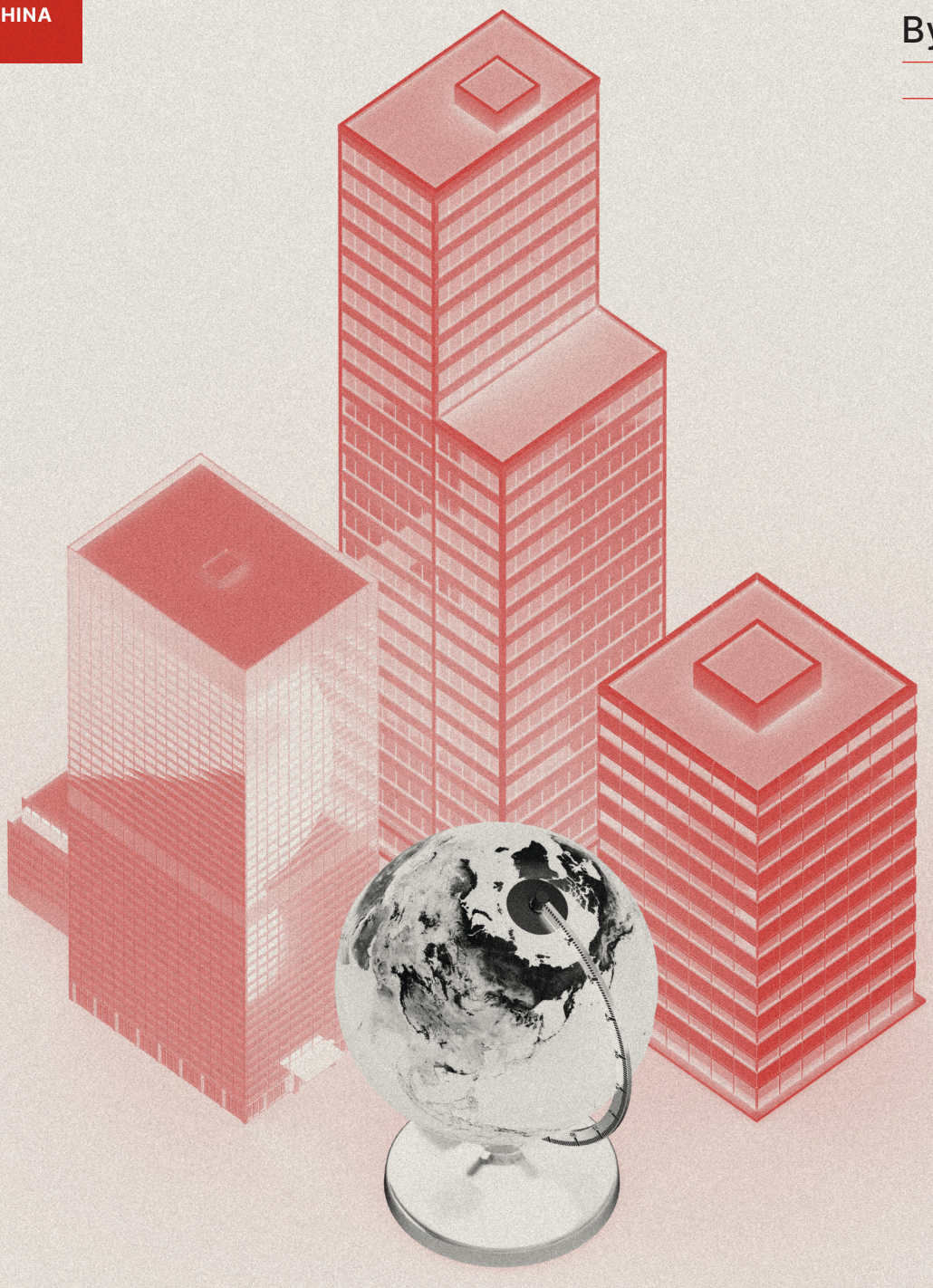
THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

July 11, 2023



China's Targeting of International Companies in Geopolitical Competition

Executive Summary

International businesses and corporate decision-makers cannot ignore geopolitics, as companies, their supply chains, and customers are increasingly targeted in cyber and non-cyber efforts to secure the national objectives of governments around the world. Companies must monitor the nexus between their business activities and countries' perceptions of national security — particularly as "great power competition" intensifies — and plan to mitigate geopolitically driven risk. China is currently among the leading sources of such risk, given Beijing's engagement in an escalating rivalry with the United States (US), assertive role in many potential flashpoints in Asia, and prioritization of national security over economics. Geopolitical competition involving China since 2017 has cost (or had the potential to cost) international businesses hundreds of millions of USD in revenue. In some cases, China's treatment of businesses during geopolitical disputes and subsequent financial losses has further prompted companies to scale back operations in or exit the country.

