REPORT

BEYOND THE GREAT FIREWALL

Analyzing the Impact of Chinese Espionage Laws, Cyber Threats, and IP Theft on International Business Operations

CHIEF EDITOR Karna McGarry

FIRST LINE EDITOR Michael Searway

CONTRIBUTING AUTHORS Chad Kunkle, Linneu Salles, Nicholas Nemtuda, Ryan Barnett

MESSAGE FROM THE CEO

In today's increasingly interconnected world, the competitive landscape for global business is evolving faster than ever. With these rapid changes, there is likewise a rapid increase in threats posed by emerging cyber risks and state-sponsored espionage, particularly from nations like China.

The recent amendments to Chinese espionage laws present unprecedented risks & challenges to companies operating in the global marketplace, with vulnerabilities extending far beyond traditional cybersecurity. These developments are not just regulatory changes but represent a tangible threat to employees and operations across the region.

KRIS COLEMAN
FOUNDER & CEO, RED5

It is my privilege to introduce our latest whitepaper, ***Beyond the Great Firewall***, where our analysts explore the far-reaching impact of Chinese espionage laws, cyber threats, and intellectual property theft on international business operations. In this paper we highlight examples of threats that have materialized, including high-profile raids on U.S. firms and exit bans affecting key executives.

Our commitment to navigating these challenges for our clients is unwavering. We are actively reassessing our strategies and enhancing our risk management protocols to ensure the safety of clients and the integrity of our operations. It is crucial that we stay informed and agile in this evolving environment.

K. Coleman

TABLE OF CONTENTS

ABOUT RED5

ABOUT US

Our purpose is to ensure bad things don't happen to good people. We leverage our depth of expertise and capabilities to deliver security and risk management services that protect clients from both known and unknown threats.

The excellence of our entire team is driven by robust and diverse backgrounds across agencies, the private sector, and public sector organizations. Red5 consists of individuals who are recognized within their networks for solving problems others couldn't. We establish strong partnerships with our clients to ensure safe and successful results.

WHAT WE DO

Red5 provides comprehensive managed service solutions for threat monitoring, privacy, and intelligence services.

We're always there to protect you, even when you don't notice. Our analysts use industry-leading intelligence tools and best practices to give you expert-led **security intelligence, threat monitoring**, and **privacy solutions**.

5 CORE TENETS

- **Confidentiality**
- **Authenticity**
- **Responsiveness**
- **Rigor**
- **Agility**

Executive Summary

Headlines about a 'new Cold War' between the United States and China can be found nearly everywhere in 2024, from specialized international affairs journals to mainstream newspapers and even pop culture blogs. The reality is that Chinese threats to U.S. enterprises–both at home and abroad–are more pronounced as China seeks to gain the advantage.

Corporate security executives should be prepared to protect against the following key threats emanating from China:

- A Chinese law presents both financial and physical threats to foreign businesses in China, **including corporate raids and exit bans.**
- **Cyber attacks** from China are likely to be more disruptive in nature and target critical infrastructure, whereas previously they were focused on obtaining sensitive information.
- The Chinese government will continue to seek the **intellectual property and trade secrets** of foreign companies by any means necessary to give State-Owned Enterprises a competitive advantage.

TRAVEL & BUSINESS OPERATIONS IN CHINA

Chinese law presents both financial and physical threats to foreign businesses in China, including corporate raids and exit bans.

The Chinese government in early 2023 passed an amendment to a law meant to defend against foreign espionage. The amendment gave the Chinese government broader controls over data and data collection activities, which made many standard business practices, such as acquiring data on market conditions and on other actors in the industry, a crime.

The amendment presents financial and physical threats to U.S. businesses operating in China, including both employees and executives, as the Chinese government has demonstrated willingness to use force against potentially violative entities.

Shortly after the amendment was passed, Chinese law enforcement raided several U.S.-based companies operating in China, targeting companies in the due diligence or consulting fields.

This included firms such as Bain & Company, Capvision, and the Mintz Group. During the raids, five employees from the Mintz Group were detained.

