China’s developing legal landscape for cyber security

The Chinese government has issued new cyber security laws and regulations with the potential to significantly impact international businesses operating in China. Dr. Michael Tan and Lynn Zhao of Taylor Wessing assess the development of cyber security law in China and the implications of the recent legislative developments.

In China cyber security has more of a political facet and is more sensitive due to the fact that China is still a socialist country having - or supposedly having - various conflicts with Western countries, not only 'soft ones' like ideological conflicts, but also conflicts that closely relate to the country’s national defence concerns. The very first set of rules addressing cyber security issues were the Regulations for Safety Protection of Computer Information Systems promulgated by the State Council on 18 February 1994, which prohibit activities misusing computer information systems to endanger the interests of the State and society. This prohibition was further expanded by the Administrative Measures for Protection of the Security of International Internetworking of Computer Information Networks ('Measures') issued by the Ministry of Public Security ('MPS') on 16 December 1997, which barred activities that endanger national security or reveal state secrets. On 28 December 2000, the Standing Committee of the National People's Congress ('NPC') further endorsed this position by subjecting offences under the above rules to criminal liability.

In recent years, a new concept of 'secure and controllable information technology' ('SCIT') has been introduced, with the strategic importance that comes with a wave of new policies and laws. On 12 November 2013, the Chinese Communist Party rolled out its Decision on Some Major Issues Concerning Comprehensively Deepening the Reform. This serves as the ruling party's policy framework on cyber security issues and, for the first time, explicitly states that an internet administrative and guidance mechanism should be developed to ensure the State's network and information security. This includes the establishment of a State Security Commission to handle national security strategies. Shortly after this, the Office of the Central Leading Group for Cyberspace Affairs was established on 27 February 2014. This is led by another high-ranking working group, with the Chinese President and Premier as group leaders.

The so-called De-IOE campaign was launched to implement the concept of SCIT and aimed to get rid of IT systems supplied by IBM, Oracle and EMC and replace them with equipment and technology developed by Chinese companies. On 28 August 2014, the Ministry of Industry and Information Technology of the PRC ('MIIT') issued its Guiding Opinions on Strengthening Network Security in the Telecommunications and Internet Sectors which, among other things, promote the use of hardware and software whose security can be monitored and controlled, and tightens control over cyber security associated with new technologies and businesses like cloud computing. In September 2014, the China Banking Regulatory Commission issued guidance - with practical binding effect - to all banks under its supervision, pushing for SCIT. The nature of the guidelines only became known after the Notice on Issuance of the Promotion Guidelines for Banking Application of Safe and Controllable Information Technology (2014-2015) (Circular 317) was implemented. Circular 317 is not officially published by the legislators, but according to the version circulated in public it includes requirements such as the submission of source codes to authorities, locally-owned IP, and local R&D and customer service centres.

The top legislators are also taking action. On 3 November 2014, the NPC presented its second draft of the envisaged Counter-Terrorism Law for public comment. Under this draft, all telecommunication operators and ISPs must set up technical interfaces and submit encryption solutions to enable audits by government agencies. In addition, their equipment and data concerning domestic users must be kept within China. What these requirements mean is not entirely clear. In theory, they could mean that no Chinese personal data can flow out of China. On 1 July 2015, the NPC released the National Security Law with immediate effect. For the first time the concept of 'maintaining cyberspace sovereignty' is explicitly addressed under a high-ranking law. Articles 24 and 25 of this law set forth the general principles with regard to cyber security issues. They stipulate that a national network and information security safeguard system shall be established to raise the capacity to protect network and information security. On 6 July 2015, the NPC further published the draft Cyber Security Law, which by solely focusing on cyber security issues added more guidelines and details to the safeguarding system. At the same time, this created new requirements and obligations to be fulfilled by businesses in China. A major feature to be noted with
regard to these new laws and regulations is the general coverage and vagueness of the various principles they outline, which very much depend on further interpretations from the authorities and could potentially have a far-reaching impact on the international business community.

Key obstacles and obligations
Investment access
The whole telecommunication and internet sectors are deemed to be closely related to cyber security concerns and are not yet fully opened up to the outside. Foreign stake in business conducting value added telecommunication services is restricted to 50%. This covers - among others - almost all types of internet-based business models.

Routine security requirements
These can be found under various laws and regulations that take the form of some general principles. Industrial standards are in general in the process of development. According to Article 4 of the Measures, nobody shall make use of computer information systems to endanger State security, divulge State secrets, or infringe upon the interests of the State, collective groups and other citizens. In particular the following actions are prohibited:
- accessing computer-based information networks or utilising such resources without permission;
- deleting, modifying or adding to computer-based information network functions without permission;
- deleting, modifying or adding to the data and applications in memory, processing or transmission in computer-based information networks without permission;
- deliberately producing and spreading computer viruses and other destructive programmes; and
- other activities that endanger the security of computer-based information networks.

For internet content providers
Chinese law provides a concept for an ‘internet content provider,’ which in general may mean any company that generates and disseminates content via the internet. This may cover all kinds of websites, who are under the supervision, inspection and guidance of the police authorities, and are obliged to provide cyber security-related data and to cooperate with police authorities when the latter conducts investigations. Providers are subject to the following responsibilities:
- establishing and improving rules for security protection administration;
- implementing technical measures for cyber security protection;
- security education and training of the users;
- registering the organisations and individuals that entrust them to publish information and carrying out censorship of the contents as listed above;
- establishing a user registration and information control system for the bulletin board systems;
- preserving the relevant original records upon discovery of any circumstances violating the prohibitive provisions relating to national security and content censorship as listed above and reporting to the local public security organ within 24 hours;
- deleting the addresses and directories in the networks violating the censorship provisions or shutting down the server.

General outlook
One may conclude that the Chinese cyber security regulations are very much associated with the national security strategy of the country. However, in the view of many foreign investors, the recent legislation goes far beyond essential security concerns related to the internet, and risks shutting China out from many of the fundamental technologies and other benefits afforded to it by the international marketplace.

Such concerns are not unusual in the Chinese legislative environment. The Chinese government is displaying a strong desire to further liberalise the market by pushing forward with the streamlining of administrative procedures applicable to foreign investment activities. On the other hand, the outside world perceives an increase in government oversight of the market. This may be a natural phenomenon, with China trying to learn how to use and adapt Western models to handle its own security concerns. But in certain aspects it appears to go quite far, particularly in comparison to its Western peers. Since this is now a strategic priority on China’s political agenda, there is no question that this will become another ‘new normal’ of the Chinese business environment that international companies will need to adapt to.

Dr. Michael Tan Senior Counsel
Lynn Zhao Associate
Taylor Wessing, China
m.tan@taylorwessing.com

2. Article 4 of the Measures.
3. Article 2 of the Measures.
6. Article 4 of the Measures.
7. Article 6 of the Measures.
8. Article 8 of the Measures.
9. Article 10 of the Measures.