March 2019

DID CHINA JUST LEGALIZE ESPIONAGE?

RECENT PROVISIONS TO CHINESE LAW INCREASES RISK TO MULTINATIONAL ORGANIZATIONS OPERATING IN CHINA

Authored By:

Drew Spaniel, Lead Researcher, ICIT
Parham Eftekhari, Executive Director, ICIT

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Did China Just Legalize Espionage?

Recent Provisions to Chinese Law Increases Risk to Multinational Organizations Operating in China

March 2019

Contents

Chinese Authorities Now Have Unfettered Access to Your Business

Imagine a scenario where Chinese government authorities could legally enter your facilities on mainland China, with zero notice, and have virtually unfettered access to your organization's data. Under a new provision to China's 2017 National Cybersecurity Law (CSL), entitled "Regulations on Internet Security Supervision and Inspection by Public Security Organs," this scenario is now a reality.

The original National Cybersecurity Law gave Chinese authorities the right to evaluate the source code of technologies used by foreign companies operating in China under the guise of identifying vulnerabilities through "national security reviews." Some firms, such as Recorded Future, postulated that the law could be abused by Chinese state agencies to identify zero-day flaws and other vulnerabilities that could later be exploited by state-sponsored attackers to compromise the systems of western companies and exfiltrate sensitive consumer data or intellectual property.

The new provisions to the CSL, issued November 1, 2018, give the Chinese Ministry of Public Security (MPS) the legal authority to remotely conduct penetration tests on the systems and networks of any Internet-related business with at least five internet-connected computers, operating in China [1].

International organizations in all sectors operating in China, including academia, healthcare, finance, energy, consulting, and critical manufacturing, should consider the impact that this new level of access has on the security of their data and react accordingly. This may call for measures which require network segmentation or closing Chinese offices and facilities.

Understanding Who's Behind This: About the Ministry of Public Security

The Ministry of Public Security (MPS) is China's primary police and security authority and is tasked with a wide variety of security duties, including but not limited to, border security, administering national identification cards, handling and collecting data according to numerous cybersecurity regulations, the Golden Shield Project (including China's Great Firewall), China's surveillance camera network, and its nationwide facial recognition system [1] [2].

In 2017, the CSL charged the MPS responsible for "cybersecurity protection, supervision, and management" within its larger scope of investigating matters in public and internal security. The MPS is also responsible for punishing violators of the CSL. Some of the new provisions to the CSL specify minimum cybersecurity measures and controls that must be implemented at the county level to manage cybersecurity under the CSL. However, other more nebulous articles within the provisions grant the MPS new sweeping powers that threaten any business currently operating in China as well as every datum of information stored on their networks [2].

The Perils of the New Provisions to the Chinese National Cybersecurity Law

Perhaps the most dangerous aspect of the new CSL provision is in how vaguely the law is written, giving Chinese authorities wide latitude to act under its purview.

According to the law, public security branches of the MPS at the county level and above can conduct inspections on networked units and ISPs that provide any of the following: internet access, data centers, content distribution, domain name services, internet information services, public internet services, or other internet services. The broad definition and authority allows for the inspection of any company providing any type of internet related service, ranging from a SaaS organization to any company that provides internet access to five or more computers within its network [2]. Since the Yunnan Network Security Corps, a branch under the MPS, defines a networked unit as "a unit with a fixed IP or with five or more computers connected to the internet to conduct internet or internet-related activity," most if not all business branches operating in China qualify as "networked units." Consequently, every branch is subject to inspections, no matter their sector or function [2].

Under Article 15 of the new provisions, the MPS can enter almost any business premises, computer room, workplace, or company area related to networked systems in order to check computer systems for network security compliance. The officers can view or copy any information deemed "related to the inspection," which includes, but is not necessarily limited to: any and all user information; technical network data; information security protection, hosting, or domain name information; and any content distributed by the organization.

Any hosted content determined prohibited information found through an inspection can be prosecuted under the Cybersecurity Law [2]. Worse, any data that government officials find on the system can be copied and later shared with other agencies [1]. Further, the inspections may be carried out at any time, with no prior notice, and for any reason, such as "checking if companies are storing illegal content" on their servers.

Nearly all foreign businesses operating in territorial China can be subject to in-person facility searches, have their company and user data copied, have their servers combed for "illegally published materials," and have their networks remotely "inspected." Chinese authorities could even search servers for content and later leverage their findings to either draft new censorship provisions or intimidate companies to restrict or ban content deemed controversial to the CCP [1].

Under the new system, the MPS has the power to:

- Conduct in-person or remote inspections of the network security defenses taken by companies operating in China.
- Perform remote inspections without informing companies.
- Perform penetration tests to check for vulnerabilities.
- Log security response plans during on-site inspections.
- Check for "prohibited content" banned inside China's border.
- Copy any user information found on inspected systems during on-site or remote inspections.
- Share any collected data with other state agencies.
- Have two members of the People's Armed Police (PAP) present during on-site inspection to enforce procedures.