The Chinese government stated reasons for these raids were allegations of bribery and collecting and disseminating confidential information, including state secrets. Chinese officials have also stated that they would take action against U.S. companies in response to actions that conflict with Chinese interests, such as those related to Taiwan, TikTok, and the Xinjiang province.

Corporate raids are not the only concern for U.S. executives and employees operating in China. Exit bans are a common tactic employed by the government, and while it usually does not involve placing the target in custody, it does prevent individuals from leaving the country.

Even when executives are permitted to leave, executives may be **harangued and even interrogated** by government officials before their departure.

- On April 12, 2024, the U.S. State Department issued a Level 3 travel advisory (Reconsider Travel) for mainland China, specifically highlighting the "arbitrary enforcement of local laws, including in relation to exit bans, and the risk of wrongful detentions," reiterating a March 2023 advisory with the same stipulations.
- Two recent high profile cases involving corporate executives include the bans placed on Michael Chan, from the U.S.-based firm Kroll, and on investment banker Charles Wang Zhonghe, from the Japan-based Nomura. Both of these individuals were based out of Hong Kong, but were denied exit from mainland China after traveling there in 2023.

Like the corporate raids, the given reasons for these actions are often related to alleged financial crimes or spying, but tend to resemble retaliations for past slights against the Chinese state. These 'slights' might include comments made on controversial topics, connections with dissidents, actions regarding Taiwan, or arrests of alleged Chinese spies in the target's home country.

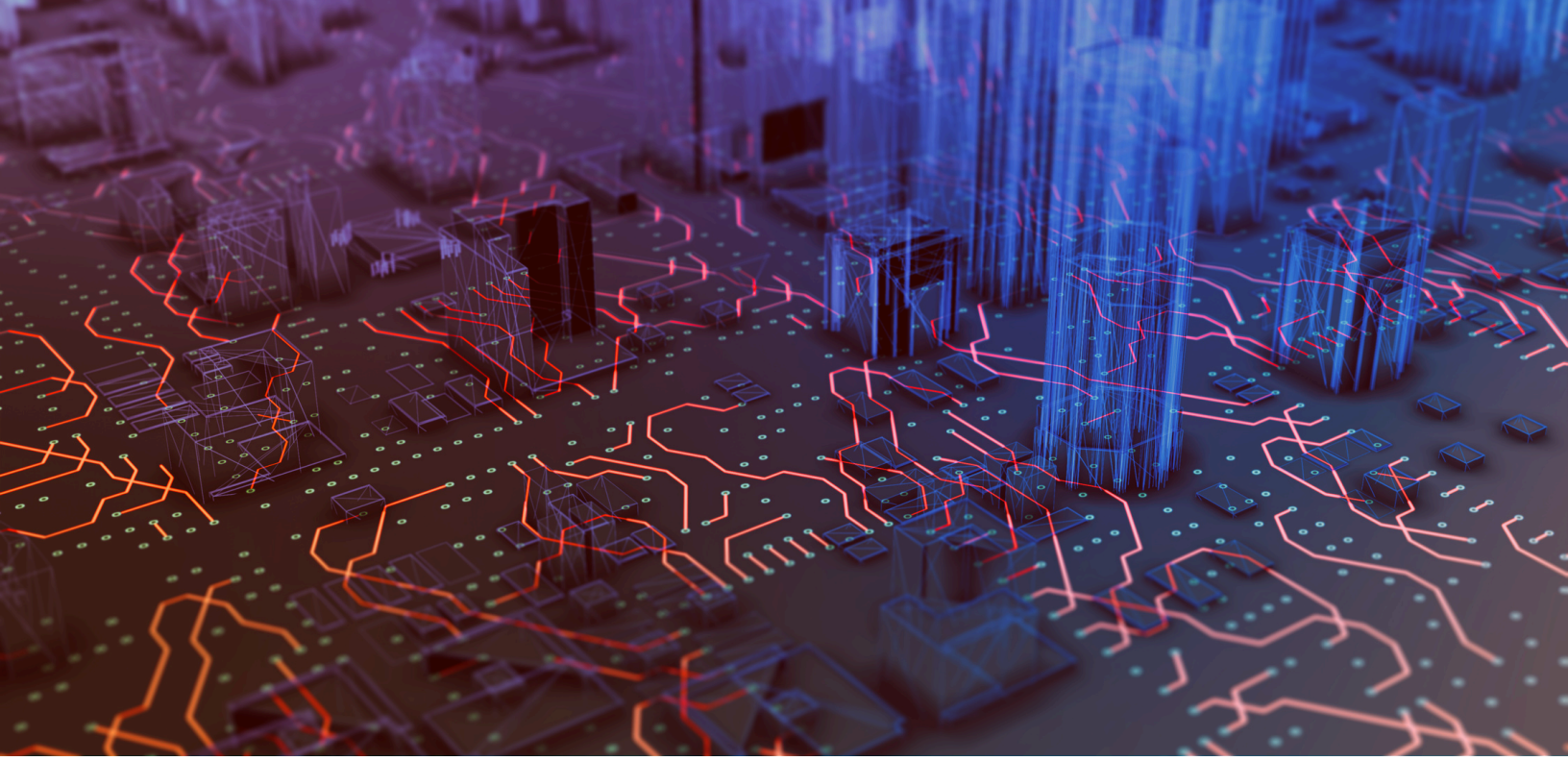
In some cases, the Chinese government has engaged in 'prisoner swap' type negotiations with other countries, allowing the individuals held by the exit ban to leave if that individual's home country releases an arrested Chinese citizen.

