RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 081 – 28 April 2017

China's Cybersecurity Policy: Security or Protectionism?

By Adam Palmer

Synopsis

China's upcoming national cybersecurity policy addresses security incidents, but also raises new challenges and concerns for global businesses operating in China.

Commentary

IN November 2016, the Chinese government adopted a new national cybersecurity policy that will become effective on 1 June 2017. The policy was adopted despite more than 40 business groups from the United States, Europe and Asia submitting petitions requesting significant changes to the policy.

These claims argue that the policy is protectionist, intrusive, and burdensome. China has defended the policy and stated that these claims are exaggerated or untrue. Like similar data breach notification laws in the US and Europe, companies operating in China will be required to report "network security incidents" to the government.

Vague New Requirements

However, the Chinese law raises concerns by adding a vague requirement for "technical support" to government agencies during investigations. The ambiguous definition of "technical support" has raised fears that this might imply government surveillance or "backdoors".

The new cybersecurity policy also includes heightened cybersecurity standards, greater controls for security of critical infrastructure, and requirements for transparency by eliminating anonymized registration for some online services.

Finally, the policy includes *data localization* requirements for critical infrastructure operators, which will restrict global businesses whose operations depend on cross-border data transfers of business information. Security experts also worry that the policy may hinder rapid cross-border sharing of threat intelligence, which is critical to improved security.

Enforcement of the new policy is outlined through fines for non-compliance and government authority to punish organisations or individuals. This includes freezing foreign-owned assets or possible physical detention of persons accused of wrongdoing.

Security or Protectionism?

As the new Chinese law requires systems to be proven to be "secure and reliable", this has raised foreign business concerns that authorities might require the disclosure of product "source code". It is feared that authorities might use these trade secrets to help domestic Chinese competitors. A business that is declared to be "not secure", might even be excluded from the China market.

Foreign businesses also worry that the policy could be used to favour Chinese hardware firms like Lenovo and Huawei or local cloud-computing services such as Alibaba, under the guise of security and reliability. The Cybersecurity Administration of China (CAC) has dismissed these concerns, stating that the new policy requirements for "secure and reliable" technologies are not intended to create a trade barrier or exploit security for competitive business advantages.

Data Localisation: China Counters Global Trends

The new cyber policy restricts "Critical Information Infrastructure Facilities" (CI) - which is defined broadly - from transferring data outside China, and only allows data transfers upon a showing of business need and approval of Chinese authorities.

China's new data localisation requirements are counter to global trends. For example, a consultation organised by the European Commission on international data flows (both personal and machine-generated data) in 2017 is expected to result in a legislative proposal outlawing unjustified restrictions by the EU Member States on data localisation requirements.

Critics of data localisation requirements argue that they hinder globalised operations and require investment in expensive local data storage centres, instead of using global economies of scale. For example, even transfers of basic internal employee data cross-border may be prohibited.

Data localisation laws may also be counterproductive for security. Cyber-attacks are nearly always cross-border. An effective response depends on borderless sharing of threat intelligence. Adopting a closed border "bunker" mentality is generally considered a hindrance to security and counterproductive.

What to Expect Next

Chinese authorities have stated intentions to stay ahead of a so-called “global cybersecurity arms race” and emphasised that China will use military means if necessary to protect its Internet sovereignty. The Chinese National People’s Congress, Legislative Affairs Commission, has dismissed concerns about China’s new cybersecurity policy and emphasised it is only “to protect the security and credibility of the Internet” in China.

This is part of an ongoing struggle to balance supporting economic growth in the digital sphere while also protecting against Internet activity that is viewed by the government as politically destabilising. China has traditionally focused on domestic control of Internet traffic and has repeatedly asserted its right to “cyber sovereignty”.

Edward Snowden’s revelations of US cyber espionage raised further concerns about foreign businesses in China. In recent years, there has been a growing call for development of Chinese IT products and increased regulation of foreign businesses. The new Chinese Cybersecurity policy is a reaction to these concerns. It is an attempt to increase transparency and control over the online operations of foreign companies in China.

End Goal: Securing Regime and its Power?

Only time will tell after June how the Chinese government will enforce the vague requirements of this new policy. Like many Chinese laws, this may be more of a “warning” before a more severe enforcement action is implemented.

Chinese law also follows a process of general adoption and then detailed implementation. It is reasonable to expect that the government will continue to have discussions with industry to clarify and refine the ambiguous parts of the new policy. Many of the concerns may be addressed during this process. In the mean-time, foreign companies operating in China may need to spend time talking with government officials to understand what this really means.

What is the purpose of the new policy? It is important to recall the guidance of a Chinese historian, who observed that “whether it is national security law or cybersecurity law, they are both an effort to secure the regime and its power”.

Adam Palmer is a Partner in CyCap, a global cybersecurity consulting firm, and Senior Research Fellow (Cybersecurity) at The Kosciuszko Institute, Poland. He is a former US Navy Officer, Prosecutor, and Head of the UN Global Programme Against Cybercrime. He contributed this exclusively to RSIS Commentary and can be contacted at apalmer@cycap.net.