.

Second, protectionism puts globalization at risk. More and more countries such as the United States, Russia and China, consider cyberspace development and cybersecurity national priorities, and will

continue to seek ways to prevent cyberattacks to critical infrastructure as well as public and commercial systems. However, there is a growing trend of using security as an excuse to limit procurement of Information and Communications Technology (ICT) products and services based on country of origin. There is also a push for data residency to restrict cross border personal and commercial data flows, although these policies do not necessarily improve cybersecurity.

Third and perhaps most importantly, in a connected world, users, including consumers worldwide, both young and old, educators, scientists, healthcare providers, entrepreneurs and technologists, depend on the Internet for their personal and commercial information exchange, searching for knowledge and solutions, advancing research and collaboration, and delivering services. The harmonization of Internet policies in support of interconnectedness among nations is needed to ensure ongoing economic and social progress.

China's New Cybersecurity Law

On November 6th, 2016, the Standing Committee of the National People's Congress of the PRC approved China's final Cybersecurity Law, effective on June 1, 2017. This law is an important milestone in China's goal to establish a legal framework for protecting its national security. Together with the Counter-Terrorism Law and The Counter-Espionage Law, the new Cybersecurity Law forms the third pillar of China's National Security Law.

This law has significant implications for both domestic and foreign businesses. In addition, it implies greater government control over Internet content and data flow emanating to and from China and within the country's borders. As a similar (or perhaps a reciprocal) measure to the United States, the final law included an article imposing sanctions against

individuals and organizations based abroad for any cyberattacks against China's critical infrastructure.

The new law covers six core areas: network security; network products and services; critical information infrastructure; data protection; security response and monitoring; and penalties. China reaffirmed its position on cyber sovereignty by instrumenting strong governmental controls over the use of technology and data flows. The law also prioritized protecting critical information infrastructure by including a high-level definition, and left the details to be addressed by a separate policy to be issued at a later date.

Evolved Thinking

Anyone involved in the development of legislation knows that drafting a law is an evolving process. This is evident in the language used, or not used, in the final version of China Cybersecurity Law. Since the first draft was released for public comments in July 2015, China continued to provide a public comment period (30-days), allowing international and domestic entities to provide input during the development process. However, it was unclear how feedback was evaluated and adopted in the final law.

Unlike other domestic security policies, the final Cybersecurity Law provides a legal and policy framework to emphasize the protection of personal information. For example, it highlights the need to protect users' data from hackers, and to crack down on resellers of personal information. The law also requires data residency, gives the government the right to restrict both personal and commercial data collected locally, and requires information to be stored domestically. Finally, the law requires special approval for cross border transfers in key sectors, including public information and commercial services, banking and financial services, transportation services, and other sectors.



Numerous fundamental issues related to the law remain unclear, including: clarity of legal authority for the enforcement of the law; separation of different levels of enforcement between national law and agency-specific policies; alignment between China's cybersecurity review which may limit procurement of foreign products and services in commercial sectors; international legal and trade obligations; potential conflict between a mandatory Real Name Registration for all web services; and legal liabilities for service providers related to the collection and protection of user data.

The definition of critical information infrastructure is an important issue in this law. In the first draft, "critical information infrastructure" (CII) was defined based on the number of users of a service. The second draft removed all language related to the definition and the parties that might be held responsible, leaving both topics to be defined in future policies. The final version of the law brought back definitions on public information and communication services, financial services, transportation, water and energy, public services and e-government systems. It is expected that future policies will define CII and protection

measures. The definition of personal and important data found under data residency rules related to CII operators is also vague given that the CII sector definition is based on the amount of user information collected by the service providers, which in turn is based on current interpretations of local experts.

The international business community appreciates precise legal terms for compliance in countries where investments are made, rather than vague language that creates uncertainty about how laws and regulations will be implemented. This challenge is even greater when China's requirements do not correspond to internationally accepted norms.

Areas of Impact to Foreign Investment

As noted earlier, the Cybersecurity Law became effective on June 1, 2017. But many questions remain about how the law will be enforced. As more and more policies and standards are released, there will be significant impacts on the ICT companies doing business in China. For example:

Residency Requirements –

Unlike China's Counter-Terrorism Law, the final version of the Cybersecurity Law requires "personal and important data" that is collected by critical information infrastructure operators in China to remain in China. Special approval is mandatory for any cross-border data transfers. This provision is designed to guarantee China's legal jurisdiction over CII sectors related data. However, in a highly globalized world, this can be impractical when the exchange of personal and business data across international borders is a necessity for global and regional operations such as telecommunications, transportation, public health, disaster response and recovery, scientific research and education, and commercial and financial services. Cross-border personal and business data flows take place in real time and are massive in quantity when associated with human activities. Even though this requirement reflects China's affirmation of its data sovereignty, it does not necessarily improve cybersecurity nor data protection given that hackers have no regard for national borders in cyberspace. It would effectively impose high costs and constraints on innovation to the detriment of China's global ambition, the wellbeing of its citizens, and global trade.

National Standards-based

Compliance - Domestic (national) standards are being used in the law for product certification and compliance. However, some of these existing standards were designed to be country specific, and in effect, were non-compatible with international security standards which prevented compliance in the global supply chain. If China desires a secure and productive cyberspace, effort must be made to prevent a "non-compatible by design" situation which could hurt both foreign and domestic industry competitiveness. China is a member of leading standards organizations such as the ISO, IEC and ITU. By aligning national standards with globally-adopted and well tested standards, and contributing to the international standard development with a market-driven approach, China will also improve its industrial competitiveness, trade fairly and benefit from stronger security protection.