The chilling effect that these tactics have had on foreign investment

An 8% decrease in 2023, and additional drops in early 2024

President Xi Jinping met with many U.S. executives in San Francisco during his visit in November 2023 and hosted executives for a meeting in Beijing.

It remains unclear if the investment decline and actions by the U.S. government will cause the Chinese government to truly reverse course in the long term, as tensions between the U.S. and China escalate, and China continues to seek economic partnerships elsewhere.



CHINESE DISRUPTIVE EFFORTS IN THE U.S.

Previous cyber attacks from China focused on obtaining sensitive information; new threats are likely to be more disruptive in nature and target critical infrastructure.

China has previously focused its cyber attacks primarily on obtaining sensitive information from intellectual property to state secrets but there may be a shift in focus by the Chinese towards critical infrastructure.

Critical infrastructure is a broad category that encompasses everything from communications and transportation to water and power. A mass outage in several key sectors could, for example, be used to spread damage, confusion, and panic across the U.S. either to sow confusion ahead of Chinese military action in Taiwan or in an effort to cause some level of instability in the U.S.

CHINESE DISRUPTIVE EFFORTS IN THE U.S.

Compounding this threat, many organizations in this space are 'target-rich, cyber-poor,' meaning they have limited IT budgets and related cyber capabilities needed to defend against disruptive threats.

- CISA (Cybersecurity & Infrastructure Security Agency), the NSA, and the FBI reported in February that 'Volt Typhoon,' a China-backed hacking group, had infiltrated the networks of critical infrastructure providers and operators - with access going back at least five years.
- U.S. government agencies and their partners have been able to find and shut down a number of these intrusions, but CISA Director Jen Easterly warned in April that they were "just the tip of the iceberg."

"[Chinese-manufactured technology] can capture wide swaths of data or remotely disable or manipulate connected vehicles."

***- Secretary of Commerce Gina Raimondo**, highlighting a potential threat from China as part of this initiative.*

China's cyber campaigns will likely involve new technologies as well. The U.S. Department of Commerce in February 2024 launched an investigation into the potential vulnerabilities and risks of the ICTS (Information and Communications Technology and Services) supply chain for connected vehicles.

China-backed groups will continue to use conventional networks and methods of intrusion to penetrate critical infrastructure providers and operators.

The Biden Administration, in March 2024, announced an indictment of seven Chinese hackers associated with the group known as APT31 or **'Judgment Panda,'** revealing that the actors sent over 10,000 malicious emails to a host of targets; which appeared to be from prominent news outlets or journalists and contain legitimate news articles.

