NEW AMERICA

China's Cybersecurity Law One Year On

An Evolving and Interlocking Framework

By:
Paul Triolo, Eurasia Group and New America
Samm Sacks, Center for Strategic and International Studies
Graham Webster, Yale Law School and New America
Rogier Creemers, University of Leiden and New America

In the year since China's Cybersecurity Law was released in its full form and the six months since it went into effect June 1, the Chinese government and the Communist Party have significantly clarified their approach to cyberspace and information and communications technology (ICT). Developments range from well-reported media control moves to early enforcement actions on data protection and still-evolving frameworks affecting foreign companies doing business in China. This interlocking matrix of regulations and standards associated with the new law is already shaping China's political and economic digital reality.

In fact, the Cybersecurity Law has been only the most visible document in a wider Chinese effort to govern cyberspace and secure the country's digital infrastructure. The 19th Party Congress, where Xi Jinping's leading position was renewed and solidified, put ICTs front and center in economic development and emphasized the importance of cybersecurity as threats and risks proliferate. Chinese policy thinkers and officials are eyeing the global stage and may announce new

international proposals as soon as at the Chinese-hosted World Internet Conference (WIC) in Wuzhen, Zhejiang, opening next week.

National plans—which can be at once aspirational and quite concrete—set ambitious goals for artificial intelligence and high-tech development, and surging public and private investment in a large and protected market raise expectations of success. Taken together, these efforts arguably constitute the most comprehensive framework for ICT governance currently underway globally.

Even if it's easy to see the forest of Chinese official efforts to shape the digital world, it can be hard to navigate the trees of implementing regulations, standards, and review regimes. Here, after a year working with the Cybersecurity Law's text and half a year nominally under its effect, we offer a guide to the emerging regime and identify some areas to watch for the most consequential developments yet to come.

The Players

Developing such a comprehensive framework naturally gave rise to much bureaucratic tumult, given the number of China's government ministries, commissions, and standards bodies involved, and the heavy input—positive and negative—the process has seen from domestic and foreign ICT players. The uncertainty and delays in the framework's legislative process reflects the complexity involved with balancing these different forces within the Chinese political system. The laws deliberately contain broad, high-level principles to accommodate competing regulatory actors.

In this jousting for influence, the primary government players are:

- *Cyberspace Administration of China (CAC)* — A relatively new agency seeking to assert its authority over cybersecurity and informatization (i.e. digital economy and the ICT industry), CAC draws its authority from its status as the office of a Xi-led Leading Small Group. CAC is the lead convener of the WIC, now in its fourth year, and its centrality appears intact even as its former leader Lu Wei faces investigation by Party authorities.
- *Ministry of Public Security (MPS)* — Responsible for running the so-called "Great Firewall of China" system that blocks Chinese access to portions of the global Internet, MPS had primary responsibility for critical infrastructure protection until the new law. Now CAC also has part of that portfolio, but the division of roles, especially over new security reviews, is not yet clear.
- *Ministry of Industry and Information Technology (MIIT)* — A major developer and manager of digital strategies and plans, MIIT has significant mandates to regulate ICT sector industrial policy. The China Academy of Information and Communications Technology (CAICT), a think tank subordinate to MIIT, also plays a role in ICT policies and standards development. CAICT has been an important interlocutor for foreign ICT firms on these issues.

- *National Information Security Standardization Technical Committee [Technical Committee 260, or TC260]* — Though sometimes caught between the three big players above, TC260 has been in hyperdrive since August 2016, cranking out detailed new standards that make elements of the new framework more concrete. TC260 includes participation by experts from outside officialdom, including domestic and foreign companies.
- *Military and intelligence establishment* — Though the evolving framework is largely civilian in nature, decisions related to what qualifies as national security will remain intertwined at top levels of the Chinese government with the military and intelligence establishment, and experts from that world play a role in developing security review systems and advocating for Chinese priorities internationally.