Cybersecurity Review and Certification Schemes -

The law introduces several new certification schemes including a "cybersecurity review"³ without any definition of certifying authority, scope, or process. By expanding its current scope in certifying security products, China may impose significant costs

on providers of ICT goods and services, especially those based abroad. A government-approved catalog of products, as proposed in the law, would be difficult to maintain. Furthermore, because security risks are constantly evolving, China has begun to promote a “secure and controllable” approach to collecting technical information, which includes not only features and functions, but also data streams from enterprise as part of its assessment. China’s proposed certification also includes a broad definition of “critical equipment,” which can be problematic for foreign-based technologies providers.

Content Censorship and Real Name Registration – The law requires service providers to enforce content self-censoring as well as notice and takedowns. Many service providers in China already

apply censorship management. The law requires service providers to demand Real Name Registration confirmation when users apply for web services. In addition, service providers may be required to collect and store large quantities of personal information. However, no matter how qualified and prepared these services are, there is no bullet proof hacking prevention. This represents a huge risk to the providers based on the legal penalty outlined in the same law for failing to protect personal information.

A Way Forward

China does not have an official system to allow active public involvement in the legislative process, apart from small windows of public comment period at undefined times. Nonetheless, multinational and domestic companies that share common interests should continue to seek clarity to improve the understanding of this new legislation.



Bilateral and multilateral dialogues at a government level should include discussions on issues that affect compliance with cyber norms and trade obligations. This would promote confidence in the global supply chain and assist in protecting cyberspace and the economy.

Cybersecurity has been a top priority during the past US-China presidential meetings. The willingness to cooperate led to the signing of a bilateral agreement at the China-U.S. Strategic and Economic Dialog in Beijing⁴ in June 2016. Both President Xi and President Obama noted that cybersecurity in commercial sectors should:

- be consistent with World Trade Organization agreements;
- be narrowly tailored;
- take into account international norms;
- be nondiscriminatory based on supplier's country of origin, and;
- not impose nationality-based conditions or restrictions on the purchase, sale, or use of ICT products by commercial enterprises unnecessarily.

The two governments also affirmed the principal that access to a full range of global technology solutions strengthens the cybersecurity of commercial enterprises. This is a significant development for the ICT industry, both in China and in the United States, which for years have struggled to gain proper acceptance and to overcome market-access barriers imposed or created by the other country.

With the implementation of China's Cybersecurity Law, governments and enterprises will be watching to see how the bilateral agreement outlined above

will be enforced. As two of the world's most influential nations, China and the United States share responsibility for leading international efforts to establish cybersecurity policies and promote fair competition. Despite improved cooperation and greater collaboration between China and the United States on cybercrime and cybersecurity, the two governments continue to hold very different positions on other cyber governance issues. While under the Trump Administration and a Republic majority Congress, one can expect a US centric market-driven policy, it is less clear how the US will address the trade deficit with China, while expecting cooperation around cyber hacking and cyber warfare.

From industry's perspective, continued challenges can be expected due to a dynamic cyber governance and trade environment in China. Companies will need to invest to be able to legally comply with the new Chinese law, associated regulations, and national security standards. There will be a major risk to the users; if an ICT company cannot find solutions to address non-compliance issues, this may force the company to remove its products and services from the China market.

Government, industry, and civil society all share a responsibility to promote cybersecurity and prevent cybercrime. Governments can partner with ICT companies to address common interests such as managing supply-chain risks in terms of provider qualifications, standard conformance, and legal compliance. Industry can offer input based on experiences and best practices to help government address cyber threats. This will create an environment where it is possible to protect critical infrastructure within and across national borders and support global economic growth.





Endnotes

- 1 The original law legal text in Chinese can be found on the National People's Congress' official [website](#).
- 2 Jing de Jong-Chen is a General Manager, Global Security Strategy, at Microsoft Corporation. She is based in Seattle Washington. The views expressed in the paper solely belong to the author.
- 3 China Administration of Cyberspace issued a draft Cybersecurity Review policy on February 4, 2017 for public comment. The official document can be found [here](#).
- 4 Fact Sheet of the US-China Strategic and Economic Dialogue concluded on June 6th, 2016 in Beijing

<http://www.cctv-america.com/2016/06/07/full-text-2016-china-u-s-strategic-and-economic-dialogue-economic-fact-sheet>

The opinions expressed in this article are those solely of the author.

The Wilson Center

-  wilsoncenter.org
-  facebook.com/WoodrowWilsonCenter
-  [@TheWilsonCenter](https://twitter.com/TheWilsonCenter)
-  202.691.4000

Digital Futures Program

-  wilsoncenter.org/program/digital-futures-project
-  digitalfutures@wilsoncenter.org
-  facebook.com/WilsonCenterDFP
-  [@WilsonCenterDFP](https://twitter.com/WilsonCenterDFP)
-  202.691.4002



Jing de Jong-Chen

General Manager, Global Security Strategy, at Microsoft Corporation
digitalfutures@wilsoncenter.org

Jing de Jong-Chen is Senior Director, Global Security Strategy and Diplomacy Group in the Corporate, External and Legal Affairs Division at Microsoft Corp. She has 20 years of industry experience and domain expertise in cybersecurity policy, technology and strategic partnership development.

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027