Morgan Lewis | Report

CHINA'S NEW 'ANTI-ESPIONAGE LAW' RAISES COMPLEX COMPLIANCE ISSUES FOR MULTINATIONAL CORPORATIONS

May 2023

www.morganlewis.com

CHINA'S NEW 'ANTI-ESPIONAGE LAW' RAISES COMPLEX COMPLIANCE ISSUES FOR MULTINATIONAL CORPORATIONS

The Second Session of the Standing Committee of the 14th National People's Congress voted and passed on April 26, 2023 the newly revised "Anti-Espionage Law of the People's Republic of China" (the New Anti-Espionage Law). The New Anti-Espionage Law, which will take effect on July 1, 2023, expands the scope of espionage activities, establishes broad criteria for determining espionage behavior, grants extensive investigative power to national security agencies, and clarifies the legal liability for espionage activities.

Against the backdrop of increasingly tense China-US relations and a growing number of cases involving suspected espionage activities, multinational enterprises outside China (foreign enterprises) should pay particular attention to related compliance risks.

EXPANDED SCOPE OF 'ESPIONAGE ACTIVITIES'

The New Anti-Espionage Law adds "joining espionage organizations and their agents" as a category of espionage activities. Furthermore, in terms of critical information infrastructure, the New Anti-Espionage Law stipulates that "espionage organizations and their agents carry[ing] out or instruct[ing], fund[ing] others to carry out, or domestic and foreign institutions, organizations, and individuals collud[ing] to carry out cyber-attacks, intrusions, interference, control, and destruction activities against state organs, sensitive units, or critical information infrastructure" also constitute espionage activities.

In terms of objects involved in espionage activities, the New Anti-Espionage Law adds "intelligence and other documents, data, materials, and items related to national security and interests" beyond the existing "state secrets." As for possible methods used to promote national officials' defection, the New Anti-Espionage Law adds "coercion" as a method along with "inciting, enticing," and "bribing."

Regarding the applicable scope, the New Anti-Espionage Law explicitly states that it applies to "espionage organizations and their agents engaging in espionage activities against a third country within the territory of the People's Republic of China, or using Chinese citizens, organizations, or other conditions, which endanger the national security of the People's Republic of China," which has extraterritorial jurisdiction.

Under the New Anti-Espionage Law's expanded scope of "espionage activities," there may be cases of broad interpretation in practice, bringing unexpected risk to the normal operation of foreign enterprises. Consider the following possible real-life examples:

- **Trade secret leakage.** A foreign enterprise hires a technical expert from a domestic company who had access to a key technology before leaving their previous employer. When the technical expert begins working for the foreign enterprise, they apply the technology to the new company's products. Although the technology is not a state secret, it is still closely related to national security and interests. In this case, the technical expert may be considered as engaging in espionage activities, and the foreign enterprise may also be subject to investigation and punishment.
- **Data sharing in collaborative projects.** A foreign enterprise cooperates with a domestic enterprise on a project involving critical information infrastructure. During the project collaboration, both parties have to share some data related to national security and interests. If there is a risk of data leakage during that sharing process, even if not intentionally leaked, the

foreign enterprise may still be considered as participating in espionage activity, thus facing investigation and punishment.