Outside the government, the main players include:

- *Chinese industry associations and alliances* — Industry groups, for example the CyberSecurity Association of China (CSAC) and China Artificial Intelligence Industry Development Alliance, are made up of dozens of Chinese ICT company members and act as intermediaries between government and the private sector. They serve as transmission belts in both directions for policy ideas, trust, and support.
- *Baidu, Alibaba, Tencent ("the BATs," or now sometimes "BATJ" to include JD.com)* — As China's largest and most influential ICT companies, the BATs are on the front lines of Beijing's global tech ambitions and also have a voice shaping ICT policies. Their affiliated research institutes in Beijing have gained more influence in recent years on public policy debates for emerging technologies. The BATs also wield tremendous power shaping next-generation technology by investing in and acquiring smaller, emerging companies.

The Framework

As the Cybersecurity Law framework develops, what has emerged is a system with several top-level guiding documents and six major systems of increasingly concrete policy, each with its own bureaucratic champions, enforcement mechanisms, and implications for China's digital life. Top-level strategies or passages of the Cybersecurity Law provide a blueprint for the Xi administration's cyberspace governance priorities, while supporting regulatory documents flesh out details for implementation and hash out conflicts in the bureaucracy. Still, the documents and regulatory moves do not align in a tidy hierarchy, but must be understood as an interconnected matrix.

Broad Statements of Principle and Ambition

While the Cybersecurity Law is highly central for ICT governance, other laws, especially the new National Security Law and Counterterrorism Law, also feed into the cyberspace governance framework. Reinforcing the logic of the Xi-era dictum that "without cybersecurity there is no

national security, and without informatization there is no modernization," these security-focused laws further mesh with development-focused national strategies that provide a touchstone as officials develop regulations and standards. They include:

- National Cyberspace Strategy (2016);
- International Strategy for Cooperation in Cyberspace (2017);
- 13th Five-Year Plan for Informatization (2016);
- 13th Five-Year Plan for Major Science and Technology Projects (2016);
- National People's Congress Standing Committee Regulations on Strengthening Network and Information Protection; and
- Technology-specific plans, e.g. for big data, semiconductors, cloud services, and with great fanfare, artificial intelligence. (See DigiChina's translation and analysis of the AI plan.)

Six Systems

In effect, as of late 2017, the laws, strategies, regulatory documents, and governing actions can be viewed as operating in six systems, which together constitute an evolving framework for governing ICT use in China. They are: the Internet Information Content Management System; the Cybersecurity Multi-Level Protection System; the Critical Information Infrastructure Security Protection System; the Personal Information and Important Data Protection System; the Network Products and Services Management System; and the Cybersecurity Incident Management System. Below are broad-strokes summaries of the status and interconnected nature of these systems.

I. The Internet Information Content Management System

The Party leadership is expanding the legal tools at its disposal to monitor and control information disseminated online. Technological developments are allowing individuals more channels to communicate outside of officially sanctioned media outlets, compelling the government to play "catch up" with new Internet media platforms.

Party monitoring and control of online information content is certainly not new in China. But a spate of new regulations enhance the government's ability in this regard.

First, this batch of regulations provides new requirements related to real-name registration for Internet users. Although the government has tried to introduce real-name requirements for years, with a mixed record of enforcement, the latest requirements may have more teeth behind them, since they are now backed by a high-level framework for bolstering security controls. Moreover, the real-name registration system is now closely connected to other account-based services in which the Internet is not merely a publishing medium, but a platform for all aspects of living (payments, travel, entertainment, work, etc.). The regulations also lay the foundation for the government to

aggregate online data on individuals to feed into a "social credit" system, although the government has a long way to go in setting up mechanisms to coordinate and process data.

Second, the regulations place an emphasis on "self-regulation" by operators and service providers. The government has outsourced regulatory responsibility to businesses for a long time, but now there is a shift in focus from regulating production to regulating access. Now those found in violation face restrictions in access to Internet content and services. Assigning responsibility to online intermediaries helps the government leverage more resources while gaining buy-in from companies to the cybersecurity framework.