Notable risks to businesses operating in China or exposed to the Chinese market include changing laws, new export controls, and potential supply-chain disruptions if regional conflict erupts. In responding to perceived threats to China's national security, human rights record, technological advancement, and territorial and sovereignty claims, Beijing has taken — and is very likely to continue taking — 8 types of actions that create special risks for international businesses: **Cyberattack**, **Boycott**, **Embargo**, **Exit Ban**, **Law Enforcement Action**, **Product Ban**, **Regulatory Action**, and **Sanctions**. Although planning for these risks is made difficult by Beijing's ill-defined laws and regulations, broad government powers, and lack of an independent judiciary, businesses should establish constant **Monitoring** teams, pursue supply-chain and market **Diversification** strategies, and increase **Resilience** through broad crisis management planning.

Key Findings

- The primary geopolitical drivers causing China to take action against international businesses are related to **National Security**, **Human Rights**, **Technology Competition**, and **Territorial and Sovereignty Disputes**.
- Businesses operating in China, and those that rely on the Chinese market, are at risk of being targeted with 1 of the 8 actions listed above because of corporate actions or (more rarely) the personal actions of their employees, and because of factors outside of their control, such as the actions of their home government or foreign governments.
- Specific issues to which China has responded by taking action against international businesses include, but are not limited to, consulting with government officials and industry insiders, expressing concern for human rights in Xinjiang, supporting foreign government initiatives to inhibit China's technology industry, and failing to align with China's position on Taiwan.
- China has almost certainly prioritized **National Security** over economic development, leading to shifting interpretations of state law and **Law Enforcement Action** against even once-accepted industries.

- Increasing international scrutiny of **Human Rights** in China is creating likely state-supported **Boycott** risks for businesses that attempt to express concern or comply with international sanctions.
- The US-China **Technology Competition** is almost certainly driving retaliatory and possibly preemptive **Product Bans** targeting international businesses operating in China.
- When foreign governments challenge Beijing on **Territorial and Sovereignty Disputes**, China almost certainly targets those nations' industries with **Embargoes**.
- Other risks that must be considered include, but are not limited to, the potential for disruptive conflict along key shipping lanes, international sanctions regimes, and evolving data governance regulations in China and elsewhere.

Table of Contents

Risks from China

While geopolitical risks are inherently a global issue, many businesses are increasingly focused on those stemming from China. Industry surveys published in 2022 and 2023 show that US-China decoupling is a top concern — shifting policies in Western countries are causing the most anxiety, but there are also fears that China could retaliate against private enterprises. Other China-related anxieties identified in industry surveys include rising US-China tensions more broadly, consumer boycotts of foreign brands, and potential flashpoints in the South China Sea and Taiwan. In 2022 and 2023, China was found to be the second of 5 top countries in which businesses surveyed by the multinational insurer Willis Towers Watson reported a financial loss as the result of a political risk.[1]

In the current geopolitical climate, there are numerous compliance risks — changing laws, data governance regimes, and general trade and export restrictions in China, the US, and elsewhere. China's territorial and sovereignty disputes are also fraught with risks similar to those that might be seen in a conflict involving any major economic region. Many of the disputes are located along key commercial shipping routes, such as in the Taiwan Strait, and conflict could (and at certain levels of intensity almost certainly would) disrupt trade and supply chains.

There are also special risks born from Beijing's tactics for managing specific geopolitical challenges, which often involves retaliatory or punitive actions against international businesses. To better understand the range of actions in Beijing's toolkit and these special risks, Insikt Group surveyed 25 instances in which companies were the target of geopolitically motivated actions initiated by authorities in China (see **Appendix A**). This sample of instances included overt forms of economic coercion — a well-documented element of China's foreign policy — as well as actions such as bans of products on national security grounds and investigations of companies according to evolving national security priorities (see the Capvision case below). While some of China's actions detailed in this report are similar to those of other countries, timing, planning for, and mitigating their impact is a significant challenge due to the combination of Beijing's ill-defined laws, broad government powers, and the lack of an independent judicial system. The result is an environment where enforcement may appear arbitrary and often cannot be readily contested, though there are steps companies can take to mitigate risks (see **Mitigation Strategies**).

