# China's second draft of the Cyber Security Law continues to propose more stringent regulation of cyberspace, further escalating concerns

July 2016

Hogan Lovells

# China's second draft of the Cyber Security Law continues to propose more stringent regulation of cyberspace, further escalating concerns

## Introduction

On 6 July 2016, a second draft of the *People's Republic of China Cyber Security Law* ("**Draft 2**") was released to the public for comment following its second reading by the Standing Committee of the National People's Congress. The deadline for submitting comments on Draft 2 is 4 August 2016.

The first draft of the law ("**Draft 1**") was issued a year ago to the day on 6 July 2015, and followed on the heels of China's National Security Law, the first comprehensive law of its type, which touched on cyber security matters by imposing, among other things, a national security review system and provision for management of internet information technology products and services that have or might have an impact on national security (more on that **here**).

Since then, a number of separate legislative and regulatory developments brought forward have demonstrated an increasing resolve by the Chinese authorities to assert control over cyber space, not only with respect to the security of networks, systems and data, but also with a focus on monitoring and censoring content, for example:

— **Counter-terrorism**, with a number of specific provisions for telecoms and internet service providers, in the *People's Republic of China Counter-Terrorism Law*, issued by the National People's Congress (more on that **here**);

— **Online publishing**, in the *Online Publication Services Administrative Provisions*, jointly issued by the *State Administration of Press, Publication, Radio, Film and Television* ("**SAPPRFT**") and the Ministry of Industry and Information Technology (more on that **here**);

— **Online games played on mobile devices**, in the *Notice on the Administration of Mobile Games Publishing Services*, also issued by SAPPRFT; and

— **App developers and app store operators**, in the *Mobile Internet Application Program Information Services Administrative Provisions*, issued by the Cyberspace Administration of China ("**CAC**").

It is also important to note that there has been a pronounced sector focus on cyber security issues by China's financial services regulators, with the publication by the China Banking Regulatory Commission in December 2014 of draft regulations prescribing minimum quotas for financial institutions' use of technologies certified by the authorities to be "secure and controllable" and the publication by the China Insurance Regulatory Commission of similar draft regulations in October 2015 (more on that **here**). While neither of these regulations have been implemented to date, they are illustrative of an overall trend towards a much tighter, more prescriptive and potentially invasive approach to technology regulation in China.

Given the growing cyber threat globally, the Chinese move towards more rigorous cyber security regulation is in line with international trends. However, the specific approach to regulation being taken in China is a clear outlier, primarily for the broad and often imprecise terminology used in the draft law and also for the invasive and potentially discriminatory nature of the regulation. The immediate reaction to Draft 1 has therefore been confusion as to who the law would apply to and what requirements the law will bring to those within its reach. More broadly, the Cyber Security Law has raised fundamental concerns about regulatory intention, and in particular whether or not the law is meant to close certain areas of business to foreign participation.

Draft 2 of the Cyber Security Law has done nothing to quell concerns raised by Draft 1. In our commentary on Draft 1, we categorised three principal areas of interest in the cyber security regulation as:

— **Technology regulation**: In this respect, the Cyber Security Law seeks to regulate what technology can or cannot be used and/or imposes requirements for pre-market certification of certain types of technology, specifically by creating a catalogue of "critical network equipment" and "specialized cyber security products" (Article 22);

— **Co-operation with authorities**: Here, the Cyber Security Law would impose duties on "network operators" to provide technical support and assistance in national security and criminal investigations (Article 27); and

— **Data localisation**: Finally, Draft 1 introduced requirements on "critical information infrastructure operators" to store data gathered and produced in China on Chinese soil (Article 35).

Our briefing here focusses on how Draft 2 has carried forward these key aspects of Draft 1.

## Technology Regulation

As in Draft 1, Draft 2 requires that "critical network equipment" and "specialized cyber security products" be inspected or certified by a qualified institution before they can be sold in China (see Article 22 in Draft 2). Both drafts envisage that an official catalogue will be issued identifying which equipment and products will specifically be subject to this rule.

The idea of restricting the use of technology in China to a closed list of pre-approved products is an important area of focus for most multi-nationals dealing in China, not just in terms of technology companies that could be facing approval requirements, but also in terms of multinationals reliant on foreign technologies that may or may not in future be available if a necessary certification is not forthcoming. Inspections and certifications may delay a product's entry to the market, and, as was the case with Draft 1, Draft 2 leaves open precisely how invasive any proposed inspections of technology would be.

Where Draft 2 differs from Draft 1 is in the introduction in Article 15 of a responsibility on the State Council and People's Governments at the provincial level to promote the use of "secure and reliable" network products and services. Draft 2 does not offer a definition of "secure and reliable" technology, nor does it elaborate on what the promotion of this classification of technology will mean in practice.

