American Security Project

U.S. Firms and China's Data Regime

Briefing Note

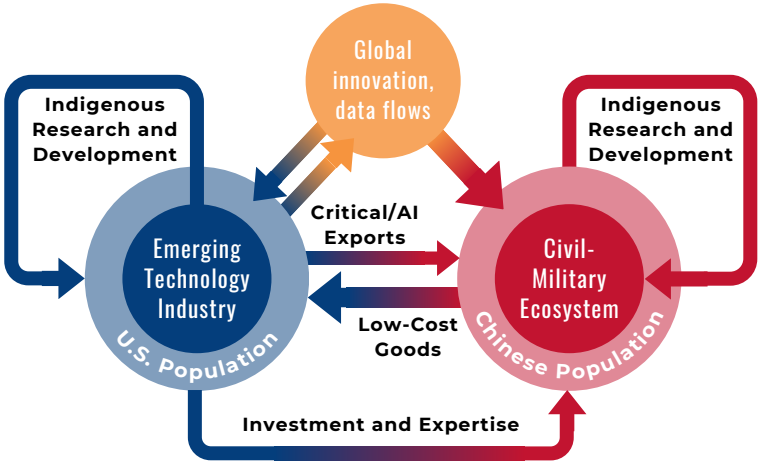
Quick Facts

- Since 2017, the People's Republic of China (PRC) has forced all domestic and foreign companies to share their intellectual property, technology, and consumer data with the Chinese Communist Party (CCP).
- American firms cannot store or share data produced in China elsewhere, creating a one-way data flow that accelerates the CCP's development of dual-use technologies like artificial intelligence (AI). Chinese entities also exploit U.S. data for propaganda, cyberattacks, and enhancing China's warfare capabilities.
- The United States must prevent China from unfairly exploiting democratic institutions by sanctioning its unacceptable data laws and preventing its contractors from operating in China. It must also prevent U.S. firms from selling consumer data that facilitates Chinese espionage, surveillance, and technonationalism.

China's Twin Goals: Technonationalism and Informatized Warfare

- China's ascent to the second-largest global economy has been fueled by norms and institutions founded and maintained by the United States and its allies. American open markets, direct investment, trade relations, and education and training programs continue to support its economic growth.
- Despite this, the CCP engages in illegal and anti-competitive practices such as espionage, forced labor, and theft of U.S. data and intellectual property to gain an asymmetric advantage over the United States.
- In 2020, Chinese General Secretary Xi Jinping's Innovation-Driven Development Plan announced the "intelligentization" of China's military and state security forces. As part of this national strategy, the Chinese Communist Party aggressively pursues U.S. critical technologies and data to use in state-sponsored cyber attacks, espionage, psychological warfare, and genocide of its religious minorities.

CHINESE TECHNOLOGY TRANSFER FLOW



Economic Levers of State Power

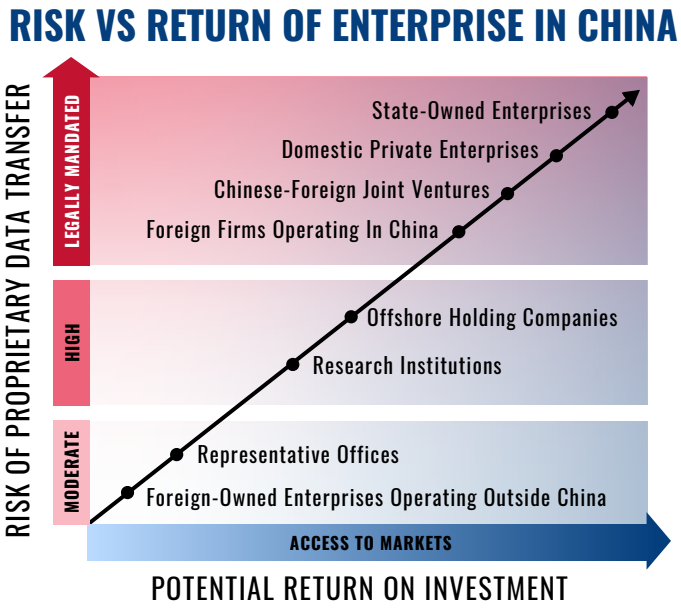
- The CCP holds absolute authority over the state's economic priorities, enabling disproportionate and highly efficient investments in strategic industries.
- Since 2000, it has invested $912 billion in advanced technology development, rivaling U.S. spending on all industrial policies combined in the same period.
- China now leads in 37 of 44 critical technologies, creating strangleholds within global defense, space, and telecommunications supply chains.

Predatory Data Transfer Regulations

- **2017 Cybersecurity Law**: "important firms" operating in China must store all data locally and transfer that data to state agencies upon request. All firms submit to preliminary state security reviews to determine the importance of their data. All firms must agree to censor free speech in line with CCP preferences.
- **2021 Data Security Law**: all tech firms operating in China are now subject to the 2017 law. Transfer terms are loosely defined, with fines exceeding $1.56 million per infraction. Firms are prohibited from providing any data stored in China to foreign entities without prior CCP approval, even when required by U.S. law.
- **2024 State Secrets Law**: any technology or data that could have an "adverse impact" on the state must be immediately disclosed to the CCP. This includes U.S. personal data, source code, and even government intelligence entrusted to or stored with American contractors such as Microsoft, Amazon, and Oracle.

Cyber Attacks on U.S. Infrastructure

- A 2022 Microsoft report warned that Chinese disclosure requirements were allowing CCP-affiliated hackers to exploit vulnerabilities in global telecom infrastructure.
- Since then, CCP hackers have continuously penetrated U.S. systems, including the U.S. State and Treasury Departments, telecom providers, and devices owned by President Donald Trump and Vice President JD Vance.
- Despite this, U.S. government contractors continue to operate in China, knowingly transferring sensitive data and technology to maintain access to Chinese markets.



Exploitation of U.S. Trade and Investment

- In 2023, 40% of surveyed American businesses in China were forced to transfer proprietary data to the Chinese state. An additional 21% voluntarily transferred data to "improve market access prospects."
- The CCP maintains a direct presence in the vast majority of companies that operate in China. Embedded CCP cells, super-minority stakes, "Golden Shares," and pre-agreement due diligence schemes allow China to influence decisions in U.S. firms and gain access to their proprietary data and intellectual property.

Policy Recommendations

1. Government contractors that handle or have access to sensitive U.S. data should not be allowed to operate in China, including through non-commercial research partnerships or mergers with Chinese firms.
2. Subsidiaries and partners of U.S. government contractors should not be allowed to store U.S. citizen data in mainland China or operate data centers or servers in China that can be accessed by U.S. citizens.
3. U.S. firms should be prohibited from selling or transferring U.S. consumer data to China-linked companies.