



Xi's National Security Agenda: How can governments and businesses de-risk?

By Dennis Kwok



June 2023

About the China Strategic Risks Institute

The China Strategic Risks Institute (CSRI) is a non-profit, non-partisan research institute providing objective and unfiltered analysis of the risks and opportunities posed by the rise of the People's Republic of China. We aim for our research to be accessible to the general public, with recommendations for policymakers, international businesses and NGOs. CSRI does not offer corporate consultancy services and is not a political campaign or lobbying group.

www.csri.global

About the Author

Dennis Kwok is the founder and Executive Director of the China Strategic Risks Institute. He formerly served as a member of the Hong Kong Legislative Council representing the legal sector from 2012-2020.

Contents

1. Introduction.....	4
2. Beijing’s crackdown on the private sector.....	5
3. Xi’s obsession with national security.....	7
4. China’s new national security laws.....	8
5. Implications for foreign businesses.....	13
6. Policy recommendations.....	17

Introduction

Under Xi Jinping, 'national security' has been placed at the forefront of China's political and legislative agenda. Understanding what constitutes "national security" within China's Counter Espionage Law and related legislation will prove crucial for individuals and companies, both local and foreign, continuing to operate in China. This paper examines the risks posed to international businesses in Xi's new area, and makes recommendations to governments and businesses on how to "de-risk" their China operations.

Key Point Summary

- Xi's expansive definition of 'national security' is not confined to conventional concerns of terrorism, separatism, or extremism. Its definition encompasses broad ranging fields across culture, technology, data and cybersecurity, with ramifications across all aspects of the economy.
- A raft of new legislation grants the Chinese government sweeping powers to override economic activity in the interests of national security. These laws give a broad remit for the Chinese government to freeze assets, seize data and conduct arrests of businesses and individuals judged to be compromising national security.
- As demonstrated by the Chinese government's recent crackdown on foreign due diligence firms, even routine business operations risk running foul of national security laws. Foreign auditing and legal firms are likely to come under increased scrutiny in coming years, leading to an increasingly challenging business environment.
- Businesses and governments must work together to 'de-risk' their China operations. Governments should ensure that public funds are not invested in Chinese assets at risk of being caught up in sanctions and counter-sanctions in the event of a geopolitical crisis, as might occur over Taiwan. Businesses should diversify their operations and evaluate their ability to implement exit plans to limit losses in such an event.
- Asset managers curating ESG funds must re-evaluate their China investments in light of the difficulties in carrying out human rights due diligence. Government regulation should seek to provide minimum standards and standardised principles around ESG funds, including transparency around due diligence procedures.

Beijing's crackdown on the private sector

Xi Jinping's personal consolidation of power over China's party-state has been accompanied by a number of government campaigns to rein in the independence of the private sector.

In 2020, concerns over the growing power and independence of technology companies precipitated a major crackdown on the sector. A new wave of regulations imposed restrictions on publishing rules, advertisements, IPOs and the ability of Chinese companies to list overseas. Since then, tech giants Alibaba, Meituan and Tencent have paid hundreds of millions of dollars in fines for "abusing their market position".¹ Jack Ma, one of China's most successful tech entrepreneurs, was forced to relinquish control over Alibaba and Ant Group, and effectively forced into exile after criticising government regulators.²

Most recently, the Chinese government has increased pressure on foreign consulting, auditing and due diligence firms. In February this year, the Chinese authorities urged its state owned enterprises to phase out the use of the 'Big 4' foreign accountancy firms of Deloitte, EY, PwC, and KPMG – who together provide services to nearly a quarter of China's 98 central state-owned enterprises.³ A month later, authorities detained five staff in a raid on US consultancy group Mintz Group. These moves were likely motivated by Mintz Group conducting corporate due diligence work in relation to forced labour abuses in China's Uyghur Region, information which the Chinese government considers to be sensitive. The company was forced to evacuate senior staff from its Hong Kong office over fears of further arrests.⁴ Another US management consultancy, Bain & Co, also came under police attention, with officials seizing company devices including computers and mobile phones.⁵ We predict that international law firms' operations in China will be equally affected going forward, with the provision of legal services considered part of the national security realm.

