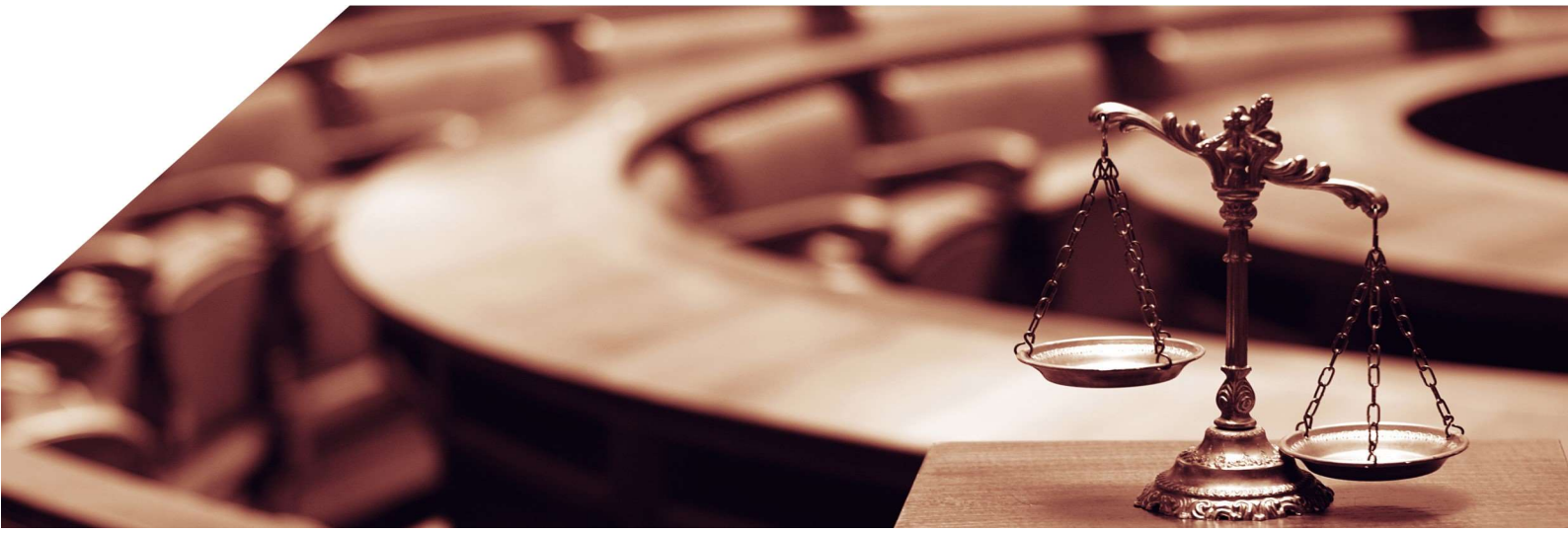
ALLEN & OVERY | 朗悦
LANG YUE | 安理国际律师事务所



The Revised PRC Counter-Espionage Law – What Has Really Changed?

June 5, 2023

On April 26, 2023, China's legislature approved revisions to the Counter-Espionage Law of the People's Republic of China (**PRC Counter-Espionage Law**). A draft version of the law had been released for public comment in December 2022. This alert highlights the significant changes to the law.

The law redesign can be viewed as an aspect of the current administration's focus on national security and concerns over the flow of data across China's borders. China has indicated an emphasis on building a more comprehensive legal system for national security with perhaps broader ramifications for legal reform and efforts at greater transparency in national security legal developments. In terms of the legislative history of the revisions to the PRC Counter-Espionage Law, legislative planning for revisions to the law were disclosed in China's 2022 version of the Legislative Work Plan of the Standing Committee of the National People's Congress (**NPCSC Legislative Plan**) (approved in December 2021 and publicly released in or about May 2022). The proposal for revising the law appeared in section 3 of the plan as a preparatory legislative item. Proposed revisions to the law were not suggested in either the 2021 or the 2020 NPCSC Legislative Plans, but that is not particularly unusual in legislative planning in China.

Official commentary suggest that at some point in 2021/2022, revisions to this law became a Central Government policy and legislative priority and the first draft of the revision was publicly released in December 2022.[1] In the 2023 NPCSC Legislative Plan (approved in December 2022, amended in April 2023, and released in or about May 2023), revisions to the PRC Counter-Espionage Law were slotted for further reading by the legislators in April 2023. The revised law was adopted and promulgated on April 26.