Specifically, since 2009, authorities in China and patriotic hacktivists have taken 8 types of actions against international businesses in efforts to manage perceived threats to China's national security and other geopolitical challenges. The list of actions below illustrates the range of punitive activities that may affect businesses exposed to geopolitical competition and disputes involving China. Note that our sample is not exhaustive, and due to numerous external factors that affect whether and what form of punitive action is taken, we cannot state which risks are more likely to challenge international businesses. Nevertheless, corporate decision-makers must consider the special risks posed by these actions as they navigate the era of so-called "great power competition".

[1] A financial loss due to a political risk, such as loss caused by sovereign non-payment of a contract, political violence, or trade sanctions, per the surveys cited.

- **Cyberattack** — Actions against companies in cyberspace; in the sample we looked at, defacement and other disruptive attacks carried out by hacktivists are the most frequent.
- **Boycott** — Efforts by authorities to stoke a refusal by Chinese consumers or organizations to purchase a company's products for a perceived political slight; in the sample, focus is placed on cases in which the state almost certainly had relatively direct involvement.
- **Embargo** — Actions to block the import of products from a specific country with which China has a dispute; in the sample, this is the second-most frequently observed risk type.
- **Exit Ban** — Refusal by Chinese authorities to allow persons to leave China; in the sample, the least frequently observed risk type.
- **Law Enforcement Action** — Actions taken against companies by law enforcement or state security agencies; in the sample, investigations and seizure of computers and similar assets is most frequent.
- **Product Ban** — Actions taken to prevent the normal commercial operation of a company and the sale of a product; in the sample, this is the most frequently observed risk type.
- **Regulatory Action** — Administrative action taken by state authorities against companies for alleged regulatory violations; in the sample, tax and fire safety violations and fines are observed.
- **Sanctions** — Sanctions declared by the Chinese government against a company; in the sample, these are only seen against American weapons developers that sell to Taiwan.[2]

A form of risk we expected to observe more frequently was **Exit Bans**. These are almost certainly of concern to international businesses. However, they appear more prominent in civil business disputes than in geopolitically motivated actions, though lack of detail around many specific cases in public sources means this risk cannot be ruled out. At least 1 case of a likely geopolitically motivated Exit Ban is seen in the Mintz Group case discussed in the **Human Rights** section.

Note that this report does not highlight China's use of cyber capabilities to acquire intellectual property or conduct espionage, unless the activity could be linked to a specific geopolitical grievance involving a targeted company.

Risk by Issue Area

This section examines how and when Beijing takes action against companies in relation to geopolitical concerns via brief case studies categorized by overarching issue areas — **National Security**, **Human Rights**, **Technology Competition**, and **Territorial and Sovereignty Disputes**. These cases, and Insikt Group's broader survey of situations in response to which China targets international businesses with punitive action, emphasize that foreign businesses in China and those that rely heavily on the China market run a risk of being targeted both because of their own corporate and employee actions and because of factors outside of their control, such as the actions of their home or foreign governments or politicians. This section begins with the rising importance of **National Security** in China, as this is a

[2] China has sanctioned entities not included in this report, including individuals and non-governmental organizations such as advocacy groups, for activities related to issue areas other than Taiwan, such as Human Rights.

feature of the current geopolitical landscape that drives Beijing's behavior and risk to companies in subsequent issue areas.

National Security

Issue Summary

The US and China are increasingly focused on national security challenges that intersect with the economy and business. Chinese Communist Party (CCP) General Secretary Xi Jinping almost certainly sees national security as of greater importance than economic development. Xi's administration stresses jointly planning for development and security, explaining that the latter is the "foundation" of the former. Critically, China's conception of "national security" is broadly defined, taking the preservation of the CCP's political power as the paramount priority while also accounting for more conventional threats (such as military threats) to the country. Xi's "comprehensive national security concept" urges the state to find and mitigate risk in every element of life, business, and government. From China's perspective, all sectors of business and industry could potentially harbor threats to the CCP and the nation. They are therefore the targets of increasing scrutiny. Foreign business is still highly valued, but security officials have been empowered to ensure that business does not occur at the expense of security.

Risk to Businesses

Beijing's national security concerns are driving compliance risks posed by changing legislation and regulatory regimes. This is similar to developments in other countries, but China's often ill-defined regulations and laws give authorities broad powers to take action against nearly any behavior (actual or perceived) that allegedly violates those laws or endangers the state. The lack of an independent judiciary and the opacity of the legal environment further heightens the uncertainty posed to businesses, and increases the risk of seemingly arbitrary enforcement. The almost certain prioritization of national security over economics in China is currently driving changes in what specific business practices and topics are acceptable, and which may give rise to politically motivated consequences (see **Human Rights** and the Mintz Group case). In addition to risks to companies as a whole, national security concerns are also very likely to drive higher levels of risks to corporate leaders and employees in China if they or their company is perceived to be involved in any activities potentially hostile to Beijing's interests.