-
1. Collier, A. (2022), *China's Technology War: Why Beijing Took Down Its Tech Giants*. London: Palgrave Macmillan. <https://doi.org/10.1007/978-981-19-3042-3>
 2. Mitchell, T. (2023), 'The Jack Ma's test for China's promised shift', *Financial Times*, 31 Jan 2023, <https://www.ft.com/content/90110e34-f1a8-40c8-bec7-2e40d9d858e1>
 3. Jaramillo, E. (2023), 'The Big Four auditors may lose state-owned business in China – would it actually hurt them?', *The China Project*, 8 Mar 2023, <https://thechinaproject.com/2023/03/08/the-big-four-auditors-may-lose-state-owned-business-in-china-would-it-actually-hurt-them/>
 4. Pomfret, J. & Tham, E. (2023), 'Exclusive: US consultancy Mintz's executives leave Hong Kong after China raid', *Reuters*, 19 May 2023, <https://www.reuters.com/world/china/us-consultancy-mintzs-executives-leave-hong-kong-after-china-raid-sources-2023-05-19/#:~:text=HONG%20KONG%20FOSHANGHAI%2C%20May%2019,direct%20knowledge%20of%20the%20matter.>
 5. Wakabayashi D. & Bradsher K. (2023), 'U.S. Consulting Firm Is the Latest Target of a Chinese Crackdown', *The New York Times*, 27 Apr 2023, <https://www.nytimes.com/2023/04/27/business/bain-china.html>

These cases are indicative of how local and foreign businesses find themselves increasingly restrained by the national security concerns of the Chinese government. Underpinning this change is a broader conception of national security that means that even ordinary business activities – such as the conducting of corporate due diligence – can fall foul of the authorities.

Table 1: China’s crackdown on the private sector (2023)

Timeline	Development
February 2023	SOEs urged to phase out services of 'Big Four' accounting firms
March 2023	Deloitte's Beijing office suspended for three months and fined USD \$30.8 million
March 2023	Raid on the US due diligence firm Mintz Group, with five employees detained
March 2023	Detention of an employee of Japan's Astellas Pharma Inc.
April 2023	Police question staff at US consultancy Bain & Company
May 2023	Raid on global consulting firm Capvision Partners

Xi's obsession with national security

In his 20th Party Congress speech, President Xi Jinping mentioned the word “security” ninety-one times, with his speech presenting a clear emphasis on the strengthening of China’s national security. As a legal concept, ‘national security’ under Chinese laws is synonymous with state security and the ‘party security’ of the Chinese Communist Party (CCP). The direct imposition of the Hong Kong National Security Law in June 2020 is manifestation of this obsession with national security, especially when it relates to the peripheral regions of China,⁶ while a raft of new, national security focused legislative initiatives have also been implemented in mainland China.

Understanding what constitutes “national security” within China’s legal framework will prove crucial for individuals and companies, both local and foreign, continuing to operate in China and Hong Kong. China’s National Security Law, enacted in 2015, provides an expansive definition of national security not confined to more conventional concepts such as acts of terrorism, separatism, or extremism. Instead, China’s National Security Law requires all actors to safeguard key economic interests.⁷ This includes industries vital to the national economy, key industrial sectors, key infrastructure projects, and key construction projects, such as:

- finance
- resources and energy
- food safety and biosecurity
- culture
- technology
- cybersecurity
- data
- ecological and environmental protection
- nuclear technology
- overseas interests
- artificial intelligence

6. Pursuant to a decision by the National People’s Congress of China on 28 May 2020, the NPCSC decided to formulate and adopt the draft NSL, and added the NSL to the list of national laws in Annex III to the Basic Law to the effect that the NSL could be applied locally to Hong Kong *by way of promulgation* by the Hong Kong Special Administrative Region. It was accordingly promulgated by Carrie Lam, the then Chief Executive of Hong Kong, who gave notice that the NSL applied as from 11 p.m. on 30 June 2020. The whole enactment process of the NSL, being a national law under the Constitution of China, bypassed the local legislature of Hong Kong, not to mention the absence of any consultation with the Hong Kong legislature and the wider public. In *HKSAR v Lai Chee Ying* [2021] HKCFA 3, the Hong Kong Court of Final Appeal ruled that “the legislative acts of the NPC and NPCSC leading to the promulgation of the NSL as a law of the HKSAR, done in accordance with the provisions of the Basic Law and the procedure therein, are not subject to [constitutional] review on the basis of any alleged incompatibility as between the NSL and the Basic Law or the ICCPR [International Covenant on Civil and Political Rights] as applied to Hong Kong” (para 37).

7. China Law Translate (2015), *National Security Law*, <https://www.chinalawtranslate.com/en/2015nsl/>

- exploration and use of outer space
- international seabed areas, and
- polar regions

This expansive definition of national security and its application across industries has been echoed by top government officials in Hong Kong on National Security Education Day.⁸ Notably, China's National Security Law and Hong Kong's National Security Law both apply to state-owned as well as private entities.

China's new national security laws

In addition to China's National Security Law, Xi's national security obsession has led to a raft of new legislation with a national security focus. These include the newly amended Counter-Espionage Law, the Anti-Foreign Sanctions Law, the Foreign State Immunity Law, and the Foreign Relations Law – legislative developments that signal a reset of China's relationship with democratic countries under Xi Jinping in his 'New Era'. These include measures to protect foreign agents, including businesses, from accessing what the government deems to be sensitive data. China has also closely observed democratic countries' response to Russia's invasion of Ukraine. Through these laws, China is preparing the legal groundwork to counter any attempts by the US and other countries to impose sanctions, embargo or other hostile measures against it – such that may arise should China take action against Taiwan. More broadly, these laws are preparing China for an economic decoupling from democratic countries. Businesses operating in China and Hong Kong must pay attention to how these news laws will impact them.

The Counter-Espionage Law

Amendments to China's Counter-Espionage Law on April 26, 2023 have significantly broadened the scope of what materials may be considered under espionage. Rather than being restricted to the mishandling of 'state secrets', the Counter-Espionage Law will now cover any "documents, data, materials or items related to national security and interests".⁹

8. National Security Education Day (n.d.), *Holistic View of National Security*, https://www.nsed.gov.hk/national_security/index.php?l=en&a=safety

9. China Law Translate (2023), *Counter-espionage Law of the P.R.C. (2023 ed.)*, <https://www.chinalawtranslate.com/en/counter-espionage-law-2023/>

Given the scope of national security is broad and all-encompassing, any collection and transfer of data (including economic and financial data) from within China to outside entities could constitute espionage activities under the new law. This partly explains why the Chinese authorities have been targeting US consultancy firms,¹⁰ and the attempt to push the Big 4 accounting firms out of China.¹¹ By conducting due diligence on Chinese supply chains, or by looking closely at Chinese firms' accounting structures, these companies may be regularly accessing information considered sensitive to national security purposes. Firms then passing this information on to foreign entities represent a particular risk. The Counter-Espionage Law provides the legal basis for cracking down on these firms, with the recent spate of investigations a warning signal.

From this perspective it is difficult to see how the Chinese government can tolerate any foreign firms which require an intimate knowledge of their Chinese counterparts. Not only will consulting and due diligence firms continue to be impacted, but we also predict that the Chinese government will soon act to phase out the provision of legal services by international law firms for national security purposes.

Aside from expanding its remit, the Counter-Espionage Law also enlarges the search powers of state security organs. Provisions allow authorities to inspect any items of suspected espionage, including documents, electronic equipment and facilities of individuals and organisations, as well as to issue fines and detain suspects. The law also requires Chinese citizens and organisations to report suspected espionage and assist the authorities in investigations. For example, telecommunications operators and internet service providers could be required to promptly provide technical support to assist with investigations.

The Anti-Foreign Sanctions Law

In addition to strengthening national security law enforcement and maintaining stability within its borders, Beijing is working to build a system for applying its laws and supervising behaviour abroad. The deterioration of China-US relations in recent years, as well as sanctions from democratic countries over human rights abuses in the Uyghur Region, have prompted China to pass the Anti-Foreign Sanctions Law. This seeks to establish comprehensive measures to counter foreign sanctions and interference.

10. Wakabayashi D. & Bradsher K. (2023), 'U.S. Consulting Firm Is the Latest Target of a Chinese Crackdown', *The New York Times*, 27 Apr 2023, <https://www.nytimes.com/2023/04/27/business/bain-china.html>

11. Makortoff, K. (2023), 'China instructs state firms to phase out big four auditors', *The Guardian*, 22 Feb 2023, <https://www.theguardian.com/world/2023/feb/22/china-instructs-state-firms-to-phase-out-big-four-auditors>

The Anti-Foreign Sanctions Law allows China to take countermeasures against a broad range of actors and actions that it deems to endanger its sovereignty, security and interests. Any person or entity that directly or indirectly participates in the sanctions or restrictive measures against China will be placed on the list of countermeasures.¹² The four main countermeasures include:

- 1) Not issuing visas, denying entry, cancelling visas, or deportation;
- 2) Sealing, seizing, or freezing movable property, real estate, and all other types of property within the [mainland] territory of our country;
- 3) Prohibiting or restricting relevant transactions, cooperation, and other activities with organisations and individuals within the territory of China;
- 4) Other necessary measures.

Foreign actors face increased risk due to the Anti-Foreign Sanctions Law. China now has significant leeway to determine triggers and use countermeasures, such as ambiguous definitions of national security threats and violations of international norms. This includes interference in China's internal affairs, which falls within this scope as well. Given that the Chinese government has previously claimed that the US and Europe's 'unilateral' sanctions on Russia following the invasion of Ukraine violate international norms,¹³ and has accused professional trade bodies such as the Hong Kong Foreign Correspondents Club of 'meddling' in China's internal affairs,¹⁴ foreign governments and businesses should expect these laws to be broadly interpreted.

It is notable that the Chinese government has already used retaliatory sanctions against foreign groups and individuals, even before the Anti-Foreign Sanctions Law was put in place. In March 2021 the Chinese government sanctioned lawmakers, academics and NGOs in the EU and UK in response to sanctions against Chinese officials responsible for human rights abuses in the Uyghur Region.¹⁵ The passage of the Anti-Foreign Sanctions Law suggests that the Chinese government is preparing for a much greater use of these measures in the near future.

12. The Anti-Foreign Sanctions Law, Article 12: Organizations and individuals must not enforce or assist in enforcing the discriminatory restrictive measures employed by foreign nations against our nation's citizens or organisations.

13. Bloomberg (2022), 'China Says It Wants to Avoid U.S. Sanctions Over Russia's War', 15 Mar 2022, <https://www.bloomberg.com/news/articles/2022-03-15/china-says-it-wants-to-avoid-u-s-sanctions-over-russia-war>

14. Kwan, R. (2021), "Know your place': Beijing accuses Hong Kong press club of being 'external force' interfering in China's internal affairs", *Hong Kong Free Press*, 26 Apr 2021, <https://hongkongfp.com/2021/04/26/know-your-place-beijing-accuses-hong-kong-press-club-of-being-external-force-interfering-in-chinas-internal-affairs/>

15. Emmott, R. & Brunstrom, D. (2021), 'West sanctions China over Xinjiang abuses, Beijing hits back at EU', *Reuters*, 22 Mar 2021, <https://www.reuters.com/article/uk-usa-china-eu-sanctions-idUSKBN2BE2LF>

The Foreign Relations Law and Foreign State Immunity Law

The Foreign Relations Law and Foreign State Immunity Law are two major pieces of draft legislation that will give the Chinese government further tools to crack down on foreign entities in response to perceived hostile actions.

The current draft of the Foreign Relations Law serves as the basic legal framework for China's foreign affairs, with a particular focus on safeguarding its national security.¹⁶ This is part of the effort to codify into law Xi's vision and strategy of "holistic" national security [總體國家安全觀重大戰略思想]. Similarly to the Anti-Foreign Sanctions Law, the legislation is designed to give the Chinese government more powers to respond to foreign sanctions, export controls and other measures that may be imposed upon it. While the law does not specify in detail what particular actions the Chinese government may take, it does provide a broad legal framework for the undertaking of "countermeasures" and "restrictive measures" against overseas foreign entities and individuals that are perceived to be harming China's interests.¹⁷

The law is also designed to give the Chinese government greater leeway to override and ignore its commitments under international law. Article 30 of the draft sets out that international treaties and conventions concluded or acceded to by the Chinese state shall not contravene its constitution, while Article 31 of the draft provides a reservation that allows national security interests to override the implementation of international treaties and conventions.¹⁸ This raises the possibility that China's agreements under the World Trade Organization, as well as regional trade agreements such as the China-ASEAN Free Trade Agreement, the China-Australia Free Trade Agreement and the proposed EU-China Comprehensive Agreement on Investment could all be overridden by China's broad ranging national security concerns. The open breach of the Sino-British Joint Declaration on Hong Kong is only a prelude of what is to be expected.

16. The Foreign Relations Law, Article 4: The People's Republic of China pursues an independent and peaceful foreign policy, observes the five principles of mutual respect for sovereignty and territorial integrity, mutual nonaggression, mutual noninterference in internal affairs, equality and mutual benefit, and peace ul coexistence, and opposes hegemony and power politics.

17. Zhao, D. & Zhou, W. (2023), *China Draft Foreign Relations Law: A Commentary*, Global Law Office, 23 Feb 2023, <http://www.glo.com.cn/Content/2023/02-24/1641474895.html#>

18. Ibid

The draft Foreign State Immunity Law abolishes the absolute immunity principle for foreign states – a principle which previously prevented cases from being brought against foreign states in Chinese courts.¹⁹ Instead, foreign states are given restrictive immunity, whereby foreign states and their property generally have immunity except in cases specified by the Law and for non-sovereign acts such as commercial activities. This measure in itself is not unusual, bringing Chinese law in line with other foreign states, including the US and UK. However, Article 20 of the Foreign State Immunity Law is particularly noteworthy, as it introduces the principle of ‘reciprocity’ in determining whether state immunity applies to a particular case.²⁰ This means that if other states’ courts exercise jurisdiction over China and its property, Chinese courts can likewise exercise jurisdiction over them. This opens the possibility to foreign states being sued in Chinese courts in response to sanctions, export controls or other measures which may impact Chinese firms. Once again, these laws show that the Chinese government is preparing the legal groundwork for a major decoupling from the democratic world, and is acting to de-risk areas of vulnerability.

Table 2: China’s new national security laws

Law	Year	Content
Counter-Espionage Law	Adopted on November 1, 2014, and revised on April 26, 2023, with effect from July 1, 2023.	Amendments expand the definition of espionage to include any documents, data, materials or items related to national security and interests.
Anti-Foreign Sanctions Law	Adopted and effective on June 10, 2021.	Grants powers to impose counter-sanctions against a broad range of actors and actions deemed to endanger national sovereignty, security and interests.
Foreign Relations Law	Pending 2nd round deliberation in 2023.	Enshrines powers to take measures against overseas foreign entities and individuals that harm China's interests.
Foreign State Immunity Law	Pending 2nd round deliberation in 2023.	Enables Chinese courts to exercise jurisdiction over foreign states and their property, should other states’ courts exercise jurisdiction over China and its property

19. Dodge, W. (2023), *China’s Draft Law on Foreign State Immunity Would Adopt Restrictive Theory*, Transnational Litigation Blog, 12 Apr 2023, <https://tlblog.org/chinas-draft-law-on-foreign-state-immunity-would-adopt-restrictive-theory/>

20. The Foreign State Immunity Law, Article 20: Where foreign states accord China and its property narrower immunity that is provided by this Law, China courts may apply the principle of reciprocity.

Implications for foreign businesses

Taken together, these legal developments have far-reaching implications for foreign companies, impacting their due diligence practices, legal risks, and overall business operations in China.

Impact on corporate due diligence

These new legal developments impose significant restrictions on the ability of foreign companies to conduct due diligence in the country. China's expansive definition of national security includes the broad fields of economic security and cybersecurity, among other areas, which makes routine business activities potentially sensitive. As a result, foreign companies must exercise caution when gathering and analysing information, as it may be deemed sensitive by Chinese authorities.

The Counter-Espionage Law has expanded the scope of materials that can be considered espionage-related, including documents, data, and materials related to national security and interests. This places foreign consultancy firms and due diligence providers at risk of scrutiny and investigation, as their collection and transfer of data outside of China could be interpreted as espionage activities under the new law. Consequently, foreign companies face legal risks and potential penalties for their due diligence activities, which hampers their ability to thoroughly assess risks and make informed business decisions in China.

The crackdown on due diligence firms will further cloud the picture for prospective investors in Chinese firms. Instances of faking credentials and resumes are prevalent in China, as exemplified by the notorious delisting of Luckin Coffee from NASDAQ in 2020.²¹ Foreign investors already face significant asymmetries of information compared to local actors. Notably, major private business information platforms in China, including Tianyancha, Qichacha, and Qixin, are no longer accessible through overseas VPNs.²²

21. RTTNews (2020), 'Luckin Coffee To Be Delisted From Nasdaq On June 29', *Nasdaq*, 26 Jun 2020, <https://www.nasdaq.com/articles/luckin-coffee-to-be-delisted-from-nasdaq-on-june-29-2020-06-26>

22. Bloomberg (2023), 'China Restricts Overseas Access to Key Corporate Information', 3 May 2023, <https://www.bloomberg.com/news/articles/2023-05-03/china-restricts-overseas-access-to-corporate-registry-databases>

Furthermore, following the revision of the Counter-Espionage law, Wind Information, one of the largest financial data providers, has imposed restrictions on offshore users accessing Chinese enterprise databases.²³ Shrewd investors are right to question the data credibility of Chinese companies, a task now made significantly harder. Foreign investors in China thus face increased financial risks, facing growing uncertainty over the true nature of partners.

The difficulties of conducting due diligence in China are particularly acute with regards to inspecting supply chains for potential human rights violations. As noted above, the raids on Mintz group were motivated by the firms conducting due diligence work on supply chains in the Uyghur Region, where there are severe concerns around widespread state sponsored forced labour programmes. The Chinese government sees its measures to repress the Uyghurs and other ethnic and religious minorities as necessary for the security of the region, meaning that information on forced labour abuses is treated as highly sensitive. Even before the pressure on Mintz group, the ethical industry alliance Better Cotton Initiative suspended activities in the Uyghur Region due to the challenge of conducting due diligence there.²⁴

Companies hoping to comply with the US Uyghur Forced Labor Prevention Act, or with their own internal modern slavery commitments, will find it increasingly difficult to provide sufficient evidence to demonstrate that supply chains in the region are free from forced labour. This also poses major questions on the ability of Environmental, Social and Governance (ESG) investment funds to conduct the due diligence needed to ensure investors that their funds are in line with ESG commitments. Major investment funds have already been linked to investments in companies complicit in human rights abuses in the Uyghur Region and elsewhere in China.²⁵

23. Ibid.

24. Business & Human Rights Resource Centre (n.d.), *China: Better Cotton Initiative suspends activities in Xinjiang due to concerns over labour abuses*, <https://www.business-humanrights.org/en/latest-news/china-better-cotton-initiative-suspends-activities-in-xinjiang-due-to-concerns-over-labour-abuses//>

25. Hong Kong Watch (2022), *(Updated) New Hong Kong Watch report finds that MSCI investors are at risk of passively funding crimes against humanity in Xinjiang*, 5 Dec 2022, <https://www.hongkongwatch.org/all-posts/2022/12/5/updated-new-hkw-report-finds-that-msci-investors-are-at-risk-of-passively-funding-crimes-against-humanity-in-xinjiang>

Accessing sensitive data

The fear of being caught in the crosshairs of national security concerns and potential legal consequences has ramifications beyond the ability to conduct due diligence. Given the broad scope of these laws, any ordinary business activity which could bring foreign companies into contact with data deemed as sensitive to national security is at risk. Accounting firms, which are required to understand the financial vulnerabilities of Chinese firms, could find themselves the target of such legislation – particularly if providing services for state-linked enterprises or other major firms.

The Chinese government's discomfort with foreign accountancy firms can already be seen in attempts to push the 'Big 4' accountancy firms out of China – even though local branches are legally and structurally independent from Western headquarters. There is a realistic possibility that this crackdown will be extended to international firms offering legal services to Chinese clients, who may similarly come into contact with sensitive information.

The inclusion of energy, technology (such as artificial intelligence) and cyber as key domains under the Chinese government's conception of national security also raises risks for foreign companies operating in these sectors. Through the 'Made in China 2025' initiative, the Chinese government is seeking to reduce its dependence on foreign technologies, particularly in strategic sectors related to national security, by the middle of this decade. Aligned with this strategy is China's new Export Control Law, in effect from 2020, which seeks to strengthen control over strategic goods and advanced technology exports – including dual use technologies with both civilian and military applications.²⁶ Within this context, it is feasible that the Counter-Espionage Law and related legislation could be used as a basis to target foreign companies working with Chinese companies in strategically important technologies.

26. Kawate, I. (2022), 'China to tighten export controls on dual-use technology', *Nikkei Asia*, 1 May 2022, <https://asia.nikkei.com/Economy/China-to-tighten-export-controls-on-dual-use-technology>

Counter-sanctions risk

China's enactment of the Anti-Foreign Sanctions Law and Foreign State Immunity Law provides the Chinese government with tools to respond to perceived hostile actions by foreign entities. The law grants broad discretionary powers to identify triggers and impose countermeasures against individuals and entities involved in such actions. The ambiguity surrounding definitions of national security threats and violations of international norms raises concerns about potential retaliatory measures targeting foreign companies.

The fallout from Russia's invasion of Ukraine shows how international firms can be caught in the regulatory crossfire. The EU plans to expand sanctions on companies that provide military support to Russia, which includes eight Chinese companies.²⁷ Both China's foreign ministry and its ambassador to the EU have signalled the possibility of retaliatory action. At the same time, the EU is considering a mandatory ban on its member states' use of Huawei's 5G equipment.²⁸ China has already banned the import of US chipmaker Micron in May as a countermeasure to US sanctions, claiming national security concerns. These new laws will further solidify China's diplomatic capabilities to pose such threats.

These concerns would be heightened in the event of an escalating geopolitical crisis, as could occur should the Chinese government take military action against Taiwan. In this event, it is likely that the US and other democratic countries will enact a raft of sanctions on Chinese firms and individuals, including asset freezes, travel bans and export controls. Foreign companies complying with these measures could be seen by the Chinese government as acting counter to its national security interests. For example, banks that act on orders to freeze the assets of Chinese government officials or state owned enterprises, companies that cancel contracts with Chinese firms in order to meet export control requirements, or airlines refusing travel to individuals on travel blacklists. In these cases, companies could be caught between orders to comply with the US and other democratic countries' sanctions requirements on the one hand, and the possibility of being targeted by China's Anti-Foreign Sanctions Law on the other.

27. Norman, L. (2023), 'EU Targets Eight Chinese Companies in Russia Sanctions Push', *The Wall Street Journal*, 8 May 2023, <https://www.wsj.com/articles/eu-targets-eight-chinese-companies-in-russia-sanctions-push-a5fe6c2e>

28. Bloomberg (2023), 'China Lobbies EU on Proposal to Punish Firms Aiding Russia', 8 Jun 2023, <https://www.bloomberg.com/news/articles/2023-06-08/china-lobbies-eu-over-proposal-to-punish-firms-supplying-russia>

It is important to note that many of the PRC laws analysed in this article have extraterritorial jurisdiction. This is China's attempt to match the United States in terms of its ability to exercise its long arm jurisdiction overseas [涉外法治]. This will have particularly strong implications when it comes to China's interests in the Belt and Road Initiatives (BRI) in over 100 countries.²⁹ This is already having an effect on the restructuring of sovereign debts and the debt relief for countries involved in BRI and the countering of international norms by China.³⁰

Policy recommendations

Xi's obsession with national security has ushered in a raft of legislation aimed at giving the Chinese government more levers of economic control, particularly over the activities of foreign companies. Through this legislation, the Chinese government is laying the groundwork for a broader divergence with democratic countries, both politically and economically. By ensuring that it has the ability to take control of its own broad security interests, while countering attempts by foreign powers to impose sanctions or other measures against it, the Chinese government is attempting to 'de-risk' its relationship with the democratic world. Foreign governments and businesses must understand the implications of these developments for their own interests, and they too should act to 'de-risk' key areas of vulnerability.

Recommendations for governments:

- **'De-risking' public funds:** State pension funds, sovereign wealth funds, local government funds and other public investments in China face a number of risks. Those invested in companies linked to China's military industrial complex may be required to quickly unwind investments in order to comply with democratic countries' sanctions on China in the event of an escalating geopolitical crisis, or may be targeted by the Chinese government under its Anti-Foreign Sanctions Law. Lessons should be learned from the experience of a quarter of UK councils' pension funds, which until recently held shares in Russian banks and companies that have been sanctioned by democratic countries following Vladimir Putin's invasion of Ukraine.³¹

29. Rudolf, M. (2021), 'Xi Jinping Thought on the Rule of Law: New Substance in the Conflict of Systems with China', *SWP Comment*, 28 Apr 2021, <https://www.swp-berlin.org/10.18449/2021C28/>

30. Kargman, S. T. (2023), 'The brave new world of sovereign debt restructuring: the China conundrum and other challenges', in *International Insolvency & Restructuring Report 2023/24*, pp.15-21. Essex: Capital Markets Intelligence.