- **Market research conducted abroad.** A foreign enterprise's overseas subsidiary conducts market research to enter the Chinese market and collects a large amount of information about domestic industry competitors, some of which may involve data related to national security and interests. Although the purpose of the foreign enterprise's investigation is business competition, if the overseas subsidiary is considered an espionage organization agent, its behavior may be deemed as espionage activity, posing legal risks to the parent company.
- **Aggressive solicitation in talent recruitment.** During the hiring process, a foreign company might use aggressive solicitation strategies to lure talent away from domestic businesses, encouraging them to leave their current jobs and join the foreign company instead. If the candidates' previous employers are connected to national security and interests, certain aggressive recruitment strategies could be seen as espionage activities, which could lead to legal risks for the foreign enterprise.
- **Hiring former government personnel.** Foreign enterprises may hire former government personnel as consultants or executives during their expansion in the Chinese market, leveraging their experience and connections in specific industries or policies. Under the New Anti-Espionage Law, if hiring former government personnel is regarded as "inciting, enticing, coercing, or bribing state personnel to defect," it may constitute espionage activity.
- **Collecting business intelligence.** In business competition, foreign enterprises may collect competitor information to understand market dynamics and optimize their strategy. However, under the broad definition of "espionage activities" under the New Anti-Espionage Law, if the collected information is deemed to involve documents, data, materials, and items related to national security and interests, such business intelligence collection activities could be interpreted as espionage activities.
- **Cross-border collaborative projects.** Foreign enterprises may be involved in technology transfer and information sharing when collaborating with Chinese enterprises on projects. If the technology or information involved in the collaboration is deemed to relate to national security and interests, even if both parties are acting within the scope of normal business cooperation, such collaboration may be considered espionage activity.
- **Data centers and cloud services.** When providing data centers and cloud services in China, foreign enterprises may be involved in storing, processing, and transmitting a large amount of user data. If some data is deemed to relate to national security and interests, the enterprise's means for data management may be considered espionage activity.

In these scenarios, foreign enterprises may face unexpected risks due to the expanded interpretation of "espionage activities." Therefore, foreign enterprises should strengthen their compliance awareness, ensure that all business activities comply with the requirements of the New Anti-Espionage Law, and reduce potential legal risk.

DETERMINATION OF ESPIONAGE ORGANIZATIONS AND THEIR AGENTS

According to the interpretation of the Legal Affairs Commission of the National People's Congress:

> A[n] "espionage organization" refers to an organization established by a foreign government or hostile forces abroad that aims to collect China's state secrets or intelligence in politics, economy, military, etc., or engage in activities such as subversion

> and destruction that endanger China's national security and interests, such as the US Central Intelligence Agency and Japan's Defense Intelligence Headquarters.
>
> A[n] "espionage organization agent" refers to a person who, at the instigation, commission, or funding of a[n] espionage organization or its members, carries out or instructs, entrusts, or funds others to engage in activities that endanger China's national security.

Article 4(1)(3) of the New Anti-Espionage Law lays out that activities carried out by foreign institutions, organizations, or individuals other than espionage organizations and their agents, or activities carried out by domestic institutions, organizations, or individuals in collusion with them, including stealing, spying, bribing, or illegally providing state secrets, intelligence, and other documents, data, materials, and items related to national security and interests, or inciting, enticing, coercing, or bribing state personnel to defect, are considered espionage activities. In other words, when multinational corporations are deemed to be facilitating espionage organizations and their agents in conducting intelligence-gathering operations, these corporations would be deemed as engaging in espionage activities themselves and thereby contravening the provisions of the New Anti-Espionage Law.

The provision covers a wide range of subjects, including foreign institutions or organizations other than espionage organizations, and a wide range of objects, including other documents related to national security and interests.

Under the New Anti-Espionage Law, the broad criteria for identifying espionage organization agents could expose foreign enterprises to unforeseen risks in the ordinary course of business. Possible scenarios include the following:

- **Partner risks.** When a foreign enterprise collaborates with other companies or individuals, if the partner is identified as an agent of an espionage organization, the foreign enterprise may also be indirectly implicated in espionage activities and face legal risks.
- **Information security compliance.** Foreign enterprises may cooperate with overseas service providers in areas such as cybersecurity and data protection. If the service provider is identified as an espionage organization agent, the information exchange and technical cooperation during the collaboration could be considered espionage activities.
- **Risks in business activities.** Foreign enterprises seeking market opportunities may participate in overseas business associations and industry events. Under the New Anti-Espionage Law, if these organizations are identified as agents of espionage organizations, the foreign enterprises' communication and collaboration with them could be considered espionage activities.
- **Academic research and exchanges.** Foreign enterprises may collaborate with overseas universities and research institutions for academic research and technology development. If these universities or research institutions are identified as espionage organization agents, the information sharing and technical exchanges during the collaboration could be viewed as espionage activities.
- **Cross-border employee hiring risks.** When hiring employees cross-border, foreign enterprises may involve sensitive areas such as intellectual property and technology transfers. If these employees are identified as espionage organization agents, their activities within the company could be considered espionage activities.

