CHINA'S NATIONAL SECURITY LAWS
IMPLICATIONS BEYOND BORDERS

The People's Republic of China (PRC), under Chinese Communist Party (CCP) leadership, uses national security laws to assert PRC interests including modernizing China's military and controlling critical technology.

- From 2014 to 2023, the PRC government passed or revised over a dozen laws related to national security.
- PRC leaders use these laws to justify a range of restrictions, demands, and punitive actions against PRC and foreign firms and individuals.
- These laws are vaguely worded and could be expansively interpreted by PRC officials.
- These laws could pose risks for foreign governments, companies, and individuals in China and abroad.

Major PRC national security legislation:

Note: the dates show the month and year that each law came into force
**The law's full title is the "Law on Safeguarding National Security in the Hong Kong Special Administrative Region of the PRC"*

PRC national security laws justify an expansive range of possible actions

For example, these laws provide justification for China to:

- Access data or encryption keys held by foreign firms with operations in the PRC (Cybersecurity Law, Data Security Law, Cryptography Law)
- Detain foreign nationals living, working, or traveling in China, Hong Kong, or Macau and possibly beyond (National Security Law, Counterespionage Law, Law on Safeguarding National Security in Hong Kong)
- Prevent PRC entities and individuals from sending "sensitive" data abroad (Data Security Law, Counterespionage Law)
- Require PRC citizens to assist in intelligence-gathering activities (National Intelligence Law)

National security laws impose obligations upon individuals and companies, including data handling obligations

As the examples on the next page illustrate, multiple PRC national security laws and policies **target both PRC and foreign citizens, companies, and other groups** as well as the data these individuals and groups possess. To exert control over these individuals and groups, these laws impose strict requirements on the handling, storage, and export of sensitive information.

PRC AND FOREIGN CITIZENS must avoid a vaguely defined list of behaviors Beijing deems harmful to its security interests. They must actively cooperate with PRC officials, and in some cases, they can be held liable for actions outside PRC territory.

PRC AND FOREIGN COMPANIES face a host of requirements related to cybersecurity and data management and storage. Companies must report to and cooperate with PRC authorities, and they must assist with state-directed intelligence and counterintelligence efforts.

DATA may fall under the broad definition of information "related to national security and interests" and be treated as a state secret even if commercial in nature. Some data are also subject to restrictions on cross-border transfer.

DMM-2023-U-037195-Final

www.cna.org | CNA

PRC NATIONAL SECURITY LAWS: GLOBAL IMPLICATIONS

NATIONAL SECURITY LAW (2015)

Passed under Xi Jinping, this law reflects Xi's effort to establish "rule by law," using legal mechanisms to entrench CCP rule throughout the economy and society. The law requires PRC government actors, companies, individuals, and groups to cooperate with the CCP on undefined "matters of national security." By leaving "national security" undefined, the law empowers the CCP to invoke it as justification for taking any action leaders deem necessary to safeguard CCP rule or assert the CCP's core interests.

CASE STUDY: SANCTIONS ON US DEFENSE CONTRACTORS

In February 2023, the PRC Ministry of Commerce added US defense contractors Raytheon and Lockheed Martin to the PRC's Unreliable Entity List—a PRC sanctions list created in 2020. The PRC claimed that the two entities' repeated arms sales to Taiwan over the years had undermined the PRC's "national security" as well as its "sovereignty and territorial integrity" and thus violated the National Security Law.

COUNTERESPIONAGE LAW (2023)

First passed in 2014 and updated in 2023, China's Counterespionage Law expands the scope of what counts as espionage. Rather than just covering "state secrets," the updated definition counts any "documents, data, materials, and items related to national security and interests" as equivalent to state secrets. Unauthorized acquisition, sharing, or mishandling of these materials can be considered espionage. The routine professional activities of a variety of groups—businesspeople, government officials, researchers, and journalists—could now be deemed espionage.

CASE STUDY: DETENTION OF JAPANESE PHARMACEUTICAL EXECUTIVE

In March 2023, a spokesperson for the PRC Ministry of Foreign Affairs stated that a Japanese pharmaceutical executive had been detained on suspicion of violating the PRC Counterespionage Law. The PRC government's willingness to invoke the law in this instance illustrates the government's increasing propensity to use a legal framework to justify its authority to detain foreign citizens at will.

DATA SECURITY LAW (2021)

The Data Security Law requires data generated in China to be stored in China, and it subjects data exported overseas to strict rules. The PRC government also established data protection levels based on the extent to which unauthorized use or sharing of the data could harm national security (among other criteria). *Core data*, the most sensitive level, is defined as data that relates to:

- National security
- The "lifeblood of the national economy"
- "People's livelihoods"
- "Major public interests"

Important data, the second-most sensitive level, is defined based on industry- and topic-specific lists but can include commercial information, such as patents and trade secrets.

CASE STUDY: WIND INFORMATION ENFORCES DATA SECURITY LAW PROVISIONS

In September 2022, the Cyberspace Administration of China asked Wind Information Company, China's biggest financial data provider, to stop providing corporate registry information—such as company shareholder and ownership information—to overseas customers. Wind Information Company halted data exports to comply with this rule.

CYBERSECURITY LAW (2017)

The Cybersecurity Law supports the PRC's long-term effort to establish legal and regulatory control over its domestic internet and data. The law regulates the behavior of PRC internet service providers (ISPs), internet content providers (ICPs), and ordinary citizens. The law requires individuals and companies to "observe public order" and not to use the internet to "engage in activities endangering national security, national honor, and national interests."

CASE STUDY: MICRON TECHNOLOGIES

In 2023, the Cyberspace Administration of China announced that products from US-based Micron Technologies sold in China had "not passed a cybersecurity review" and posed "serious network security problems." Citing the Cybersecurity Law, the PRC government barred companies that handle "critical information infrastructure" from purchasing Micron products. The PRC may have been motivated by a desire to strike back at US export restrictions or to protect its domestic competitors. This example shows the PRC's willingness to use the law to promote China's control over critical technologies.

For additional information, please contact: *chinastudies@cna.org*

For additional CNA work on this topic, see: *https://www.cna.org/economic-statecraft*

December 2023

This work was created in the performance of Federal Government Contract No. N00014-22-D-7001.