China's New Counter-Espionage Law: National Security Rationale and Risks

Che-Chuan Lee
Research Fellow

Division of National Security Research
Keyword: CCP Politics

1. News Highlights

On April 26, 2023, the Standing Committee of the National People's Congress in China voted to pass the revised draft of the "Counter-Espionage Law", which will come into effect on July 1. The new version increased to 71 clauses, while the original had only 40.[1] Due to multiple suspected violations of the "National Security Law" and the "Counter-Espionage Law" that have occurred this year, combined with a significant increase in the new law and vague definitions concerning "espionage activities" and "national security and interests", this has caused concern and discussion from outside. In early May, consulting firm Capvision Partners was accused of being an "accomplice of overseas intelligence agencies"; on May 21, American memory chip giant Micron was accused by the Cyberspace Administration of China of posing "serious security risks" to critical information infrastructure supply chains, further raising concerns about China's government's intentions and related risks regarding national security control.[2]

1. "The Newly Revised Counter-Espionage Law will be Implemented from July 1," *Xinhua News Agency*, April 26, 2023, https://reurl.cc/YelMOD; "Counter-Espionage Law of the People's Republic of China," *Central People's Government of the People's Republic of China*, April 27, 2023, https://reurl.cc/eD50Ej.
2. Capvision has over 1000 clients, and its business is divided into three major categories. "Expert Interviews" account for 80% of its total business. The interviewed experts are mainly focused on areas of policy research, national defense and military industry, finance and currency, high technology, energy, and healthcare. See "'Alarm bell are ringing!' The National Security Agency Reveals that A Certain Company Has Become A Foreign Intelligence Agency Accomplice," *CCTV News*, May 9, 2023, https://reurl.cc/WDprRx; "Products Sold by Micron in China Have Not Passed Network Security Review," *China's National Internet Information Office*, May 21, 2023, https://reurl.cc/p6na9a.

2. Security Implications

The new version of the "Counter-Espionage Law" can be divided into four main chapters: security risk prevention, investigation and handling, protection and supervision, and legal liability, in addition to the general provisions and supplementary provisions. As this is an amendment based on the 2014 version of the "Counter-Espionage Law", its additions and revisions are worth exploring. By examining the differences between the old and new versions, we may gain insight into the purpose and reasoning behind Beijing's revision of the new law.

2-1. Simultaneous expansion of the patterns and enforcement powers of "espionage activities"

The 2014 version of "Counter-Espionage Law" regulations is quite ambiguous, leaving much room for interpretation and becoming a "powerful" enforcement tool for the Chinese authorities. In the 2014 version, there was no specific definition or specification of "spy activities"; it was only briefly mentioned as "(activities) endangering the national security of the People's Republic of China".[3] The new version of the "Counter-Espionage Law" presents six "espionage activities" types in Article 4.[4] However, after the fifth type of activity, the sixth type is classified as "other spy activities". The new law still does not define "national security" or "national interests" in China. Therefore, if individuals or any company or organization acquires "non-confidential information" about China's economy or politics, but Chinese authorities deem that this information involves national

3. The 2014 edition of "Counter-Espionage Law" only specifies in Article 6 that all acts of espionage that endanger the national security of the People's Republic of China carried out or instigated by foreign institutions, organizations, individuals, or funded by others, or in collusion with domestic institutions, organizations or individuals and foreign institutions, organizations, individuals, must be legally pursued.
4. The acts include activities that endanger the national security of the People's Republic of China; participating in spy organizations or accepting missions from spy organizations and their agents, or defecting to spy organizations and their agents; stealing, probing, bribing, illegally providing documents, information and other items related to national security and interests, or engaging in activities that incite, induce, intimidate, or bribe government workers to defect; targeting national agencies, confidential units, or critical information infrastructure for network attacks, intrusions, interference, control, destruction, etc.; directing enemy attacks on targets; conducting other espionage activities.

security or interests, they can still be regarded as "espionage activities" based on the arbitrary definition "other documents, data, information, and items related to national security and interests". Article 7 prohibits Chinese citizens from engaging in any behavior that endangers the country's security, honor, and interests; it also makes criticizing the Chinese government a potential illegal offense. The new law also adds "joining spy organizations and their agents" and "cyber attacks against national agencies, confidential units, or critical information infrastructure" as espionage activities.

In addition, although the old "Counter-Espionage Act" has already granted law enforcement personnel many powers, the new version further expands their jurisdiction. In the "Investigation and Disposition" chapter, the new law has added or expanded the administrative law enforcement powers such as summons, property information inquiry, the search of suspect's personal belongings, and prohibition of border entry and exit for suspects. From the perspective of China's law enforcement agencies, they may need such broad enforcement discretion to deal with various national security threats; however, the high degree of uncertainty resulting from these provisions not only deviated from the rule of law but will also lead to fear and mistrust among Chinese and foreign citizens and businesses.