In these scenarios, foreign enterprises may face unexpected risks due to the broad criteria for identifying espionage organization agents. To avoid these risks, foreign enterprises should strengthen their compliance awareness, ensure that all business activities comply with the New Anti-Espionage Law, and enhance their review of third parties such as business partners and suppliers to ensure their compliance.

At the same time, companies should establish sound internal risk-prevention mechanisms, strengthen employee training and education, and ensure that employees clearly understand the relevant legal and regulatory requirements.

INVESTIGATIVE AND HANDLING POWER OF NATIONAL SECURITY AGENCIES

The New Anti-Espionage Law grants unprecedented investigative powers to national security agencies.

According to the New Anti-Espionage Law, when national security agency staff carry out anti-espionage tasks in accordance with the law, they need only present their work credentials to "question" relevant individuals and organizations about the situation. And for individuals with "unidentified identity and suspected of espionage activities," national security agency staff can "inspect" their belongings.

Further, under the New Anti-Espionage Law, when national security agency staff carry out anti-espionage tasks in accordance with the law and with the approval of the head of the national security agency at the districted city level or above, after presenting their work credentials, the national security agency staff can examine electronic devices, facilities, relevant procedures, and tools of related individuals and organizations and can also access, collect, and review relevant documents, data, materials, and items.

The New Anti-Espionage Law explicitly states that relevant individuals and organizations must cooperate. In certain cases, national security agency staff may even seize and detain relevant electronic devices, facilities, and related procedures and tools.

Since the New Anti-Espionage Law does not clearly define the criteria for "unidentified individuals with suspected espionage activities," and national security agency staff only need the approval of national security agency at the districted city level or above (i.e., the national security agency can approve its own examination actions), national security agencies and their staff essentially have unparalleled investigative power.

This expanded authority given to national security agencies under the New Anti-Espionage Law has significant implications for multinational companies operating in China. These companies may face increased scrutiny and potential investigations by national security agencies, even in situations where there is no clear evidence of espionage activities. Furthermore, the vague criteria for identifying "unidentified individuals with suspected espionage activities" may result in a higher degree of uncertainty for businesses.

OTHER STRENGTHENED REQUIREMENTS

In addition to the above content, the New Anti-Espionage Law has also strengthened security measures against espionage attacks in many aspects.

Construction Project Restrictions

Any new, renovated, or expanded construction projects within the security control zones around important state organs, defense industry units, and other significant units involving state secrets and military facilities must obtain permission from the national security agency for any national security–related matters.

Immigration Restrictions

According to the New Anti-Espionage Law:

- For Chinese citizens who may pose a risk to national security or cause significant harm to national interests after leaving the country, the national security department of the State Council can decide to restrict their departure for a certain period and notify the immigration authorities.
- For individuals suspected of espionage activities, provincial-level or higher national security agencies can notify immigration authorities to deny their exit from the country.
- For foreign nationals who may engage in activities harmful to the national security of the People's Republic of China after entering the country, the national security department of the State Council can notify immigration authorities to deny their entry.

Cybersecurity Protection

In compliance with the New Anti-Espionage Law, when national security agencies discover cybersecurity risks related to espionage activities, such as harmful online content or cyberattacks, they should notify relevant departments according to the responsibilities stipulated in the Cybersecurity Law of the People's Republic of China.