The revised law is set to become effective on July 1, 2023. The law:

- Brings under one heading various disparate counter-espionage rules that have been enacted since the first counter-espionage law in 2014.
- Provides express penalties, including fines and cancellation of business licenses, for foreign-invested and other domestic companies engaged in non-criminal espionage.
- Expands the scope of espionage activities to include cyber-intrusion.
- Cautions that the provision to parties abroad of unmarked items that concern national security or interests in various forms is illegal.
- Provides more detail on the investigative powers of state security organs, but with additional balancing language to suggest some legal restraints on those powers.

For a deeper dive into the weeds on the changes to the new law, please see below.

Criminal and Non-Criminal Espionage

There is now an express general charging provision set out in Article 10 of the revised law. Legal liability ensues for (a) foreigners engaging in "espionage activities" that harm the national security of China or (b) to those domestic organizations or individuals who collude with foreigners and engage in espionage activities that harm the national security of China. The term "espionage activities" (间谍行为, in Chinese) is defined in the law and will be discussed in the *Activities Constituting Espionage* section below.

Perhaps most significant from the perspective of foreign-invested businesses operating in China are the clarifications to the law's liability provisions. The liability provisions *now expressly recognize administrative liability for an espionage offence that does not constitute a crime*. In other words, there is now a clear legislative basis for administrative penalties (fines, cancellation of business, detentions, etc.) for "non-criminal" espionage.

The original PRC Counter-Espionage Law (2014) set out administrative liabilities for certain acts pertaining to espionage investigations, but arguably not for espionage itself, which created certain headaches in practice. For example, under the earlier version of the law, administrative penalties could be assessed for obstructing an espionage investigation, but other situations that could result in administrative sanction were not detailed. The 2014 version of the law suggested there might be administrative penalties by implying in Article 27 that there could be espionage which did not constitute a crime, but there was no clear guidance. *The 2017 Detailed Implementation Rules for the Counter-Espionage Law* (**Implementing Rules**) (a regulation promulgated by the State Council rather than the legislature) indicated that relevant departments could take "disciplinary actions" (处分) or the state security organs may give "warnings," but there was no further guidance as to what such might

[1] Offfical commentary suggests the process for the revisions may have begun as early as 2021 when the Supervisory and Judicial Affairs Committee of the National People's Congress (NPC) conducted a special inquiry regarding the implementation of the Counter-Espionage Law, and suggested to include the revision of the Counter-Espionage Law in the legislative work plan of the NPC Standing Committee for 2022. From December 2021 until January 2022, the Supervisory and Judicial Affairs Committee of the NPC, together with seven other departments, formed a working group responsible for drafting, and solicited opinions and suggestions from other government departments, localities, and experts and scholars, forming the Draft Revision of the Counter-Espionage Law of the People's Republic of China. See "The Notes on the Draft Revision of the Counter-Espionage Law of the People's Republic of China", delivered by Mr. WU Yuliang (Chairperson of the Supervisory and Judicial Affairs Committee) in the 36th session of the NPC Standing Committee on August 30, 2022.

mean in practice and the legal basis was uncertain. Differences in terminology can be significant from the perspective of PRC sources of law. Under China's hierarchy of sources of law only those sources that have been promulgated as "laws" (法律, in Chinese) by China's legislature can provide for administrative punitive measures that restrict one's freedom, such as detentions.[2]

By contrast, under the 2023 revisions to the PRC Counter-Espionage Law, the state security organs are expressly authorized to impose administrative detentions of up to 15 days and fines for non-criminal acts of espionage. The newly added Article 54 also unequivocally empowers the state security organs to propose additional administrative measures to be taken by other government departments, including suspension of business, and revocation of licenses or company registration. The relevant departments receiving such "proposals" are required to report to the state security organs in respect of the measures taken.

There is thus now a clear legal basis for administrative liabilities that may arise from an act of espionage. Of course, one would expect some differences between administrative actions and criminal charges, but an immediate question is the standard of proof. The PRC Criminal Procedure Law has established a "beyond-reasonable-doubt" principle, applicable to crimes of espionage; by contrast this is not addressed in the context of administrative law.

It will take some time to see how the state security organs might wield these newly clarified administrative powers in reality, and also how other departments might interact with the state security organs in respect of the proposed additional measures like suspending business or revoking licenses.

[2] See Article 10, the PRC Administrative Punishment Law.