While Article 15 may just be a general call for technology to meet "secure and reliable" standards in the ordinary sense of the word (which may well be hard to argue against), the provision comes against the backdrop of the introduction of similar terminology ("secure and controllable") to technology guidelines put forward in the banking and financial services sector. Those guidelines proposed a "secure and controllable" quota system, which engendered strong pushback, primarily driven by concerns that "secure and controllable" might in effect mean that only domestic Chinese products hand-picked by the authorities would be available for use in those industry sectors. If this view is correct, there would be a regulatory basis to discriminate against foreign technology businesses who have developed their products offshore and so may be viewed by Chinese authorities and businesses to be inherently incapable of being "secure and controllable". Article 15 of Draft 2, by introducing a concept of "secure and reliable" into the Cyber Security Law, requires elaboration in order to avoid adding further to these concerns.

We can also see privileged status for domestic Chinese technology in other regulations. For example, under the *Administrative Measures for Hierarchical Protection of Information Security*, information systems in China classified (on the basis of potential national security implications) as being tier-3 or higher must procure their information security products from manufacturers invested by Chinese citizens or legal persons and the core

technologies or key parts and components of such products must have be proprietary domestically developed intellectual property rights.

If there is any bright spot in the formulation of technology regulation under Draft 2, it is in a clarification that government-issued standards are mandatory (such as for certification processes) whereas industry standards are not.

## Co-operation with Authorities

Article 27 of Draft 2 continues with Draft 1's obligation on "network operators" to provide technical support and assistance to public security organs and national security organs for their activities of lawfully protecting national security and investigating crimes.

The scope of the term "network operator" is considered by many observers to be unclear. In Draft 1, a network operator was defined to be "an owner or manager of any cyber network, and a network service provider who provides relevant services using networks owned or managed by others, including a basic telecommunications operators, network information service provider, important information system operator and so forth." Draft 2, by contrast, pares this back to "owner or manager of any cyber network, and a network service provider."

While there is a difference of wording, we still read both texts to define the term on fairly broad terms and so expect that Draft 2 would likely be interpreted in practice, as Draft 1 would have been, to include any businesses operating over networks and the Internet, from basic carriers to companies operating websites, with the consequence that all such businesses will be under Article 27's obligation to provide technical support and assistance (in Draft 1 this was limited to *necessary* support and assistance, but Draft 2 has deleted the word necessary).

The breadth of duties to cooperate with authorities in investigations, in particular with the expansive wording in Draft 2, is a concern, in particular given the relatively small role for judicial oversight in the procedures for conducting investigations in China. There have been a number of well-publicised instances in which investigations by Chinese authorities have raised brand or public relations challenges for technology companies.

Draft 2 also introduces some new requirements that appear to be directed at making network operators duty to co-operate more effective from the authorities' point of view, including:

— Article 20's requirement that network operators keep network log records for 6 months; and

— Article 21's requirement that network operators notify the authorities of security defects discovered in their systems.

## Data Localisation

"Data localisation" is a term used to describe a legal or regulatory requirement to keep data in the jurisdiction where it has been collected or generated. Article 31 of Draft 1 introduced data localisation in the form of an obligation on "critical information infrastructure operators" to store personal information collected or generated in their networks onshore in mainland China. Draft 1 defined "critical information infrastructure operators" very broadly to mean the operators of:

— basic information networks of providing public communication, radio and television transmission services;

— important information systems in energy, transportation, water conservancy, finance and other key industries;

— power, water and gas suppliers;

— medical care, social security and other public service sectors;

— military networks;

— government affairs networks of state organs above the city level; and

— networks and systems owned or managed by network services providers with a large number of users.

Notably, Draft 1 did not provide any clarity as to which businesses (or which operational streams and functions) in the sectors mentioned above, or which of their specific networks, would be considered to be "critical information infrastructure".

The final bullet point raised particular concern on the basis that looking simply at the number of users of a system as the measure for identifying critical information infrastructure could potentially implicate a wide range of commercial businesses that have a large number of users but have little practical bearing on national security, such as e-commerce businesses or online game platforms.

Draft 2 introduces an important structural change to the definition. The itemized list has been removed and instead there is a provision appointing the State Council to make a separate enactment setting out the specific scope and definition of "critical information infrastructure operators". Whether this leads to a broadening or a narrowing of remains to be seen, adding yet another layer of uncertainty to the developing law.

A second key change to Article 35 is Draft 2's extension of the data localisation requirement from personal data to also include "important business data". Neither category of information may be sent outside China unless it is "truly necessary" for business and the operator has conducted a security assessment in support of the offshore transfer. These security assessments will need to be carried out in accordance with measures to be jointly formulated by the state-level cyberspace administration authorities and the relevant departments of State Council. No detail is provided in Draft 2 as to how broad the exemption for "truly necessary" international transfers would be or what the criteria for clearing the associated security assessment would be.

A third key change is the removal of "storage" of such information outside China. Draft 1 contemplated both the storage and sending of such information outside of China where necessary. The removal of this term in Draft 2 suggests that China no longer contemplates the possibility of data storage outside its borders, even if necessary.