These departments must then legally handle the situation or instruct telecommunications operators and internet service providers to promptly take measures such as patching vulnerabilities, strengthening network defenses, stopping transmission, eliminating programs and content, suspending related services, removing related applications, and shutting down related websites. The telecommunications operators and internet service providers should also preserve relevant records.

In urgent situations wherein not taking immediate action could cause severe harm to national security, national security agencies can order relevant units to fix vulnerabilities, stop related transmissions, and suspend related services while they are notifying the relevant departments.

It is crucial that multinational companies be aware of these strengthened requirements and adjust their operations accordingly to ensure compliance with the new law. This may involve obtaining necessary permits for construction projects, adhering to immigration restrictions, and enhancing cybersecurity measures.

LEGAL RESPONSIBILITIES FOR ESPIONAGE ACTIVITIES

The New Anti-Espionage Law specifies the types of responsibilities more clearly and stipulates corresponding responsibilities for both individuals and organizations.

Personal Responsibility for Espionage Activities

If an individual engages in espionage activities or assists others in doing so, and it does not constitute a crime, the national security agency shall issue a warning or impose administrative detention for up to 15 days. The individual may also be fined up to five times the amount of their illegal income, but not exceeding 50,000 renminbi (approximately $7,233).

Organizational Responsibility for Espionage Activities

If an organization engages in espionage activities or assists others in doing so, the national security agency shall issue a warning and may impose a fine of up to five times the amount of their illegal income, but not exceeding 500,000 renminbi (approximately $72,333).

In addition, based on the severity and consequences of the violation, the national security agency may recommend that relevant authorities order the cessation of related business or services, suspend

production or business, revoke relevant licenses, or cancel registration. The individual in charge of the organization shall bear corresponding personal responsibility.

Responsibility for Violating Construction Project Regulations

The national security agency may order corrections, issue warnings, or impose penalties on entities that violate regulations for new, renovated, or expanded construction projects. If the related entities refuse to correct their actions or the situation is severe, the national security agency can order the cessation of construction or use, or even temporarily withhold or revoke their permits. Furthermore, the national security agency may also recommend that relevant authorities take legal action against the violating entities.

Criminal Responsibility for Espionage Activities

If espionage activities constitute a crime, the perpetrators shall bear corresponding criminal responsibility according to the Criminal Law of the People's Republic of China. Relevant crimes related to espionage activities include, but are not limited to, espionage, theft, spying, bribery, illegal provision of state secrets or intelligence to foreign entities, subversion of state power, and funding activities that endanger national security. The minimum penalty is imprisonment for a minimum of three years. In cases where the harm to China's national interests and people is particularly severe and the circumstances are particularly egregious, the death penalty may even be imposed.

PRACTICAL IMPLICATIONS FOR MULTINATIONAL COMPANIES WITH OPERATIONS IN CHINA

In light of the expanded scope of espionage activities and definition of espionage organizations and their agents under the New Anti-Espionage Law, multinational corporations with operations in China should consider the following recommendations to ensure compliance and protect their local employees, especially expatriates.

Review and Update Internal Policies

Examine existing internal policies and procedures to ensure that they address the expanded scope of espionage activities and definition of espionage organizations and their agents under the new law. Make necessary revisions to explicitly outline the prohibition of seeking, obtaining, or storing sensitive information related to state secrets or intelligence.

Develop Clear Reporting Protocols

Establish a well-defined process for employees and vendors to report incidents where they inadvertently come across sensitive information as well as any suspicious activities that could be considered espionage. This process should include escalation procedures and designated points of contact within the organization for handling such reports. Establish reporting policies and procedures to avoid the spread of sensitive information during the reporting process.

Strengthen Due Diligence Processes

Review existing due diligence processes for employee recruitment, vendor selection, and business partnerships. Enhance background checks to identify potential connections with espionage organizations or their agents and ensure that employees and vendors are aware of their legal responsibilities.

