THE IMPACT OF CHINA'S NEW CYBERSECURITY LAW

SHIH Hui Min & XUE Jianyue

EAI Background Brief No. 1344

Date of Publication: 19 April 2018

Executive Summary

1. In November 2016, China passed the Cybersecurity Law to consolidate and expand many existing laws and regulations governing cyber activities on the Chinese mainland. The Cyberspace Administration of China (CAC) and the relevant provincial departments are in charge of implementing and executing the law.

2. The Cybersecurity laws are passed to enforce China's cyber sovereignty, protect critical information infrastructure (CII), gather sensitive data through CII within mainland China, institutionalise and legalise China's cyber management, strengthen security of citizens' personal information, and improve quality and credibility of online discourse.

3. Since the Cybersecurity Law came into effect in June 2017, CAC and several provincial authorities have released new strategy papers, regulations and standards to enforce the law.

4. CAC and local cyberspace authorities have prosecuted both public and private entities for neglecting to plug security loopholes in their websites, failing to obtain the required certifications and allowing their websites to host banned content. Chinese internet giant Tencent has been slapped with the "highest fine" after harmful banned content was found posted on WeChat.

5. Foreign multinational companies have expressed concern over higher operating costs, reduced innovation due to data localisation and loss of intellectual property during security reviews by the government.

6. According to data released by various Chinese government agencies, the new Cybersecurity Law has reduced cybersecurity incidents experienced by netizens. However, the leaking of users' data, hacking incidents and telecommunication fraudulent activities are still frequent.

7. Many websites remain vulnerable to cyberattacks in China. The China National Vulnerability Database recorded 15,981 “national information security vulnerabilities” in 2017, a big 47.7% jump from 2016.

8. China’s cybersecurity industry is growing rapidly. CAC estimates that the Chinese cybersecurity industry (including products and services) will reach RMB45.71 billion in 2017. Cybersecurity clusters and new cybersecurity companies are rapidly emerging in major cities such as Chengdu, Shanghai and Wuhan.

9. In the process of implementing the Cybersecurity Law, China has to continue to assuage international concerns over its tightening internet controls. China will need to strike a balance between cybersecurity needs and ensuring sufficient data flows to promote industrial and technological development. Cyberspace sovereignty does not equate to “data sovereignty”.

10. Although the Cybersecurity Law had some positive results, data shows that some cyber threats remain persistent. China needs to continuously conduct research on cyber threats and make the necessary changes and expansions to provisions in the Cybersecurity Law.