Activities Constituting Espionage

There has been much discussion concerning the revisions to the scope of activities which may constitute "espionage activities" under Article 4 of the PRC Counter-Espionage Law. However, in our view, at least so far as concerns those activities that relate to penalties for criminal espionage, the scope has not changed very significantly from current law (with the exception of the cyber-intrusion provision in Article 4(4), discussed briefly below).

The provision that has been getting a fair amount of attention is Article 4(3). Under the 2014 law, "espionage activities" included *stealing, prying into, purchasing or illegally providing state secrets or intelligence* by an individual or organization separately or in collusion with a foreign organization or individual. This language has now been changed to include "other documents, data, materials, or articles related to national security or interests" *in addition* to state secrets and intelligence, and some observers see the revision as significantly broadening activities that may be deemed espionage activities. The revised Article 4(3) now provides, in relevant part (the new language is bolded):

> *… activities of stealing, prying into, buying or illegally providing state secrets, intelligence or* ***other documents, data, materials or articles relating to national security or interests****…;*

But does the change to the language really signal a significant change from current law? Arguably, at least as such may relate to criminal espionage, the inclusion of the new language had already been captured by a Supreme People's Court interpretation from 2001 and consequently the new language may not change things very much. Put another way, under current law, the provision of documents, data, materials, or items that may relate to national security or interests can already be penalized under existing provisions of the criminal law as interpreted by the Supreme People's Court (**SPC**).

Criminal Espionage and the 2001 SPC Judicial Interpretation of Article 111 of the PRC Criminal Law

The relevant charging provision for criminal espionage is Article 111 of the PRC Criminal Law. Article 111 prohibits the provision of PRC state secrets or intelligence to individuals or organizations outside of China:

> *Article 111: Whoever steals, spies into, buys or* ***unlawfully supplies state secrets or intelligence*** *for an organ, organization or individual outside the territory of China shall be sentenced to fixed-term imprisonment of ...*

A judicial interpretation promulgated by the SPC in 2001 defines what may be afforded protection similar to "state secrets" for purposes of Article 111 of the PRC Criminal Law. Article 5 of the SPC's Judicial Interpretation (Fa Shi [2001] No. 4) (**2001 SPC Interpretation**) provides in relevant part:

> *A perpetrator who knows or should know that an item without a classification marking concerns national security or interests and who for overseas [interests] steals the item, obtains it by spying or bribery, or illegally provides it, shall be punished … under Article 111 of the PRC Criminal Law.*

In other words, a person may be held criminally liable for illegally providing state secrets if he or she "*knows*" or "*should have known*" that an unmarked item (e.g., one that had not been red stamped with a formal classification designation) related to PRC national security or interests.

National Security / National Interests – A Question of Definitions?

"National security" is defined under Article 2 of the PRC National Security Law (2015) as "the state of a nation's political power, its sovereignty, unity and territorial integrity; the welfare of its people; of having sustainable economic and social development; of having the other major interests of a nation relatively safe from internal and external threats as well as its ability to ensure and maintain a state of security."

The term "national interest" is not clearly defined under the law, but an unofficial definition that has been getting some play in academic circles in Mainland China provides: "'National interests' refers to the collective sum of a sovereign state's development needs in the international community. Each country has three basic existential needs: 1. Ensuring its survival, including protecting its territorial integrity and the lives of its citizens; 2. Promoting the happiness and economic welfare of its people; and 3. Maintaining self-determination and the autonomy of its society and system of government."

There are a couple of additional concepts worth considering as to the kinds of items the provision of which overseas can lead to criminal liability for espionage.

The general definition for "state secret" is set out in Article 2 of the Law of the PRC on Guarding State Secrets as "items which concern national security and interests and which have been confirmed in accordance with statutory procedures and for which access is vested in a limited scope of persons during a period of time." State secrets are those that have been expressly marked as "Top Secret" (绝密), "Secret" (机密) or Government "Confidential" (秘密) under the Law of the PRC on Guarding State Secrets and its implementing regulations. However, items that have not been expressly marked may also be treated as state secrets under the criminal law if the actor who provides the suspect item does so knowing (or who should know) that the item in question concerns national security or the national interests (Article 5, 2001 SPC Interpretation).

The PRC National Intelligence Law (2018) does not provide a general definition of what constitutes "intelligence," but the focus of that law is on PRC efforts to collect intelligence, not on protecting against the collection of intelligence in the PRC.