2-2. Many foreign-owned enterprises in China have been searched

Recently, Beijing has prohibited access to key corporate information, including patents and annual reports of Chinese companies; moreover, a series of surprise inspections of foreign companies, especially due diligence firms, has raised concerns among the international community, particularly the business sector. In late March of this year, a US diligent investigation firm, the Mintz Group, stated that Chinese officials raided its Beijing office, and five Chinese employees were detained. In response, the Chinese Ministry of Foreign Affairs only stated that the Mintz Group was suspected of engaging in "illegal business activities".

On April 15, which is China's "National Security Education Day", an official report stated that a consulting firm in Shenzhen provided foreign organizations with information regarding labor in Xinjiang, which constitutes a violation of "Counter-Espionage Law"

and "poses risks and potential dangers to China's national security and interests". In late April, the Shanghai branch office of Bain & Company, headquartered in Boston, was searched by Chinese national security agents; the agents questioned its employees and confiscated their computers and cell phones. Astellas Pharma, a Japanese pharmaceutical company, has Hiroshi Nishiyama, a senior executive in Beijing, accused of engaging in espionage activities and was arrested.

On the evening of May 8, Jiangsu Radio and Television Station, China Central Television, and other Chinese official media outlets openly revealed that high-level Chinese law enforcement units had launched a joint operation against Capvision Partners consulting company, accusing it of being an "accomplice of overseas intelligence agencies" and providing consulting services of sensitive nature related to military affairs for overseas organizations, posing "significant risks" to China's national security.[5]

The Chinese government has recently taken a series of actions to strengthen restrictions on outpouring domestic information in addition to preventing the US from investigating internal conditions in China. Experts speculate that China's related actions may be due to the following reasons: 1. blaming the foreign manipulation of "zero COVID-19" protests at the end of last year; 2. avoiding the outflow of actual economic data to reduce the effectiveness of the US suppression toward China's economic strategy; 3. preventing reporters and scholars from using Chinese official data to investigate China's social truths and human rights violations. [6]

3. Trend Observation

Since taking office, Xi Jinping has placed a high priority on national security issues. In addition to emphasizing ideology and carrying out CCP and government system reforms (such as establishing a National Security Committee and proposing a national security strategy), since 2014, a series

5. See footnote 2.
6. James Palmer, "China's Latest Data Restrictions Could Scare Off Investors," *Foreign Policy*, May 2, 2023, https://reurl.cc/lv3db9.

of laws have been enacted and passed, including the "Counter-Espionage Law", (2014), "National Security Law" (2015), "Anti-Terrorism Law" (2015), "Law for the Management of Activities of Foreign Non-Governmental Organizations within China" (2016), "Cyber Security Law" (2016), "National Intelligence Law" (2017), "Nuclear Safety Law" (2017), "Cryptography Law" (2019), and "Data Security Law" (2021). The series of laws shows an obvious context that China is gradually strengthening the structure of its national security legal system.

3-1. The "holistic view of national security" for "securitization of everything"

Under the rule of Xi Jinping, almost everything can be attributed to the extent of national security. Many scholars believe that Xi's highly valued "holistic view of national security" not only emphasizes the need to consider potential security risks in all areas but also seeks to implement "securitization of everything" through policy, institutional, and regulatory construction to shape a society and country that is highly alert and capable of responding to risk threats.[7]

That means Xi's "holistic view of national security" is about every citizen and is also a concept that involves "the whole of society". Therefore, since the enactment of the "Counter-Espionage Law" in 2014, the Chinese government has been committed to conducting counter-espionage propaganda and urging the general public to "beware of foreign spies". Article 14 of the National Security Law, promulgated in July 2015, stipulates that April 15 of each year is designated "National Security Education Day". The National Security Bureau established the "12339" reporting hotline in the same year and offered lucrative rewards to encourage citizens to report espionage acts. On the eve of this year's National Security Education Day, Chinese officials revealed several national security crime cases to urge the public to enhance their awareness and be vigilant against acts that harm national security.

7. Nadya Yeh, "Should You be Frightened by China's Revision to the Anti-espionage Law?" *China Project*, May 2, 2023, https://reurl.cc/OVxjVv.