The examples below illustrate the actions China has taken against international businesses in efforts to mitigate national security risks. These cases highlight the following risk types: **Cyberattack, Law Enforcement Action**, **Product Ban**, and **Regulatory Action**.

- In May 2023, Capvision, an international consulting firm, was accused of illegally obtaining information deemed sensitive by Chinese authorities from expert networks in CCP, government, and defense industry organizations. Its offices in multiple Chinese cities were subject to **Law Enforcement Action** in the form of raids. Company personnel were questioned and "articles" — almost certainly including documents and computers in the raided offices — were inspected.

Consulting firms will reportedly pay for information from ex-government officials and industry insiders. While expert networks — including Capvision's — have been applauded by Chinese state media for helping the economy in previous years, the rising power of the national security apparatus and expanding national security and counter-espionage laws signal Beijing's decreasing tolerance of their activities.

- Lotte Group subsidiaries and their websites were targeted in **Cyberattacks** in 2017, including defacement and distributed denial-of-service (DDoS) attacks, by state-linked actors and likely hacktivists after Lotte Group agreed to provide land on which the South Korean government would deploy a Terminal High Altitude Area Defense (THAAD) battery. Lotte Group businesses in China were also targeted in **Regulatory Action** through investigations of alleged fire safety and tax violations as early as December 2016, after it became known the company was in talks with the South Korean government. Between December 2016 and March 2017, 87% to 90% of Lotte Marts in China were closed, and by 2019 Lotte Group began seeking an exit from the country.
- After Bloomberg reported on the financial assets of Xi Jinping's family members in June 2012, the news outlet and data provider faced a **Product Ban**. The company's website was blocked in China, its data services stopped being purchased by state-owned enterprises, and Bloomberg journalists' residency visas were delayed or denied. The New York Times has reportedly faced similar consequences over its publications. The family of the lead reporter on the Bloomberg story also reportedly received death threats.

Businesses operating in or selling to the China market are also targeted as China manages threats wholly unrelated to business activities. National security issues between China and the home governments of international companies — and even third-party governments — can have sudden impacts. For example, the Australian government called for investigations into the origins of COVID-19 in 2020. Almost certainly as a punitive measure, China subsequently imposed heavy tariffs and an **Embargo** on products from Australia such as barley, red meat, wine, and coal, almost certainly negatively affecting the businesses and industries dealing in these goods. The import restrictions on Australian coal, timber, and beef were fully lifted between late 2022 and mid-2023. It is likely that other import restrictions will also be lifted in 2023. In another example, almost certainly to more broadly hurt the South Korean economy after Seoul agreed to host the aforementioned THAAD battery, China banned travel agencies from arranging trips to Korea. South Korean entertainers and products such as TV shows were also subject to **Product Bans**, being barred from the Chinese market. Additional examples are available in the **Territorial and Sovereignty Disputes** section below.

Human Rights

Issue Summary

In recent years the US government, other governments, and various international non-governmental organizations have increasingly criticized China's human rights record. China's intensified suppression of civil liberties and democracy in Hong Kong caused great concern among the international community in 2019, for example. The most prominent issue, however, is Chinese authorities' treatment of Uyghur and other ethnic minorities in the Xinjiang Uyghur Autonomous Region, which an August 2022 United Nations report asserted "may constitute … crimes against humanity". Among other abuses, Uyghurs and

other groups are almost certainly subjected to forced labor related to factory, textile, and agricultural production, mass detention, and mass surveillance. Some governments, including the US government, have called China's actions in Xinjiang genocide.

Risk to Businesses

Risks to international businesses exposed to China's human rights record, and specifically the situation in Xinjiang, are multifold. Most prominently, companies must navigate export and import restrictions by the US and other countries aimed at curtailing China's practices and avoiding forced labor products. Businesses and brands outside of China must also contend with name-and-shame efforts by international consumers if their supply chains touch Xinjiang. Corporate leaders from The Walt Disney Company reportedly admitted that the movie Mulan (2020) led to "a lot of issues" after international consumers discovered parts of it were filmed in Xinjiang.