Enhance Data Classification and Management

Develop a more comprehensive data classification system that clearly distinguishes between sensitive and non-sensitive information. Implement data management procedures that limit access to sensitive information and provide guidelines for securely handling, storing, and disposing of such data.

Conduct Regular Compliance Audits

Schedule periodic internal compliance audits to assess adherence to the updated policies and procedures. Identify potential risks and gaps in the compliance system and take corrective actions as needed. In addition, exercise caution in accepting and handling sensitive information. If specific information is believed to involve Chinese state secrets or intelligence or pertain to industries of particular interest to the Chinese government, such as military information, human genetic resources, or advanced technical data, it is advisable to avoid processing such data to the extent possible, or to segregate the relevant sensitive data. Subsequently, engage the services of a qualified professional to manage the data and determine whether it is necessary to report the matter to local authorities.

Expand Employee Training Programs

Update employee training programs to include information on the New Anti-Espionage Law, such as the expanded scope of espionage activities, the definition of espionage organizations and their agents, and the legal consequences of noncompliance. Provide case studies or practical examples to help employees understand the risks and consequences.

Develop a Crisis Management Plan

Create a crisis management plan that outlines the steps to be taken following an incident related to the New Anti-Espionage Law. The plan should include communication protocols, legal and public relations support, and guidelines for cooperating with local authorities.

Prepare for Dawn Raids

Develop a detailed plan to respond effectively to unannounced inspections or dawn raids by authorities in relation to the New Anti-Espionage Law:

- Designate a response team that includes legal counsel, senior management, and public relations personnel.
- Provide training to employees on how to respond to a dawn raid, including their rights and responsibilities during the raid, preserving company documents and electronic data, and communicating with the authorities.
- Establish a clear communication protocol to inform the response team and relevant stakeholders, such as senior management and legal counsel, in the event of a dawn raid.
- Prepare a designated meeting room for authorities to conduct their investigation, ensuring it is free from confidential information and electronic devices.
- Regularly review and update the dawn raid plan to ensure its effectiveness.

Address Risks for Expatriates Traveling to and from China

- Provide pretravel briefings to expatriates that cover potential risks associated with the New Anti-Espionage Law, including travel restrictions, customs checks, and interrogations by authorities.
- Establish protocols for the secure transfer of sensitive information across borders. Encourage employees to avoid carrying sensitive documents, data, or electronic devices when traveling.

- Create a 24/7 emergency contact for expatriates to report incidents or seek assistance during their travel. This contact should be able to provide immediate legal and logistical support.
- Monitor changes in the political and regulatory landscape in China and update expatriates on any new risks or requirements related to the New Anti-Espionage Law.
- Encourage expatriates to maintain a low profile during their stay in China, avoid discussions on sensitive topics, and limit contact with individuals or organizations that may be connected to espionage activities.

CONTACTS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:

Author
Todd Liao +86.21.8022.8799 todd.liao@morganlewis.com

Beijing/Shanghai
Todd Liao +86.21.8022.8799 todd.liao@morganlewis.com
Sylvia Hu +86.21.8022.8527 sylvia.hu@morganlewis.com
K. Lesli Ligorner +86.21.8022.8777 lesli.ligorner@morganlewis.com

Hong Kong
Charles Mo +852.3551.8558 charles.mo@morganlewis.com

London
Pulina Whitaker +44.20.3201.5550 pulina.whitaker@morganlewis.com

Philadelphia
Gregory T. Parks +1.215.963.5170 gregory.parks@morganlewis.com
Ezra D. Church +1.215.963.5710 ezra.church@morganlewis.com
Kristin M. Hadgis +1.215.963.5563 kristin.hadgis@morganlewis.com

San Francisco
W. Reece Hirsch +1.415.442.1422 reece.hirsch@morganlewis.com

Silicon Valley
Mark L. Krotoski +1.650.843.7212 mark.krotoski@morganlewis.com

Tokyo
Mitsuyoshi Saito +81.3.4578.2668 mitsu.saito@morganlewis.com

ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.