3-2. Sacrificing certain economic and trade benefits is necessary for countering US suppression

The new "Counter-Espionage Law" not only creates a shocking effect on Chinese people, foreigners, Taiwanese, journalists, scholars, and non-governmental organizations but will also significantly increase the operational risks of Chinese enterprises, foreign enterprises in China, and Taiwanese businesses. Consulting firms with a business nature involving market research and company operation data may become prime targets of Beijing authorities' supervision. On the evening of May 21, China's Internet Information Office announced that the products of Micron Technology, a US semiconductor giant, "have serious potential network security risks" that "pose significant security risks" to China's critical information infrastructure supply chain. The Office, therefore, did not pass Micron in the cybersecurity review and ordered that "Chinese operators of critical information infrastructure should stop purchasing Micron products". In response, the US Department of Commerce stated that China's restrictions on Micron are "groundless", and the department will contact China directly to seek a solution to lower the Chinese restrictions.[8]

At the end of April, the Standing Committee of the National People's Congress of China stated that the fight against espionage activities in China is "very serious". The recent search and shutdown of American corporate offices may be a retaliatory measure by the Chinese government in response to the US technology war. Amid intense competition with the US, China is concerned that American and Western powers are infiltrating Chinese society in an attempt to engineer a "color revolution" and gain sensitive information on Chinese companies and markets to exploit China's economy, technology, and society weaknesses to undermine the country further. To China, only stronger counter-espionage measures can "unhook" its economy, society, and industry from potential risks and threats; and only by making China "fully secured" can it withstand pressure and ultimately achieve victory in the competition against the US.

8. See footnote 2; Eric Martin and Iain Marlow, "US Expresses 'Serious Concerns' About China Move Against Micron," *Bloomberg*, May 23, 2023, https://reurl.cc/51k9Yn.

(Originally published in the 80th "National Defense and Security Biweekly", May 26, 2022, by the Institute for National Defense and Security Research.)

(The contents and views in the assessments are the personal opinions of the author, and do not represent the position of the Institute for National Defense and Security Research.)

Table: Cases of arrests and convictions in China in 2023 on suspicion of violating national security or espionage

Dates	Case	Charges
May 21	China's Internet Information Office announced that the products of Micron Technology, a US memory chip maker headquartered in Idaho, "have serious potential network security risks" and therefore did not pass Micron in the cybersecurity review and ordered that "Chinese operators of critical information infrastructure should stop purchasing Micron products".	Micron products "have serious potential network security risks" that "pose significant security risks" to China's critical information infrastructure supply chain.
May 8	The Shanghai, Beijing, Suzhou, and Shenzhen offices of consulting firm Capvision have been searched, and at least two consulting experts have been arrested.	Sending sensitive information overseas.
April 26	The Taiwan Affairs Office confirmed that "Fucha" (a.k.a. Li Yanhe), the editor-in-chief of Gūsa Publishing, was arrested by national security units in Shanghai in March and is currently under investigation.	The Taiwan Affairs Office alleges that he is suspected of engaging in activities that endanger national security.
April 25	The Supreme People's Procuratorate of China announced the conclusion of the investigation and conviction of Yang Chih-yuan, Vice Chairman of the Taiwan National Party, and approved the arrest on suspicion of "state secession". On August 3, 2022, Yang Chih-yuan was criminally detained by the National Security Bureau of Wenzhou, Zhejiang Province, for his long-term involvement in "Taiwan independence separatist activities" and alleged endangerment of national security.	Charged with the crime of "state secession".

Dates	Case	Charges
Mid-April	The Shanghai office of Bain & Company, a US management consulting firm, was searched multiple times by Chinese police. The police confiscated computers and cell phones and interrogated several employees.	Official explanation not provided.
April 10	Xu Zhiyong, a Chinese political dissident and founder of the "New Citizens Movement", and rights-protecting lawyer Ding Jiaxi were sentenced by the Intermediate People's Court in Linshu County, Shandong Province. Xu was given a 14-year sentence and deprived of civil rights for eight years, while Ding received a 12-year sentence and was deprived of civil rights for three years.	Suspected of subverting the government.
March 20	US due diligence firm Mintz Group was searched, five Chinese employees were detained, with its Beijing office was forced to close.	The Chinese Ministry of Foreign Affairs claims that the company is suspected of operating illegally. Reuters reveals the possible connection between the company's research and the forced labor in Xinjiang.
March 19	Japanese pharmaceutical company Astellas Pharma was searched, and Hiroshi Nishiyama, a senior executive stationed in China, was arrested in Beijing.	The Chinese Ministry of Foreign Affairs identified that Nishiyama is suspected of engaging in espionage activities.
February 21	Dong Yuyu, deputy director of the Comment Department and columnist for the CCP's "Guangming Daily", was arrested while having lunch with a Japanese diplomat at the Novotel-Xinqiao Hotel in Beijing.	Accused of espionage.

Source: Compiled by Che-Chuan Lee based on public information.