Yet international businesses that seek to mitigate human rights concerns risk **Boycott**, **Product Bans**, and potentially **Law Enforcement Action** in China. For example, H&M, a Swedish multinational retailer, issued a statement in March 2021 to say the company was "deeply concerned" by forced labor and other allegations in Xinjiang. The statement further vowed that H&M did not work with garment factories in Xinjiang, and that its practices for sourcing cotton would no longer rely on Xinjiang. Beginning with social media posts, consumers in China subsequently called for a **Boycott**. H&M also faced a **Product Ban** in which H&M stores were removed from e-commerce platforms and mobile map applications. As a result, the company reportedly lost $74 million USD.

The response to H&M was likely stoked by state authorities; according to reporting in the Wall Street Journal, CCP propaganda authorities had discussed how to respond to companies making "improper" statements about Xinjiang in February 2021. They reportedly heard suggestions from scholars and advisors that "pressure [against companies making statements about Xinjiang] should come from the public and industry, not the government". A month later, the first social media posts targeting H&M appeared on social media and were amplified by CCP accounts and state media outlets. After approximately a year and a half, H&M returned to some e-commerce platforms. Companies, including H&M through a subsequent statement, which try to straddle the line to appease both international and Chinese sensibilities have also been publicly shamed.

Law Enforcement Action is another risk. China has warned due diligence firms against Xinjiang supply-chain investigations. Xinjiang human rights issues have likely intersected with **National Security** concerns (discussed above) in at least 1 case, resulting in a law enforcement raid in March 2023 against the Beijing office of Mintz Group — a US corporate investigations company. Authorities detained 5 local employees, and the company has since reportedly vacated its Hong Kong offices. According to a Reuters report, a Singaporean executive at the company was also placed under an **Exit Ban**.

Technology Competition

Issue Summary

The US government is actively seeking to maintain its leading global position in science and technology on the grounds that stronger technology means greater national prosperity and security. China's leaders also recognize the critical importance of technological innovation on the same grounds and have bent their nation's industrial policies toward rapid advancements in cutting-edge fields. The result is a technology race, wherein the US is particularly concerned about China's military modernization, reliance on foreign technology acquisition and intellectual property theft, and the notion that American entities are supporting China's strategic goals through investment and other activities. US export controls, reshoring legislation, sanctions, and other measures, coupled with China's own self-sufficiency efforts, stringent data security regulations, and other actions, have created a situation in which the 2 countries are "decoupling" in certain sectors. Given the US's partner-based approach to ensuring China is unable to overtake the US as a global leader (in technology and more broadly), the competition is global in scope.

Risk to Businesses

In this competition, international businesses face rapidly changing technology and data restrictions and import and export controls. The result is a significant uncertainty in the market that makes long-term planning difficult. The specific requirements and restrictions can almost certainly create additional costs for businesses or place the revenue streams of businesses in certain sectors at risk, such as for Nvidia and Micron Technology in the semiconductor industry. China's pursuit of domestic advances and investment in key technologies also creates increasing competition that affects market share and talent retention.

Beyond ever-changing regulatory regimes and market competition, Beijing's approach to managing the global technology rivalry and threats to Chinese companies also includes targeting international businesses with **Product Bans**. China's response to US efforts to prevent the adoption of Huawei and ZTE technologies, particularly 5G technologies, in Europe and elsewhere — an issue of **National Security** from the US's threat perspective — highlights this risk type. In 2021, China warned — via embassy communications and CCP-affiliated media — that a decision by Sweden and other European countries to ban Huawei could negatively affect the development of Swedish telecommunications company and Huawei competitor Ericsson. Ericsson's revenue from China reportedly dropped from approximately 10% to 3% of the company's total revenue — a loss of more than $400 million USD — in the year after Sweden banned Huawei and ZTE equipment from 5G networks, following which Ericsson's share of Chinese telecom tenders also fell. The losses reportedly prompted Ericsson to restructure and scale down its operations in China.

The 2023 case of Micron Technology, an American semiconductor firm, also highlights how Beijing uses **Product Bans**. In March 2023, an office of the Cyberspace Administration of China (CAC) launched a security review of Micron Technology and subsequently banned procurement of Micron products for

critical information infrastructure projects in China. The exact reason for the review and ban is unclear, but there was likely a political element to the decision, based on the lack of details regarding the security flaws, limited scope of the ban, and other factors. The CAC asserted that Micron products presented "relatively serious network security problems and dangers", but the ban does not appear to order the removal of Micron products from existing critical infrastructure. The analyses of Chinese observers have suggested alternative explanations, including that the ban could have been a preemptive action to drive critical infrastructure toward domestic alternatives before future US restrictions cut off access to more technologies, or that it may have been informed by Micron's support of US policies restricting American semiconductor technology exports to China. Regardless, the ban will very likely reduce (but not eliminate) Micron's potential revenue from the China market.

