China Expands its Counter-Espionage Law

Date Published: May 12, 2023

Summary

In late April, the People's Republic of China (PRC) passed amendments expanding its counter-espionage law, by broadening the definition of spying and the transfer of national security information. In tandem with several recent incidents of private sector organizations facing law enforcement action, OSAC members have increasingly expressed concerns over the security of the operating environment in the PRC. This report examines the updates to the counter-espionage law, outlines several of these recent private sector incidents, and provides guidance to the private sector.

New Counter-Espionage Law

On April 26, the Standing Committee of the National People's Congress (NPC) amended the PRC's counter-espionage law. The additions to the 2014 law, which will take effect on July 1, add to the already broad definition of what the PRC deems to be national security-related information and data. With the new amendments, all "documents, data, materials, and items related to national security and interests" fall under the same legal protections and category as state secrets. However, the PRC has yet to define what is considered "national security and interests."

The revision to the law also expands the definition of espionage broadly, to include cyber attacks against government entities or critical infrastructure. While conducting counter-espionage investigations, the amendments include the authority to access data and electronic equipment; seek out information on personal property; and ban border crossings (i.e., "exit bans").

Recent Issues for Private Sector Organizations

In recent weeks, around the time of the counter-espionage law amendments, several incidents of private sector organizations facing PRC law enforcement action have been recorded, across several different sectors:

- **Mintz Group:** In the first case to make international headlines recently, the U.S. due diligence firm Mintz Group had five of its local staff detained in late March. PRC security services raided the firm's Beijing office and arrested five local nationals working for the company. According to reports, Mintz's Beijing office was conducting audits into Xinjiang supply chains, an area allegedly considered sensitive by the PRC.

- **Astellas Pharma:** Following immediately on the heels of the Mintz raid, Astellas Pharma, a Japanese pharmaceutical company with operations in the PRC, had an employee detained in late March just before he was set to depart the country. The individual, a Japanese national, was allegedly arrested on espionage charges and had been held since early March. Though he had lived and worked in the PRC for more than 20 years, he was arrested by authorities connected with the national security establishment.

- **Bain & Company**: In late April, the PRC security services visited the Shanghai office of the management consulting firm Bain & Company. According to one source, the authorities questioned employees and confiscated computers and phones; no employees were reportedly detained, however. This was also not the first time Bain's Shanghai office had been visited, according to the *Financial Times*.

- **Micron Technology**: In the first major incident involving a U.S. chip manufacturer following the U.S. export controls on semiconductors to China, PRC authorities launched an investigation into Micron in early April. China's Cyberspace Adminstration noted that it would "review imports of Micron's products in order to maintain national security, ensure the security of its information inftastructure and prevent risks caused by product problems."

- **Capvision:** Details emerged in early May that the dual U.S.-China headquarted company—which operates a network of experts available for business consultations with clients across several industries—had several of their offices in the PRC raided; employees in their Shanghai, Beijing, Suzhou, and Shenzhen offices were questioned as well. China's national broadcaster, CCTV, even singled out the firm in a news broadcast on May 8. According to that report, the company "accepted a large number of consulting projects from overseas companies on industries sensitive to China, and some of these firms had close ties with foreign governments, military and intelligence agencies."

Private-Sector Impact

Following a string of detainments and raids on private sector organizations, several OSAC members have expressed concerns regarding travel to and operations in the PRC. Based on the revised counter-espionage law as well as commonalities among those organizations targeted by PRC security services, OSAC members are advised to deeply examine the type of work their organizations are engaging in within the PRC. As several of the abovementioned examples underscore, work that in the past may have been allowed or even considered routine, is increasingly being labeled as sensitive, and therefore cause for action from the security services.

While due diligence and audit firms have made a majority of recent headlines, it remains unclear what sectors—if any—are under particular focus from authorities. Therefore, it is imperative that OSAC members consider reevaluating engaging in sensitive work or research, particularly in areas of political sensitivity or related to national security (i.e., Xinjiang, Taiwan, personal identifiable information (PII), etc.). While the recent additions to the counter-espionage law broaden the definition of espionage—and therefore muddy where the PRC's red lines are—OSAC members should ensure that the work their organizations engage in do not run afoul of the law.

OSAC members are also advised to comply with PRC authorities' investigations, as non-compliance may exacerbate the situation. Should a U.S. citizen employee be detained by PRC authorities, the U.S. Department of State provides guidance on the ways in which the nearest embassy or consulate can assist.

Additional Information

For more information on the security environment in the PRC and across Asia, contact OSAC's Asia team.

- OSAC Country Page: China
- OSAC Country Security Report: China
- U.S. Department of State Country Page: China
- OSAC Report: The Effects of China's New Data Security Law and VPN Restrictions on Information Security
- OSAC Report: China's Data Security Law