The recent indictment of Huawei and its Chief Financial Officer on charges related to sanctions evasion and theft of trade secrets was the latest salvo in the United States’ multi-pronged pressure campaign targeting China. Even if U.S.-China trade disputes are resolved in the coming weeks, institutions engaging in business with China, Chinese state-owned entities, or private individuals and entities subject to Chinese government influence should be cognizant of the escalating enforcement and regulatory risks. The charges in the indictments—which were unsealed in January 2019 after Canada detained Huawei’s CFO at the request of the United States—echoed those in other recent indictments and enforcement actions targeting Chinese actors, including violations of U.S. sanctions, money laundering, financial and wire fraud, and theft of U.S. trade secrets. The charges also implicated Huawei’s CFO in directly defrauding financial institutions.

The Trump Administration has deployed a variety of policy and enforcement tools from across U.S. government agencies to protect the United States’ national and economic security in accordance with the objectives laid out in its 2017 National Security Strategy. Its focus has expanded beyond the proliferation, financial crimes compliance, and banking issues central to many of the most high-profile past actions to encompass issues related to cyber and economic espionage, intellectual property theft, sensitive areas of foreign investment, and trade and export violations. The U.S. Department of Justice in November 2018 launched a China Initiative to investigate and prosecute intellectual property theft. In the past two years, the United States’ coordinated pressure campaign has leveraged the authorities of financial sector supervisors as well as the Justice, Treasury, and Commerce departments, the FBI, the legislative branch, and the Committee on Foreign Investment in the United States (CFIUS) to target Chinese actors through the use of regulatory enforcement actions and fines, sanctions, export controls, criminal prosecutions, legislative authorities, and tariffs. In addition, the Trump Administration considered using executive authority to ban Huawei and its Chinese rival ZTE from being able to sell products to U.S. companies, and in 2018 the Commerce Department briefly banned ZTE from using American products.

The U.S. strategy to exert pressure on Chinese actors also encompasses domestic trade policy and the imposition of U.S. tariffs on Chinese goods to
combat unfair practices—including intellectual property theft, forced technology transfers, ownership of American companies in China, and tariff and non-tariff barriers to U.S.-China trade—that were described in reports from the Office of the U.S. Trade Representative and the White House Office of Trade and Manufacturing Policy. Recently, U.S. diplomatic outreach to other countries about the risks that China poses to their national and economic security also has become a public element of the U.S. strategy.

The escalation of U.S. pressure through the expansion of both the authorities being deployed and the target sets for enforcement actions demonstrate the Trump Administration’s willingness to pursue sensitive targets to push back against perceived Chinese aggression. During the decade prior to the Trump administration, enforcement actions against Chinese actors were often more limited in scope or focused on smaller or less sensitive targets, and the United States used multilateral channels such as the World Trade Organization rather than unilateral tariffs to raise concerns about unfair trade practices.

▶ In contrast, Huawei is China’s largest private company, was founded by a former People’s Liberation Army officer, and has operations and products that are deeply embedded in many foreign markets and foreign businesses. The charges against Huawei and its affiliates, coupled with the detention of its CFO in Canada, signal that the Trump Administration may not shy away from targets previously deemed too large or sensitive to pursue.

▶ In addition to targeting large Chinese private entities, the Trump Administration has also pursued enforcement actions against elements of the Chinese government. Two employees of China’s Ministry of State Security were indicted in late 2018 for their roles in intellectual property theft and cyber security breaches. The previous administration reportedly declined to pursue similar action in the wake of revelations that China had hacked the U.S. Office of Personnel Management.

▶ Separately, in September of 2018, the United States sanctioned the Chinese military’s Equipment Development Department for buying military equipment from Russia.

The expanding, multi-pronged approach to targeting Chinese actors requires financial institutions, multinational companies, and jurisdictional authorities awarding public contracts to take a comprehensive approach to managing risk that encompasses not only illicit finance risk but also broader concerns about the economic and national security implications of relationships and partnerships.
with Chinese actors. The targeting of Huawei and ZTE, which are two of China’s most prominent companies and are highly integrated with foreign markets and foreign businesses, illustrates the complex consequences and financial implications for companies navigating relationships with Chinese entities amid changing attitudes toward the threats that they may pose.

- Global and regional financial institutions, particularly those based in the United States or that use dollar-clearing services, must conduct comprehensive and ongoing due diligence to understand the risks posed by their relationships with Chinese correspondent banks, their customers, and their technology partners and suppliers. Comprehensive due diligence and robust transaction monitoring are particularly critical to understanding exposure to corruption-related financial flows and potential sanctions evasion activities, both of which continue to be an enforcement focus for the United States.

- Multinational companies, investors, and jurisdictional authorities awarding public contracts must maintain compliance with any legal, trade, and technology strictures put forth by relevant governments, while also being aware of the potential national security implications of connections...
with Chinese actors. In the United States, changes to the CFIUS regime call for more stringent oversight of transactions and partnerships in 27 industries, and U.S. diplomatic outreach is encouraging other governments to apply additional scrutiny to key industries such as telecommunications and technology.49

- Allegations about Chinese human rights abuses in China and about the role of Chinese state-owned entities and technology companies in furthering repression domestically and abroad also raise reputational risks that financial institutions, multinational companies, and investors need to gauge.50-51 Conducting comprehensive due diligence prior to establishing relationships and engaging in ongoing monitoring of risk are critical to avoiding reputational and financial harm.

- Companies wishing to protect themselves from intellectual property theft while conducting business in China or with Chinese actors, or companies that possess data that may be of interest to a foreign government, should be vigilant regarding their current cyber risk profile and undertake vigorous measures to test the efficacy of their cyber security policies and procedures.
Endnotes


42 United States Department of the Treasury, Office of Foreign Assets Control, Specially Designated Nationals List at https://sanctionssearch.ofac.treas.gov/.