Territorial and Sovereignty Disputes

Issue Summary

China has territorial, resource, or maritime boundary disputes with many of its regional neighbors, including Japan, South Korea, India, Vietnam, and the Philippines. Disputes in the South China Sea — where Chinese authorities claim several million square kilometers of sea area — as well as those with Japan over the Senkaku (Diaoyu) Islands in the East China Sea, and others along the China-India border, have led to repeated incidents of varying intensity — such as protests, physical confrontations, and cyberattacks and intrusions — since 2010. Although not a claimant in any of these disputes, the US is involved in the South China Sea and East China Sea as a perceived champion of "peace and stability" in support of Japan and others as well as for its own interests, which has led to several military-to-military encounters between American and Chinese forces. The politics of Hong Kong, Tibet, and other Chinese territories are other sources of potential conflict, but Taiwan's contested sovereignty as a province of China or an independent country carries even greater risk. The CCP almost certainly continues to prefer a peaceful solution, and Insikt Group assesses that an amphibious invasion and occupation of Taiwan in the near term (before 2027) is not likely. However, the risk of other uses of force by China against Taiwan (such as a blockade) is very likely increasing gradually.

Risks to Businesses

International businesses could have to contend with disrupted supply chains and endangered property, operations, and personnel if a high-end or prolonged conflict — which could involve military, diplomatic, mass protest, or other activity — erupts. Many of China's disputes fall along highly trafficked maritime shipping lanes, and Taiwan contributes significantly to the global economy, particularly in the technology sector. Use of force on the island (such as a missile bombardment or cyberattack) would very likely lead to heavy disruptions to business operations and loss of company assets depending on the location and nature of the attack. An invasion would almost certainly have the same impact on an even larger scale. Companies must also consider reputational and brand damage that could affect their market share in other participants to a conflict (such as in Vietnam or China) and elsewhere in relation to their response to a given conflict. For instance, companies that decided to remain active in Russia in spite of the war in Ukraine have been subject to name-and-shame reporting and calls for **Boycott**.

Outside of a kinetic conflict, China's methods for rectifying businesses whose intentional or unintentional actions — or those of its employees or affiliates — run afoul of Beijing's view on these territorial and sovereignty disputes also pose particular risks. The selection of brief examples below highlight the following risk types: **Boycott**, **Regulatory Action**, and **Sanctions**.

- Lockheed Martin; Raytheon Technologies; and Boeing Defense, Space, and Security; their subsidiaries; or executives have all been subject to **Sanctions** multiple times by the Chinese government for arms sales to Taiwan, most recently in 2022 (Boeing) and 2023 (Lockheed and Raytheon).
- In an example of **Regulatory Action**, authorities in 5 Chinese localities investigated subsidiaries of Far Eastern Group, a Taiwan-based multinational firm accused of financially supporting Taiwanese "separatists", in November 2021. Authorities discovered alleged violations related to environmental safety, land use, product quality, and taxes, resulting in fines totalling $74.4 million USD.
- In October 2019, after general manager of the Houston Rockets Daryl Morey expressed support for pro-democracy protests in Hong Kong on his personal social media, the Houston Rockets and the National Basketball Association (NBA) — whose commissioner subsequently expressed support for free speech — became the target of a **Boycott**. The Chinese Basketball Association stopped cooperation with the Houston Rockets, sports broadcasters in China stopped streaming NBA games, and the NBA's China sponsors ended their relationships with the association. According to NBA commissioner Adam Silver, the controversy cost the league "'hundreds of millions of dollars' in revenue".
- A similar dynamic — in which the non-work activities of business personnel can create risks for companies — was also seen in August 2019 after the Civil Aviation Administration of China banned certain Cathay Pacific flight crew from flying into mainland China for allegedly participating in the Hong Kong protests. Other **Regulatory Action** was taken against Cathay Pacific, such as requiring the airline to obtain pre-approval from mainland authorities for all crew members who would fly to mainland China or pass through mainland Chinese airspace. The company further faced calls for a **Boycott**, with prominent state-media outlets reportedly publishing headlines such as "The Four Sins of Cathay Pacific".
- In January 2018, Marriott International was subject to a **Product Ban** from the CAC. The US hotelier and lodging firm was ordered to shut down its website and online reservation portal for a week in January 2018 after a customer survey by the hotel chain "seriously violated [China's] national laws" by listing Tibet, Taiwan, Hong Kong, and Macau as separate countries.
- Muji, a Japanese retailer, was subject to **Regulatory Action** when the company was fined more than $31,300 USD in May 2018 for using packaging that listed Taiwan as the "country of origin", allegedly violating China's advertising laws.