However, 2001 SPC Interpretation does provide a working definition of "intelligence." Article 1(2) defines "intelligence" (情报) as "those items which relate to national security or the national interests which have not yet been made public or which should not be made public in accordance with relevant provisions." Arguably, depending on the content, a document that had been marked "内部参考," (for "internal distribution," in English)—a fairly common marking on official PRC government documents—might constitute "intelligence" for purposes of this definition.

So what are the sort of items relating to national security or interests contained in documents or data not expressly marked, but the provision of which overseas might result in criminal penalties based on prior cases anecdotally reported? Here's a non-exclusive list:

- Location of oil fields in China (Xue Feng matter circa 2007)
- Document 9, an internal CPC policy document (Gao Yu matter circa 2015)
- State official participates in government meetings, takes notes of speech, and uploads notes on the internet (from J. Fang and J. Fei, "Chinese "state secrets" demystified," China Law & Practice, posted January 18, 2016)
- Local AIC official uploads internal document onto AIC's public website (Id.)
- Eight individuals from the National Bureau of Statistics and People's Bank of China prosecuted for leaking macro-economic data before PRC government official's official announcement (Id.)
- Process for promoting or recruiting certain individuals as government employees (Id.)
- Photos taken publicly of military aircraft uploaded online (Id.)
- Former state officials discloses information on government pricing (Id.)
- Power project bidding information (Id.)
- SOE trade secrets, including product profit margins, product gross product, product costs (CCTV-13 Special Report on Counter-Espionage, May 2023)
- Classified information relating to aerospace research (Cases unveiled on the 8th National Security Education Day, April 15 2023)
- Running an offshore "immigration service company" that coerced and enticed their "clients" to fabricate evidence of persecution in China and apply for political asylum abroad (Id.)
- Collecting and providing documents from local Party and government institutions, including five identified as intelligence (Id.)
- Publishing posts in foreign social media sites deemed to defame China's national image (Id.)
- Undertaking investigation projects in relation to alleged labor practices in Xinjiang (Id.)
- Monitoring China's air military operational zones and providing sensitive data such as tides and currents in non-open sea areas (Id.)

Given this judicial interpretation, even before the revisions to the PRC Counter-Espionage Law, both expressly marked items as well as unmarked items could be found to be punishable as state secrets. The standard for this is whether the person providing the information/document knew or should have known that the information related to national security or interests. The new language contained in Article 4(3) addresses the provision of documents, data, information or materials which, although they may not have been specifically marked as being classified, are still to be treated as classified from the perspective of the 2001 SPC Interpretation. Under Article 5 of the 2001 SPC Interpretation, such unmarked documents could still be afforded protection similar to those for state secrets (and thus their provision could amount to a violation of Article 111 of the PRC Criminal Law) if they related to national security and the proper level of intentionality was reached. For an intentional *mens rea* (criminal culpability), there would need to have been actual knowledge that the documents related to national security or the national interests or the party providing the information should have known the document related to national security or the national interests. So from the perspective of criminal espionage, the new language regarding "documents and data" arguably has not really changed those sorts of activities which could be punished under Article 111 of the PRC Criminal Law.

For a state of mind less than intentional and thus penalized with an administrative sanction, perhaps something more like negligence would be required, but the PRC Counter-Espionage Law does not expressly provide the standard for administrative sanction. As such, how the new provision will be implemented in practice, and whether the provision overseas of certain documents, data, materials, etc. relating to national security could also lead to an administrative sanction for non-criminal espionage in the right circumstances and state of intentionality, remains to be seen.

Cyber-intrusion – Article 4(4)

In addition to Article 4(3), Article 4(4) is a new subsection manifesting the importance of cybersecurity in the context of espionage law. The subsection has undergone a substantial change compared to the earlier draft for comments (in December 2022). Whereas the earlier draft contained narrower language that only concerns "*disclosing security loopholes of critical information infrastructure*", the enacted Article 4(4) now addresses cyberattacks on "*state organs, units involved with secrets, or critical information infrastructure.*" Consequently, the state security authorities may now prosecute cyberattacks on a range of entities with espionage charges.

Investigative Powers of the State Security Organs More Specifically Expressed

The revised PRC Counter-Espionage Law has an updated chapter detailing the powers of the state security organs in investigating espionage.

Most of these powers had been provided in the original PRC Counter-Espionage Law (2014) and/or the accompanying Implementing Rules, such as accessing electronic devices, etc. The revisions largely reiterate these powers, with some fine-tunings, such as the express language authorizing "inquiries into the relevant property information of persons suspected of acts of espionage" (Article 29).

