The Institute for National Security Studies
Strategic, Innovative, Policy-Oriented Research

INSS Insight No. 912, April 3, 2017

China's New Cybersecurity Law

Israel Kanner and Doron Ella

China's new Cybersecurity Law will go into effect on June 1, 2017. According to official statements, the purpose of the law is to protect China's national security and social stability through close supervision of internet content and technologies. The law has the potential to affect every Chinese or foreign internet or information technology business operating in China. After the law was announced, there were concerns in the West that the continued operation of foreign companies in China will be conditional upon their providing information and technologies to Chinese authorities, or on the inclusion of "backdoors" in their products. Another concern is that foreign companies will be forced to make way for local governmental companies that develop products that are adapted to the regulations of the Chinese market.

Background to the Law

The new Cybersecurity Law joins the NGO law and the anti-terror law that were passed last year with the purpose of limiting and restraining the activity of organizations and individuals within mainland China. The law is part of an intensifying legislative trend that seeks to increase the Chinese government's control over the technology-internet realm, thereby reducing potential threats to the regime's stability as a result of free discourse over the internet. An example of this is the self-restraint charter of 2002 of the Chinese internet industry, which transferred legal responsibility for preventing the distribution of unauthorized content to the content providers themselves, thus turning them into agents of government censorship. The 2016 Chinese legislation on cybersecurity, international NGOs, and terrorism demonstrates the Chinese communist party's increasing fear of the penetration of foreign influences, including Western liberal or Islamic ideas and inspiration from national separatist movements. One of the tools the party uses to control content disseminated on the internet is the "Great Firewall of China," which is responsible for blocking access to prohibited Western internet services, such as Google and Facebook. The cyber law is another step in the party's tightening grip on such information and in solidifying its governmental power.

Israel Kanner is an Israel Institute Research Associate. Doron Ella is a Glazer Research Associate.

Main Points within the Law

The Chinese Cybersecurity Law, which has the potential to affect the West in general and Israel in particular, is meant to protect China's national security and the communist party's rule. The law requires internet users to refrain from activities that endanger Chinese security, honor, or national interest (article 12), and prohibits opposition to the communist party and attempts to overthrew the socialist system, promote terrorism and religious separatism, or disseminate false information that could harm the economy or the social order. This provision demonstrates an attempt to shape the use of the internet in a way that matches the party's needs and aims. The law calls on the nation to take an active part in enforcing it, and thus demands (article 14) that every person or organization that identifies subversive activity on the internet report it immediately to the relevant government ministries.

The law includes a number of articles that raise specific concerns for Western companies. First, the law calls for gathering civilian information and keeping it within China's borders. Article 37 states that all personal information gathered in China by companies involved in essential information infrastructure must be saved on Chinese servers (there is a special protocol regarding information that must be saved on servers outside China). Article 24 states that companies that provide services such as domain names, distribution of information online, messaging services, and so on must demand customers' authentic personal information and, if they refuse to provide it, must not provide them with service.

Second, companies are required to assist governmental-party agencies involved in national and public security. Thus, article 28 states that network operators shall provide technical assistance to public security agencies that require it. The law's vague wording here raises concerns that companies will be required by law to disclose information on their customers, with no legal ability to refuse. Article 49 states that network operators must also cooperate with government departments regarding routine checks and supervision. Article 50 adds that government authorities have the right to require companies to erase information if, in their opinion, it is dangerous or illegal.

Anyone who violates the law is subject to a fine of up to 1 million yuan ($144,000). However, article 75 provides a few details on the nature of punishments for foreign companies: when foreign institutions, organizations, or individuals engage in illegal cyber activity that endangers essential Chinese information infrastructure and national security, the relevant government ministries will be entitled to freeze their assets and take any punitive measures necessary. Here too, the law's expansive wording, especially "any punitive measures necessary," places the future of companies seeking to operate in the Chinese market at the discretion of the various government authorities in China.

Implications for Israel

The legislation demonstrates the Chinese government's awareness of the increasing economic and governmental potential of internet applications that can be used to accumulate economic power in mainland China and abroad and exert political influence. It likewise bespeaks the government's intention to strengthen its supervision and control measures over internet operations by citizens and foreigners within Chinese territory, in order to fortify governmental stability. Since from the government's perspective depending on foreign technologies constitutes a potential threat to national security, it seeks to upgrade its interest services and cyber capabilities vis-à-vis its competitors in the West. The new legislation sets out a course of action for Chinese companies, which will need to improve their technology to meet the government's needs and demands.

China sees Israel as a source of technological knowledge and innovation, which has helped deepen trade relations between the two countries in recent years. However, the new Cybersecurity Law could complicate the continued positive development of these relations. Every Israeli technology company that is involved in social media or information will be supervised by the Chinese authorities and will be forced to operate under many more restrictions than before. Israeli companies interested in operating in China will have to take into account the fact that the Chinese government will be able to demand that their source code be submitted for review (for example, the case of Apple). This demand gives the government a "backdoor" through which it can access the source code of Western companies and make use of it for its own purposes, as well as allowing the code to be copied by Chinese companies connected to the government. In addition, the government will be able to demand the information collected on the companies' Chinese customers, which could create an ethical problem if the information is used against citizens. Therefore, the relevant Israeli government ministries would do well to work together in order to raise awareness about the new Chinese Cybersecurity Law among Israeli companies currently operating in China or those interested in operating there in the future. Furthermore, even though Israeli companies in foreign countries are required to operate in accordance with local regulations, there is room to consider the possibility of providing special legal assistance to companies operating in China in view of the unique challenges they will confront.