II. The Cybersecurity Multi-Level Protection System (MLPS)

Originally launched in 2006, the Multi-Level Protection System (MLPS, also translated as the "Multi-Level Protection Scheme") is an element of the MPS critical infrastructure protection system that ranks networks by sensitivity on a scale of one to five, with stricter security requirements for networks ranked at higher levels, Level 1 being the highest. Even as the Cybersecurity Law and related documents established new elements of a regime for "critical information infrastructure" (CII) and new procedures for reviewing network products and services (both of which are discussed below, under *III* and *V*), the MLPS was reinforced in the law.

MLPS developer and proponent Guo Qiquan has emphasized that, according to the Cybersecurity Law: "MLPS shall be used as a basic regime and national policy for cybersecurity in the new era. New laws, policies, standards, technical support, talent, education and training, and guarantee systems will be built." Guo holds that the MLPS is a broader regime than the two new systems and that MLPS and CII protection are on two inseparable sides of the cybersecurity equation.

The exact breakdown in scope between the MLPS and the new Cybersecurity Review Regime (CRR, see *V* below) remains unresolved and is a major issue that must be clarified between CAC and MPS. This issue likely accounts for the current delay in implementation of the CRR. One major difference appears to be that the CRR includes examining the background and supply chains of network and product service providers, focusing on risk management, whereas MLPS is more about compliance.

III. The Critical Information Infrastructure Security Protection System

Soon after the final text of the Cybersecurity Law was made public, analysts in China and abroad identified "critical information infrastructure" (CII) as one of the law's most consequential concepts. It both reinforced and stood apart from previous efforts to protect "critical infrastructure," and if an entity was to be classified as a CII operator, it would be subject to some of the law's most novel and potentially burdensome requirements. The question of what is and isn't CII, then, became crucial.

The law itself identifies sectors like "public communication and information services, power, traffic, water resources, finance, public service, and e-government," and draft regulations in July

[translated and analyzed by DigiChina] added news media, healthcare, and, significantly, cloud computing and big data providers. Nonetheless, the specific boundaries of CII remain indistinct.

Also in question is who has responsibility for regulating various areas of CII. Sectoral regulators are clearly assigned responsibility to ensure security of CII in their areas of authority, but some may lack existing competencies in cybersecurity administration. The MLPS, discussed above in *III,* may apply in an overlapping way.

Standards developed by TC260 and updated regulations can be expected to provide some further clarity, but regulators appear to maintain significant freedom to interpret the reach of CII—likely in a very broad way. That means a wide variety of organizations will at least consider the Cybersecurity Review Regime in procurement, and domestic storage of data may emerge as a default procedure. This will likely create challenges for foreign suppliers and Chinese firms operating across borders, both of whom maintain some voice in how the details take shape over time.

IV. The Personal Information and Important Data Protection System

As Chinese regulators cope with a lively proliferation of online platforms and services, developing protections for the great volume of data produced by and collected on users or businesses is a major challenge. The Cybersecurity Law calls for several forms of regulation, including: requirements to store certain information inside China and at certain levels of security; procedures before transferring certain information out of China; and consent requirements when collecting personal data.

Each of these requirements hinges on definitions of the data covered, i.e. whether it is either "personal information" or "important data." [See DigiChina's analysis of the evolving Chinese controversy over how to implement cross-border data flow regulations, and of the overlap between "personal information and important data" and CII.]

At the center of this system is the definition of personal information, which will be used to determine whether an organization must conduct a security review of the data it holds. The scope of the definition of personal data was clarified somewhat in the second draft of the Personal Information Security Specification [draft], released in early September 2017. There has been significant change in the content of this document since a first draft was released earlier this year. The most important changes include greater clarity in the requirements for how data collectors handle user consent requirements.

CAC, MIIT, MPS, and TC260 have already teamed up for an early effort to shape how Internet companies inform users of their privacy practices by examining the practices of 10 prominent services—including Alibaba's Taobao, Tencent's Wechat, and the ride-hailing giant Didi Chuxing—and convening their representatives to promote best practices. Authorities consider this a type of enforcement, even short of finalized standards and detailed definitions.