Data localisation laws are not new to China. There are some confined localisation requirements in specific industry sectors such as e-banking, insurance, credit reporting, and network-based payment services. By contrast, the Draft Cyber-Security Law would apply to all "critical information infrastructure operators", a potentially much larger segment of industries, depending on how the State Council proceeds to give life to this term.

It is hard to tell at this stage what approach the State Council would take to filling in this critical missing definition. It may be that the CAC will be "holding the pen" for the State Council given that the *Notice of the State Council's 2016 Legislative Work Plan* indicates that the CAC has been commissioned to draft a Safety Protection Regulation for critical information infrastructure operators, a regulation which will no doubt need to include a clear definition.

If this assumption is correct and the CAC will be providing the necessary missing details, there may be some publicly available documentation that sheds light on the likely direction. A CAC press release dated 8 July 2016 announced that it will soon kick off network security inspection work on critical information infrastructure (see **here**)(Chinese only). This announcement states that "critical information infrastructure" means "information systems or industrial control systems that provide network information services to the public or support the operations of energy, telecommunications, finance, transportation, public utilities and other important industries."

The inclusion of "information systems ... that provide network information services to the public" is the potentially the broadest part of the definition. The term is not defined in the press release, but if it is anything similar to the way the term of art "internet information services" is used in the *Administrative Measures on Internet Information Services* issued by the State Council, it could be so expansive as to include all businesses operating over the Internet and all websites. If so, this would make critical information infrastructure operators virtually indistinguishable from "network operators" as used in Draft 2 of the Cyber Security Law, and this could greatly extend the reach of the data localisation requirement beyond the requirement set out in Draft 1.

There are a number of information security obligations tied to the data localisation requirements carried forward in Draft 2. Draft 2 carries forward duties on critical information infrastructure operators that are in addition to those imposed on network operators (Article 32), including a duty to enter into security confidentiality agreements with network product and services providers (Article 34) and a duty to accept government security inspections in relation to network products and services that might have a bearing on national security issues (Article 33). Interestingly, some of the security protection duties in Article 32 appear on their face to overlap with the requirements of network operators found in Article 20, but as they are stated to be additional to the requirements of Article 20, it is reasonable to expect the seemingly overlapping parts will represent an increase in the regulatory burden here.

## Conclusions

Draft 2 of the Cyber Security Law stands as the latest in a series of regulatory developments that demonstrate a China increasingly focused on national security, stability, control of cyberspace and imposing restrictions on those who may operate and publish in it, and the particular challenges that a digitally connected world pose for China's unique political, culture and economic context. Against a backdrop of geopolitical tensions over cyber security and Chinese concerns about the position that western technology companies hold in the domestic industry, there can be no doubt that there is a much bigger picture to this draft law. The more typical concerns of cyber security regulation involve moves to shore up operational risk standards and facilitate the sharing of information about cyber incidents. China's approach to cyber security regulation includes some challenges to conventional wisdom on these fronts.

It is clear that Draft 2 is very much an evolution of Draft 1 rather than a re-write. The amendments introduced to this new draft will, if anything, stoke further concerns amongst multi-national businesses operating in China that lawmakers are taking cyber security as a basis to limit foreign access to China's vast, expanding markets for technology and technology services. The scope for technology regulation has both been made wider and less clear. Authorities' access to systems and data has been broadened. The scope of data localisation requirements is very likely to have increased.

Clouding the picture further is the fact that Draft 2 introduces more delegation of critical points of definition to implementing rules and regulations. There may, of course, be some mitigation of the impact of the Cyber Security Law in this. However, at the moment the key consequence of these changes is uncertainty.

Fortunately, Draft 2 has also been opened for public comments, which means there still may be room for engagement and negotiation on some of the more challenging aspects of the draft law. We do not necessarily expect to see any further clarification per se on the uncertain elements of the draft law prior to its final enactment, as it is likely there is also uncertainty within the various government departments who may be charged with

implementation as to exactly how they intend to or will actually apply the law in practice. However, during the comment period, we do hold some optimism that the law-makers will be responsive to concrete suggestions for improvement.

**Alicante**
**Amsterdam**
**Baltimore**
**Beijing**
**Brussels**
Budapest
**Caracas**
**Colorado Springs**
**Denver**
**Dubai**
**Dusseldorf**
**Frankfurt**
**Hamburg**
**Hanoi**
**Ho Chi Minh City**
**Hong Kong**
**Houston**
Jakarta
Jeddah
**Johannesburg**
**London**
**Los Angeles**
**Louisville**
**Luxembourg**
**Madrid**
**Mexico City**
**Miami**
**Milan**
**Minneapolis**
**Monterrey**
**Moscow**
**Munich**
**New York**
**Northern Virginia**
**Paris**
**Perth**
**Philadelphia**
**Rio de Janeiro**
Riyadh
**Rome**
**San Francisco**
**São Paulo**
**Shanghai**
**Silicon Valley**
**Singapore**
**Sydney**
**Tokyo**
**Ulaanbaatar**
**Warsaw**
**Washington, D.C.**
Zagreb

**Our offices**
Associated offices

# www.hoganlovells.com