Forum for American Leadership

China's Crackdown on Foreign Business and How Congress and the Private Sector Should Respond

July 19, 2023

Executive Summary

- **China is cracking down on foreign and foreign-facing companies, launching raids and investigations, freezing acquisitions, and arresting Chinese and foreign nationals**. This campaign underscores the **increasing risks** that foreign businesses take in conducting business in China.

- The U.S. government and American companies operating in China **should prepare for ongoing Chinese pressure** by exposing Beijing's coercive actions, developing public-private coordination and intelligence sharing, and establishing contingencies for hostage taking, data theft, and other malign activities.

The Current Situation

China has taken a range of steps targeting foreign interests that fall into two broad categories: (1) legal and regulatory measures to hamper foreign business transactions and increase the risk of conducting basic business activities; and (2) raids, investigations, and arrests targeting foreign businesses.

Since March, China has:

- Passed a new counter-espionage law, which takes effect July 1, banning the transfer of any information related to "national security", expanding the definition of what could constitute espionage to capture a wide array of regular business activity, and permitting inspection of baggage and electronic devices;

- Slowed merger reviews of several proposed acquisitions of U.S. companies, including Intel's purchase of Israel's Tower Semiconductor, meant to boost Intel's planned semiconductor foundry business, a core aspect of its plan to restore its competitive edge;

- Considered banning exports of critical materials, including rare-earth magnet technology used for electric vehicles;

- Suspended the consulting firm Deloitte's operations in Beijing and imposed a $31 million fine;

- Conducted a rapid cybersecurity investigation of the U.S. memory chip maker Micron, and within two months banned major Chinese firms from purchasing Micron goods;

- Raided the U.S. due diligence firm Mintz and arrested five local employees;

- Conducted a surprise visit of four offices of Capvision, which provides expert consultants and research, and forced the company to publicly confess its alleged crimes;

- Raided the consulting firm Bain & Co.'s office in Shanghai, interrogating employees; and

- Barred people from leaving the country, including foreign executives.

Implications

- Despite official rhetoric about Chinese openness to foreign capital, China's assault on foreign businesses signals that **Beijing seeks to tightly circumscribe the nature of that investment.** The Chinese Communist Party views foreign capital with suspicion and seeks to extract value from foreign companies while restricting information flows and subjecting them to the specter of investigations, data theft, and hostage diplomacy. To underscore this point, Xi Jinping has reportedly put his Minister of State Security, Chen Yixin, in charge of the campaign against foreign corporations.

- China also wants to limit even routine information collected by foreign companies—such as auditors, management consultants, and law firms—that underpins investment opportunities. Chinese authorities seem particularly sensitive to the notion that these entities would help their clients comply with U.S. law in ways that might run contrary to Chinese interests, such as strictly complying with the Uyghur Forced Labor Prevention Act, or determining how to restructure their supply chains to reduce dependence on China.

- China may increasingly retaliate against U.S. and allied companies in response to trade and technology restrictions imposed by the U.S. and allied governments, such as the controls issued in October 2022 that restrict chip and equipment exports to China. One recent example of such retaliation can potentially be seen in the Micron investigation.

The Way Forward

The U.S. government should take several steps to help protect American business interests in China.

1. **The Biden Administration and Congress should publicly expose China's actions**, as House China Select Committee Chairman Congressman Mike Gallagher did when he publicly encouraged U.S. companies to recognize that China's recent behavior represents a clear trend, rather than random anomalies. For example, the Administration should publicize Chinese intimidation and blackmail efforts against U.S. firms and make clear that ongoing aggressive actions against them will result in diplomatic consequences, such as delaying sought-after high-level engagements. It should also educate U.S. businesses on the increasing risks of operating in China.

2. **The Administration and Congress should establish formal and informal mechanisms to facilitate intelligence sharing and cooperation with private-sector actors operating in China**, similar to those established for cyber threats, such as the Joint Cyber Defense Collaborative. For example, the U.S. government should encourage U.S. companies to report Chinese malfeasance and establish outreach programs that offer toolkits, such as recommended risk reduction measures, best practices for travel policies and data protection, and playbooks for arrests of employees. The Administration and Congress should also consider asymmetric responses to China's crackdown, such as expanding the work of the new "technology strike force" established earlier this year to counter Chinese espionage and sanctions evasion efforts.

3. **The Administration should prepare for ongoing episodes of hostage diplomacy, in which it may need to protect Americans unjustly detained in China.** Congress should insist that the Administration develop a strategy that does not involve lopsided exchanges or other concessions that incentivize further hostage-taking.

4. **The Administration and Congress should substantiate the Coordination Platform on Economic Coercion announced by the G7 in May**. This channel is meant to increase G7 collective assessment, preparedness, and deterrence and response to economic coercion. Through the Coordination Platform on Economic Coercion, as well as other channels, the Administration should coordinate allied responses, including potential defensive and retaliatory measures. They should also coordinate support for victims, such as by pooling costs to aid targeted companies and preventing companies in allied nations from taking advantage of Chinese actions to increase their own market share.

Ultimately, **the U.S. government's ability to protect U.S. business operations in China is limited. Companies themselves will need to mitigate their own risks**, such as by not sending U.S. nationals to work in China, limiting their exposure to intellectual property (IP) risk in China by refusing to enter into joint ventures or holding IP in China, encrypting data being transmitted in and out of China, and by adding risk clauses to contracts with clients in the event of CCP raids or geopolitical tensions.

The CCP continues to believe that multinational corporations and investors do not wish to lose their access to the Chinese marketplace and therefore will ultimately fall in line. In the face of that belief, U.S. companies should prepare for escalating pressure.

This paper is a product of the Forum for American Leadership's Technology and National Security Innovation Working Group.