V. Network Products and Services Management System

The Network Products and Services Management System, because it interlocks with the CII and MLPS systems, highlights the way in which the framework is best understood as a matrix. On May 2, CAC released the Security Review Measures for Network Product and Service Security Inspection (Interim). The measures, which establish the Cybersecurity Review Regime (CRR) discussed under *II* and *III* above, require network products and services used in critical information infrastructure (CII) to undergo a cybersecurity review administered by CAC. The final definition of CII is still pending, and the full criteria for assessments and list of those conducting them are unknown. Without these pieces of the puzzle, the practical implications of this system remain murky.

The government has started 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 by TC260 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, in addition to some specifics, 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.

With the creation of the CRR, the list of security reviews for the ICT sector is growing. In addition to the MLPS, ICT companies also must undergo security reviews associated with different parts of the cybersecurity framework, including cross-border data transfer assessment and separate CII security evaluations. The government has yet to work out coordination among the different review bodies and agencies, increasing risks of regulatory gridlock and turf battles.

VI. The Cybersecurity Incident Management System

An evolving system for coordinating China's public and private sector response to cybersecurity incidents is built on a number of measures and draft standards related to incidents, definitions, and cyber threat information sharing. It includes standards from TC260 addressing cybersecurity incident response exercises and developing a cybersecurity vulnerability discovery and reporting management system. MIIT has a major role in this effort, as it oversees the current incident response system run by the National Computer Network Emergency Response Technical Team (CNCERT).

MIIT in August issued the Public Internet Cybersecurity Threat Monitoring and Mitigation Measures, which call for: the development of a cybersecurity threat information sharing platform; unified collection, storage, analysis, and notification; the release of network security threat information;

the formulation of relevant interface specifications; and the development of interoperability with related cybersecurity monitoring platforms. CNCERT is responsible for platform construction and operational and maintenance work.

The August document references the Cybersecurity Law, which among other things places heavy requirements on "network operators," which it says "shall formulate emergency response plans for cybersecurity incidents, promptly addressing system vulnerabilities, computer viruses, cyber attacks, network incursions, and other such cybersecurity risks."

As in several areas of the evolving framework, it remains unclear whether foreign companies will eventually be designated as network operators with the associated responsibilities. Foreign companies providing telecommunications or cloud services in China, in any case, will almost certainly be required to step up participation in the evolving incident management system and provide incident reports to MIIT/CNCERT and CAC.

The Continuing Search for Clarity

Over the next six months and beyond, Chinese regulators will work to refine the key implementing regulations that remain in interim form. They will continue to release new drafts of standards associated with these six systems, some for public comment and others initially shared only with industry groups and domestic and foreign companies that are participants in TC260 working groups. This suggests that CAC, MPS, and MIIT are attempting to engage in a real dialogue with industry, though it remains short of the type of intense and extended level of collaboration between regulators and stakeholders that is typical of U.S. and EU regulatory development. Chinese regulators will continue to seek a better interoperability with global best practices in key areas such as cross-border data flows, and are likely to carefully study how companies are preparing to comply with the Europe's General Data Protection Regulation (GDPR) and how regulators react to major emerging issues such as the Uber data breach.

Regulators will also face a lack of capacity and shortage of personnel to support the implementation of this framework. For example, it remains unclear which organizations will be designated to conduct security reviews of the many sectors, products and services, and personal and important data sets. CAC's Cybersecurity Review Office is staffed by personnel seconded from other agencies. The office has already done a series of informal reviews of a small number of foreign products, but it is not clear whether it could facilitate reviews of large numbers of products across multiple and large sectors designated as CII. No sectoral regulators have put in place adequate implementing regulations or a transparent system for conducting reviews.

Big questions remain around China's participation in global cyberspace governance. The Chinese government's robust development of a domestic regulatory regime that affects both those operating online in China and Chinese companies operating globally has already made Chinese cyberspace policy relevant worldwide. Chinese ideas and proposal in international discussions are

also relevant in addressing concerns the status quo does not—even if from a different ideological starting point. Many governments have long been content to dismiss Chinese ideas such as cyber sovereignty as the work of an "enemy of the global Internet" seeking to undermine a functional and virtuous model. In the coming months, governments and civil society are likely to discover about Internet governance what companies have already learned about the digital economy: Chinese initiatives are evolving, have appeal to some actors, create problems for others, and absolutely cannot be ignored.