The hacker group, Judgment Panda, campaign took place over years, and focused on cyber-espionage targeting government and political officials.

The U.S. Department of Justice (DOJ) noted that *"dozens of companies operating in areas of national economic importance"* were also among the targets, including firms in:

- IT
- Telecommunications
- Manufacturing
- Trade

As with the Volt Typhoon campaign, the indicted APT31 hackers are merely the tip of the iceberg–or rather, multiple icebergs–that infrastructure operators and partners will need to be wary of going forward.

IP THEFT

The Chinese government will continue to seek the intellectual property and trade secrets of foreign companies by any means necessary to give state-owned enterprises a competitive advantage.

China views innovation and the economic achievement of SOEs (state-owned enterprises) as a top priority, and their success as a prerogative of the government to facilitate. China sees SOEs as an extension of the state, a view that justifies the use of extraordinary measures to ensure SOEs can outperform competitors globally.

Taking this a step further, China typically considers the economic development of SOEs as a national security concern, which creates a pathway for government entities to utilize additional resources to achieve market dominance by any means necessary.

IP THEFT

The government engages in a host of preferential economic practices to strategically ensure SOEs can dominate the domestic market before expanding internationally.

A particularly serious threat is the loss of IP (intellectual property). The Chinese government will continue to seek the IP and trade secrets of foreign companies by any means necessary to give SOEs a competitive advantage and pursue this through two broad methods.

Methods of IP Theft

The first, and more efficient, method of IP theft is through regulations requiring foreign corporations to enter business partnerships with a Chinese business entity, or manufacture a certain percentage of a product domestically, in order to operate within China. Once this agreement is entered, the Chinese business is obligated by law to provide the government with sensitive information upon request.

This information is then used by SOEs to dominate the domestic market and expand internationally. This method is often used against companies in fields of emerging technologies, where companies look to expand into new markets and are burdened with R&D costs. The Chinese competitors are able to undercut the original developer globally, as an SOE has no requirement to recuperate initial R&D costs.

It's important to be aware of all methods of IP threats that can happen to you or your business. Make sure you have the right tools to be prepared for any threats that may come in.

Methods of IP Theft Continued

The second broad method of acquiring IP and trade secrets is the outright theft of information, typically accomplished by illegal intrusion into a foreign company's network or human intelligence sources.

China regularly engages in government-sponsored economic espionage to steal:

- IP
- Trade secrets
- Data
- Valuable information

There is little that can be done by international organizations and governments to prevent or punish China from targeting foreign companies operating within its borders. China operates a large network of human intelligence sources around the world with the intent to steal sensitive information firsthand or through an intermediary.

IP THEFT

Intelligence agencies target disgruntled employees that work within sensitive offices of desirable companies, and may offer to buy information or intimidate or coerce targets into providing it.

The level of IP theft risk a firm may be exposed to generally correlates with China's desire to onshore certain industrial and technological capabilities. Some industries face a higher risk than others, such as technology, agriculture, and defense.

Technology companies are usually targeted the fiercest, as their innovations can be applied across multiple industries and markets.

For example:

- U.S. Attorney General Merrick Garland announced charges of theft of trade secrets in March 2024 against Linwei Ding, a Chinese national and Google employee.
- Ding was accused of stealing trade secrets associated with Google's development of AI, which he allegedly planned to use at his China-based startups, according to DOJ reports.

- In May 2021, the DOJ charged multiple Chinese nationals in APT 41 for their role in a multi-year, multi-target IP theft campaign targeting companies in energy, pharmaceutical, and manufacturing sectors.
- The group exfiltrated hundreds of gigabytes of IP from companies based in North America, Europe, and Asia, according to a May 2022 CBS News report.

- In 2020, the DOJ announced charges of racketeering conspiracy and conspiracy to steal trade secrets against Huawei and several of its subsidiaries.
- The DOJ alleged Huawei stole trade secrets from U.S. companies, including original source code and other IP, to drastically reduce its R&D costs and delay times.