Authorities in China also target wider swathes of the business world for decisions made by their home or foreign country governments or politicians in some cases. The selection of brief examples below highlight the following risk types: **Cyberattack, Boycott,** and **Embargo**.

- After then-Speaker of the US House of Representatives Nancy Pelosi visited Taiwan in August 2022, 7-Eleven convenience stores, Taiwan Power Co. — a state-owned electricity provider — and other government and transportation services were targeted in retaliatory **Cyberattacks** likely conducted by hacktivists. Just before Pelosi arrived, China also suspended food imports of numerous Taiwanese companies, thereby implementing a de facto **Embargo**.
- When then-Speaker of the Czech Parliament's Senate Jaroslav Kubera planned to visit Taiwan in 2022, China's embassy in Prague reportedly sent a letter to the president of Czechia stating that "Czech companies whose representatives visit Taiwan with Chairman Kubera will not be welcome in China or with the Chinese people", and that "Czech companies who have economic interests in China will have to pay for the visit to Taiwan by Chairman Kubera". Kubera died before visiting Taiwan, and Senate President Miloš Vystrčil made the trip instead. After a second visit in the same year by a separate official, at least 1 company named in the Chinese embassy's letter, piano maker Klaviry Petrof, had a $23.8 million USD order from a company in China canceled — a likely instance of **Boycott**.
- After Taiwan established a Taiwanese Representative Office (TRO) in Lithuania in November 2021, China Customs reportedly removed Lithuania from its "list of origin countries", effectively placing an **Embargo** on Lithuanian exports. Compared with the year prior, China's imports of Lithuanian products dropped by 91%, affecting a broad range of industries. Further, China reportedly urged multinational firms in other countries to cut Lithuania from their supply chains; Continental AG (Conti), a German automotive company, had its imports to China blocked because they were produced in Lithuania. An April 2022 publication by Lithuania's State Security Department reportedly asserted that **Cyberattacks** from China increased following Lithuania's acceptance of the TRO, though it is unclear if businesses were the target of these attacks. Although still only a fraction of what it once was, China-Lithuania trade began climbing in approximately Q2 2022.
- Philippine fruit producers and exporters were negatively affected after China subjected pineapple, banana, and other fruit imports from the Philippines to an **Embargo**, almost certainly as part of a territorial dispute. China began a first round of import restrictions on bananas in March 2012, a month before initiating a standoff over Scarborough Shoal — a contested atoll in the South China Sea. Starting in May 2012, other fruit imports received greater scrutiny over claims the shipments contained invasive insects, reportedly slowing customs clearance. Likely hacktivists also targeted the Philippine News Agency, a university, and a government department in **Cyberattacks**, including defacement attacks.

Mitigation Strategies

First and foremost, international businesses that might perceive their economic activities as separate from national politics, security, and defense must reexamine how their operations could be viewed from an adversarial and political perspective. The specific activities of a given company, the topics it works on, and how the results of its work might support perceived "anti-China" activities should all be considered in a comprehensive risk assessment. Underlying China's response to challenges in each of the issues areas outlined above — **Human Rights**, **Technology Competition**, and **Territorial and Sovereignty Disputes** — is Beijing's approach to managing **National Security**.

For the majority of risks identified in this report, including the special risks born from the 8 types of actions seen in Beijing's toolkit for managing geopolitical challenges — **Cyberattack**, **Boycott**, **Embargo**, **Exit Ban**, **Law Enforcement Action**, **Product Ban**, **Regulatory Action**, and **Sanctions** — the level of impact to normal business operations and revenue opportunity is related to the level of a given business's dependence on supply chains in China and reliance on (or hopes in) the Chinese market. The impact of other risks, such as those related to changing laws and the potential for disruptive conflict over territorial or sovereignty disputes, can also depend on the level of exposure to affected shipping lanes, air routes, and the markets of non-China participants (such as the US or Taiwan).

To avoid and mitigate the potential impact of risks created by the behavior of authorities in China and patriotic hacktivists, as well as other risks associated with global geopolitical competition, international businesses should develop **Monitoring**, **Diversification**, and **Resilience** strategies. In doing so, companies should strive to overcome potential siloes between parts of their business — such as operational and cybersecurity leadership, legal teams, strategy groups, and human resources departments — to holistically address emerging concerns.

- **Monitoring** — Businesses should constantly monitor the domestic and international landscape as it pertains to China and their operations. Through in-house teams or partnerships with threat intelligence companies such as Recorded Future, businesses should strive to stay informed of not only legal and regulatory developments, but also political and public sentiment developments that may forecast shifting interpretations of existing laws and regulations and other potential threats. Where possible, specific sets of warnings and indicators should be tailored to individual businesses for each of the risks discussed in this report.