31. Lavin, S. (2022), "Profiting from Putin's Russia: Quarter of Council Pension Funds Invested in Russian Firms", *Byline Times*, 25 Mar 2022, <https://bylinetimes.com/2022/03/25/profitting-from-putins-russia-quarter-of-council-pension-funds-invested-in-russian-firms/>

To mitigate this risk, governments should:

- Conduct an audit of public funds invested in China and other authoritarian states through sovereign wealth funds, local government funds and public pension funds.
- Stress-test the exposure of public funds to geopolitical shocks, including the impact of sanctions and counter-sanctions in the event of China taking action against Taiwan.
- Set in place guidelines to minimise and phase out public funds invested in China, particularly those invested in state corporations or the military industrial complex.
- **Advising the private sector:** Democratic countries such as the UK, the US, Canada, Germany and France issue country-specific profiles to offer advice to businesses trading and investing internationally. At the time of writing, only the UK and the US highlight the likely impact of the Anti-Foreign Sanctions Law on business risks in China, and even then neglected to mention the Counter-Espionage Law or other legislative developments analysed in this paper.³² Canada's advisory mentioned the importance of conducting due diligence in China but has not been updated to reflect recent challenges in this area. To mitigate this risk, governments should:
 - Update business risk advisories to take into account the increased difficulties that these laws pose to everyday business activities, such as corporate due diligence, as well as the increased chance of seizure of assets or data.
 - Monitor the impact of new legal and political developments on business risks, such as proposed laws in Hong Kong targeting misinformation or 'fake news' and imposing internet controls.³³

32. UK Government (2022), *Overseas business risk: China*, 11 Mar 2022, <https://www.gov.uk/government/publications/overseas-business-risk-china/overseas-business-risk-china>; U.S. Department of State (2022), *2022 Investment Climate Statements: China*, <https://www.state.gov/reports/2022-investment-climate-statements/china/>

33. The so-called unofficial Hong Kong national anthem "May Glory be to Hong Kong", which was widely played during the 2019 protests, was accidentally played in a few international sporting events, prompting local officials and politicians in Hong Kong to call for the investigation against Google for possible breach of the HK NSL.; Siu, D. & Pang, J. (2022), 'Google refused Hong Kong request over protest anthem - HK official', *Reuters*, 12 Dec 2022, <https://www.reuters.com/technology/google-refused-hong-kong-request-over-protest-anthem-hk-official-2022-12-12/>

- **ESG reform:** The challenges facing firms seeking to conduct human rights due diligence in China reveals broader issues within the ESG investment sector. While asset managers are able to market certain funds as meeting ESG principles, there is little regulation guiding what due diligence must be carried out to ensure that ESG standards are met, nor regulations establishing what these standards should be. To ensure that those investing in ESG funds do not unwittingly fund human rights abuses, governments should:
 - Begin consultations with civil society groups and businesses on establishing common standards and principles for ESG investment funds to abide by, including due diligence procedures.
 - Draft regulations mandating large asset managers to give clear information to investors on the principles, standards and due diligence procedures guiding their ESG investment funds.
 - More emphasis should be placed on the social and governance components within ESG principles. They should include clear standards for companies that do business in authoritarian regimes, human rights violations in supply chains, and CCP cells that are now mandatory for firms operating in China.

Recommendations for businesses:

- **De-risking China funds:** Banks and investment funds should assess their ability to quickly unwind investments and move assets held in China in the event of a major geopolitical crisis or imminent anti-sanction measures. Firms should come up with plans to limit their losses in this scenario and stress test their ability to withstand these losses. Efforts to diversify investment portfolios away from China can help reduce these risks in the long term.
- **Assessing legal risks:** Firms conducting due diligence, auditing and other services with Chinese counterparts should assess their risk levels in relation to China's Counter-Espionage Law. Those with clients working in the technology or military industrial complex may be at particularly high risk, as well as those working with major state corporations. The new national security laws that will be enacted in Hong Kong later this year or early next year (known as Article 23 legislation) should also be taken into account. These new laws will see the enactment of Hong Kong's own version of anti-foreign espionage laws, laws against fake news, and internet control.

- **Re-thinking corporate strategy:** Firms investing in and trading with China should consider the long term implications of the increasingly challenging environment with regards to the ability to conduct corporate due diligence. Corporate strategy on the Chinese market must take into account the growing risks that may be posed by difficulties in gaining holistic information on Chinese counterparts, including governance structures and financial information.
- **Evaluating human rights due diligence structures:** Firms must assess whether proper human rights due diligence is still possible in China in light of the increasing pressure on firms working in this area. This must be evaluated against each firms' own corporate social responsibility policies, as well as requirements under modern slavery and mandatory human rights due diligence legislation. Asset managers curating ESG funds should review investments in China, with a view to removing those linked to the Uyghur Region that cannot demonstrate their distance from human rights abuses.



Copyright © China Risks Ltd, 2023

Cover image: New York; Shanghai; London
Photo credit: sungmu heo; zhang kaiyv; Samuel Sweet