RISKS IN EMERGING MARKETS

Chinese telecom providers are heavily engaged in technology markets worldwide, creating many potential cyberspace vulnerabilities due to the extensive use of Chinese telecommunications hardware that could potentially be accessed by Chinese state actors.

Through a combination of private sector innovation and state financial support, Chinese telecommunications providers, such as Huawei and ZTE, have become heavily engaged in technology markets worldwide.

These investments in developing markets have become a key component of the Digital Silk Road (DSR) initiative, alongside other sectors such as cloud computing, mobile payment systems, 'smart cities,' and artificial intelligence.

The cost-effectiveness of Chinese equipment and solutions, coupled with ultra-competitive pricing and state-subsidized financing, have enabled Huawei and ZTE to become the dominant actors in many markets across both regions.

- Huawei is one of the main 5G infrastructure providers for Latin America's two largest markets, Brazil, and Mexico. Huawei experienced a 10.9% increase in equipment and cloud service sales in Latin America in 2023.
- During the same period Huawei's two main regional competitors, Nokia and Ericsson, experienced a 14% and 3% decline in sales, respectively.
- Huawei has provided up to 70% of Africa's IT infrastructure. Together, ZTE and Huawei have likely built at least 40 telecommunications networks in over 30 countries across Africa.
- Nine African countries have acquired 'safe city systems' from Chinese suppliers, which enhance government surveillance, among other functions.

China's extensive penetration into developing telecommunications and technology markets creates many potential cyberspace vulnerabilities.

In 2020, a Chinese state-owned telecommunications provider allegedly used equipment based in the Caribbean to send signaling messages to mobile devices owned by U.S. citizens, enabling the surveillance of possibly thousands of overseas travelers.

These vulnerabilities underscore the many dangers raised by the penetration of Chinese equipment and services in digital networks worldwide, especially in developing regional markets.

Given the variety of products sold by Chinese telecommunications providers in these markets, it is likely that local state-sponsored communications networks include some amount of Chinese technology - and may be compromised.

For private individuals and enterprises, these risks can be reduced by either limiting what type of information is transmitted in such networks, or by avoiding them altogether and opting for third-party telecommunications providers that are not associated with Chinese corporations.

OUTLOOK

China’s aggressive posture towards foreign businesses–especially U.S. corporations–is unlikely to abate in the next 3-6 months. The risks discussed in this whitepaper are broad risk categories and a firm’s exposure to them will depend on its location, industry, supplier ecosystem, and other factors.

One consistent theme is China’s willingness to use both official tools and state-backed threat groups to achieve its economic and security objectives. China's willingness to use every tool at its disposal will likely increase if tensions between the U.S. and China intensify.

Corporate security and intelligence teams should be watching closely for potential escalations, especially over the major flashpoints of the Taiwan Strait and the South China Sea.

How Red5 Can Help

Escalating global security trends highlight the need for corporations to be well-informed of the unique threats they face, which are multiplying in an increasingly uncertain and unstable world.

Red5 analysts leverage their in-house expertise to proactively monitor the global threat space to remain well-informed, decipher ambiguous security challenges, and produce tailored and actionable security solutions for our clients. Our analysts use industry-leading intelligence tools and best practices to give you expert-led managed security intelligence, threat monitoring, and privacy solutions.

Managed Intelligence & Analysis

- Expert-led monitoring, analysis, and insights
- Flexible investigations and reports, adaptable to changing needs and risks
- Monitor for threats across mainstream and alternative social media

Managed Threat Monitoring

- Remove fake or impersonation accounts
- Dark web surveillance for compromised credentials
- Geofenced monitoring of location-specific threats

Managed Privacy Solutions

- Understand the full-picture of your digital footprint and how to minimize risks
- Remove your personal information as quickly as its bought, sold, and shared with WebScrub
- Protect against common attack tactics, hacking attempts, scams, and spam

GET IN TOUCH TO LEARN MORE


red5security.com/contact-us


info@red5security.com