The provisions concerning exit restrictions (which some have labelled "exit bans") contained in Article 33 do not look particularly new in our view, at least from the perspective of criminal investigations of espionage acts. The Implementing Rules in place already provided an exit restriction mechanism for personnel (人员, in Chinese) suspected of criminal espionage. And more broadly, under the existing PRC Exit and Entry Law of 2013 (Article 28(1)), foreigners who have been named as a suspect of crimes may be refused exit from PRC borders.

Notably the revisions contain some expanded balancing language, which is meant to circumscribe the investigative powers of the state security organs. Multiple provisions now imply a principle of necessity and relevance. For example, Article 26 provides that accessing the relevant information "*must not exceed the scope and extent necessary to carry out tasks of counter-espionage efforts*." Article 27 caps the time for questioning an alleged perpetrator to eight hours, or twenty-four hours for a detainable/criminally prosecutable perpetrator; it also requires the state security authorities to notify the perpetrator's family in a timely manner. How these provisions will be implemented in practice is an open question, particularly in investigations for non-criminal espionage or for activities which might not be viewed as espionage if they were to take place in other jurisdictions.

Conclusion

Cases in China and in Western countries that may implicate national security concerns have become commonplace in global business today. In such an environment, it is important for businesses to keep changes to legislation in perspective. While there have been changes to the PRC Counter-Espionage Law, and questions remain as to how the new law will be implemented in practice, on balance, the revisions suggest that China continues to support advances to its version of the rule of law, which at the end of the day, may help promote a more transparent environment for business in China. The law is, in some respects, less opaque than the earlier 2014 version and consolidates under one heading many of the developments that have taken place in the decade since.

Contacts

Victor Ho
Registered Foreign Lawyer, Cal – A&O – Hong Kong
Tel +852 2974 7288
victor.ho@allenovery.com

Melody Wang
Partner – Lang Yue – Shanghai/Beijing
Tel + 86 21 2067 6988
melody.wang@allenoveryly.com

Jane Jiang
Partner – A&O – Shanghai
Tel +86 21 2036 7018
jane.jiang@allenovery.com

Matt Bower
Partner – A&O – Hong Kong
Tel +852 2974 7131
matt.bower@allenovery.com

Richard K. Wagner
Registered Foreign Lawyer – A&O – Hong Kong
Tel +852 2974 6907
richard.wagner@allenovery.com

Ran Chen
Litigation Counsel – Lang Yue – Beijing
Tel +86 10 8524 6100
ran.chen@allenoveryly.com

Jason Song
Senior Associate – Lang Yue – Shanghai
Tel +86 21 2067 6838
jason.song@allenoveryly.com

Biyu Wang
Associate – Lang Yue – Shanghai/Beijing
Tel +86 10 8524 6109
biyu.wang@allenoveryly.com

Allen & Overy Lang Yue (FTZ) Joint Operation Office

Room 1501-1510, 15F Phase II IFC Shanghai, 8 Century Avenue, Pudong, Shanghai China

Allen & Overy LLP, Shanghai office: Tel: +86 21 2036 7000 FAX: +86 21 2036 7100 www.allenovery.com

Shanghai Lang Yue Law Firm: Tel: +86 21 2067 6888 FAX: +86 21 2067 6999 www.langyuelaw.com

Allen & Overy Lang Yue (FTZ) Joint Operation Office is a joint operation in the China (Shanghai) Pilot Free Trade Zone between Allen & Overy LLP and Shanghai Lang Yue Law Firm established after approval by the Shanghai Bureau of Justice.

Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. It is authorised and regulated by the Solicitors Regulation Authority of England and Wales. Allen & Overy LLP is a multi-jurisdictional legal practice with lawyers admitted to practice in a variety of jurisdictions.

The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of members' names and of the non-members who are designated as partners is open to inspection at its registered office, One Bishops Square, London E1 6AD, United Kingdom and at the above address. Services in relation to the laws of the People's Republic of China are provided through Allen & Overy LLP's joint operation with Shanghai Lang Yue Law Firm.

Shanghai Lang Yue Law Firm is a general partnership formed under the laws of the People's Republic of China with law firm licence number 23101201410592645 whose registered office is at Room 1514 – 1516, 15F, Phase II, IFC, 8 Century Avenue, Shanghai 200120. It was established after approval by the Shanghai Bureau of Justice. A list of the partners and lawyers of Shanghai Lang Yue Law Firm is open to inspection at its registered office or via the Shanghai Bar Association.