Under the new law, the MPS is not required to notify companies when it remotely inspects a system or conducts penetration testing. The scope of remote inspections is not defined and could include activities ranging from traditional penetration testing to the installation of system backdoors [2]. Article 16 only requires that the MPS notify the inspected company of the date and scope of the inspection. The regulations do not limit the scope or time frame of the inspection. Article 17 empowers the MPS to involve third-party “cybersecurity service agencies” in the inspections. As a result, organizations may be at substantially greater risk of vulnerability discovery, compromise, and data leakages.

The MPS is not required to share a report of its findings with the company nor is it required to report what data is collected from "inspected" firms. Article 18 dictates that a supervisor within the inspected organization must sign an inspection report produced by the MPS during an on-site inspection, but no signature is required for remote inspections. The only mandatory communication between the MPS branch and the company prior to a remote inspection is notification of the inspection time, scope, and "other matters." Which systems were inspected, the purpose of the inspection and the findings are not required to be communicated to the company. The wide scope of Article 16 may authorize MPS officers to access portions of the company’s network that are not related to or within territorial China [2].

Article 6 requires that the MPS share reports of the inspections with relevant government departments. The provisions do not specify which PRC divisions are deemed “relevant”. Therefore, any information obtained during an inspection could be leveraged by a state or foreign surveillance entity to monitor corporate and customer data. Meanwhile, Article 19 requires that MPS branches supervise and guide organizations to mitigate against any hidden network security risks found during inspection; however, the mechanism by which guidance is

offered is not specified. Legally, under the new provisions, MPS agents could discover a vulnerability in "inspected' company's systems, gather its data, and later share the vulnerability or data with other agencies or state-sponsored entities [1].

The vague language of the law does not specify which data MPS officials are permitted to copy. It is not clear if only the information of Chinese citizens may be copied and shared or if the purview allows for the collection, storage, and transmission of all company data, including that of foreign citizens and consumers [1]. It is also not clear whether content published outside of the Chinese language internet is subject to the CSL [2].

The Risk to Organizations

Organizations and consumers alike are at greater risk of having their data held by the Chinese government and are at a significantly greater risk of third-party data breaches and Chinese government surveillance [1]. The possibility of unlimited, unbounded "remote inspections" of international corporations presents a significant threat to consumers, corporations, and governments. The vague and remarkably broad articles of the new provision mean that at any time, any company operating in China could have its domestic or foreign networks compromised while its company IP, consumer PII, and other valuable data is "legally copied" and later shared with unspecified entities [2].

In short, the new regulations place companies' network infrastructure, data, and proprietary information at risk of sabotage, surveillance, censorship, or intimidation operations. Companies may be extorted with the threat of inspection that "will find illegal material." Consumer data may be stolen, exploited, or sold without any notice or choice. State-sponsored APTs and authorized third-parties may breach, surveil, and laterally infect corporate systems. US and other nations' companies operating in China may be pressured or have their IP stolen so that Chinese companies with similar goods can excel. The armed officers present at in-person inspections ensure that any employee who resists the checks may experience physical harm [2].

International organizations should consider their technology footprint within China and evaluate how to best minimize their system architecture to limit their presence. If possible, they should segment their network in China from their international networks. They should also evaluate their evacuation and government relations policies. They should routinely and rigorously inspect their systems for exploitable vulnerabilities, malware, or any indication that state-sponsored threats may have compromised their network. To quantify the risk to global operations, firms should ascertain which parts of their Chinese infrastructure have been registered as networked units and they should prioritize updating, patching, and segmenting those systems. Finally, organizations should take great care in considering if any information

stored on their network may be deemed illegal to publish under the CSL and they should minimize, sanitize, or eliminate that content [2].

Conclusion

Since 2017, China's Cybersecurity Law posed a risk to any company operating within its territory. The new provisions issued on November 1, 2018, amplify the risk that systems and networks may be compromised while also significantly increasing the risk to consumers' data and corporate infrastructure located outside of China. Companies with a physical presence in China must fully understand the impact of these laws on their security posture based on their risk tolerance and make necessary changes to their network, office and facility strategies accordingly.

Sources

[1] C. Cimpanu, "China's cybersecurity law update lets state agencies 'pen-test' local companies | ZDNet", *ZDNet*, 2019. [Online]. Available: https://www.zdnet.com/article/chinas-cybersecurity-law-update-lets-state-agencies-pen-test-local-companies/. [Accessed: 25- Feb- 2019].

[2] “China’s New Cybersecurity Measures Allow State Police to Remotely Access Company Systems", *Recorded Future*, 2019. [Online]. Available: https://www.recordedfuture.com/china-cybersecurity-measures/. [Accessed: 25- Feb- 2019].