- **Diversification** — Businesses should diversify their supply chains and markets. While China will almost certainly remain an important element of businesses' activities in the long-term, decreasing reliance on the country should mitigate potential losses from geopolitically motivated risks. As part of diversification, companies in sectors heavily affected by changing regulations and export controls should consider developing China-specific product lines that address China's industry needs without violating outside restrictions (from the US, for example). Nvidia, for instance, has reportedly begun producing a slightly lower-performance graphics processor as an "alternative" product for the Chinese market to replace revenue lost due to US export restrictions on its more advanced chips.

- **Resilience** — With their specific conditions in mind, businesses should develop comprehensive crisis management plans with playbooks for addressing each risk type identified in this report. In many cases, such as with **Cyberattacks**, these plans will likely overlap with existing crisis management measures. Moreover, businesses should develop clear channels for communicating warning indicators of risk or explicit risk developed or spotted by the aforementioned monitoring team. Warning indicators (if and when available) should be used to begin initial crisis management preparedness before major risk events occur.

Appendix A

Table 1 lists instances of companies or industries exposed to or targeted by Beijing's response to geopolitical concerns. It is not an exhaustive list of all such instances. As stated in the report, many, but not all, of these instances are retaliatory in nature, caused by a particular company's actions or the actions of its home or a foreign government. More details can be found in the sources provided or the case summaries in the report.

Target	Year(s)	Issue Area	Risk Type	Sources
Capvision Partners (Shanghai) Corporation Limited	2023	National Security	Law Enforcement Action	1, 2, 3
Mintz Group	2023	National Security	Law Enforcement Action; Exit Ban	1, 2, 3
Bain & Company	2023	National Security	Law Enforcement Action	1, 2
Micron Technology	2023	Technology Competition	Product Ban	1, 2, 3, 4, 5, 6
Lockheed Martin	2023 (Most Recent)	Territorial/ Sovereignty Dispute	Sanctions	1, 2
Raytheon Technologies Corporation	2023 (Most Recent)	Territorial/ Sovereignty Dispute	Sanctions	1, 2, 3
Boeing Defense, Space, and Security	2022 (Most Recent)	Territorial/ Sovereignty Dispute	Sanctions	1, 2
Taiwanese Industry	2022	Territorial/ Sovereignty Dispute	Cyberattack; Embargo	1, 2, 3, 4
H&M Group	2021	Human Rights	Boycott; Product Ban	1, 2, 3, 4, 5
Lithuanian Industry	2021	Territorial/ Sovereignty Dispute	Embargo	1, 2, 3, 4, 5
Continental AG (Conti)	2021	Territorial/ Sovereignty Dispute	Embargo	1, 2

Ericsson	2021	Technology Competition	Product Ban	1, 2, 3, 4, 5, 6
Far Eastern Group	2021	Territorial/ Sovereignty Dispute	Regulatory Action	1, 2, 3
Klaviry Petrof	2020	Territorial/ Sovereignty Dispute	Unspecified Threats; Boycott	1, 2, 3, 4
Australian Industry	2020	Other (COVID-19)	Embargo	1, 2, 3, 4, 5, 6, 7, 8
Dell; Microsoft; Samsung; Arm	2019	Technology Competition	Unspecified Threats	1
Houston Rockets; National Basketball Association	2019	Territorial/ Sovereignty Dispute	Boycott; Product Ban	1, 2
Cathay Pacific	2019	Territorial/ Sovereignty Dispute	Regulatory Action; Boycott	1, 2, 3
Marriott International	2018	Territorial/ Sovereignty Dispute	Regulatory Action	1
Muji	2018	Territorial/ Sovereignty Dispute	Regulatory Action	1
Lotte Group	2017	National Security	Cyberattack, Regulatory Action	1, 2, 3, 4, 5, 6, 7, 8, 9
Korean Industry	2017	National Security	Product Ban; Other (Travel Restrictions)	1, 2, 3
Bloomberg	2012	National Security	Product Ban, Other (Intimidation)	1, 2
Japanese Industry	2010	Territorial/ Sovereignty Dispute	Other (Export Restriction)	1, 2, 3, 4
Philippine Industry	2012	Territorial/ Sovereignty Dispute	Embargo; Cyberattack; Other (Travel Restrictions)	1, 2, 3, 4, 5, 6

Table 1: *Instances of companies and industries exposed to geopolitically driven risk*

Recorded Future®

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture