CHINABRAND®
International Consulting

WHITEPAPER

Legally Compliant Defense Against Chinese Industrial Espionage

CHINABRAND IP CONSULTING GMBH
Grashofstrasse 3 ▪ 80995 München ▪ +49 89 32 12 12 800
info@chinabrand.de ▪ www.chinabrand.de

The Growing Threat of Industrial Espionage

Increasing geopolitical decoupling between China and Western countries fundamentally changes the conditions for internationally operating companies. While China reduces its dependence on the West through economic policies and technological self-development, foreign companies operating in China face a dual challenge: they must adapt their business models to meet regulatory requirements and simultaneously implement protective measures against targeted industrial espionage. This particularly affects companies with unique technological features or innovative solutions in sectors like automotive, mechanical engineering, biotechnology, and information and communication technology.

Chinese industrial espionage mainly occurs through two methods: digital attacks and personal networks within companies. While espionage attacks in Germany are primarily conducted through remote access, espionage activities in China predominantly involve direct personal information acquisition. This happens through infiltrated employees, negotiation partners, or networks involving research institutions, authorities, and state-supported enterprises.

The Chinese economy is undergoing fundamental structural changes. The desired economic upgrade from a production-oriented economy to a high-tech and innovation-driven economy increases the demand for advanced know-how. Although China already leads in many sectors, it still relies heavily on Western knowledge in strategic technologies such as industrial automation, biotechnology, and high-performance materials. This intensifies the need to find alternative ways to acquire these technologies—including unethical methods such as industrial espionage.

Legal Framework

To protect against industrial espionage, companies must not only take technical and organizational measures but also comply with China's complex legal framework. The tightened Counter Espionage Law of 2023 significantly expands the definition of espionage. Previously limited primarily to military and state secrets, espionage now encompasses economic and technological data. Companies must therefore be particularly cautious when handling security-critical information or sharing it with headquarters outside China.

Besides the Counter Espionage Law, the Cyber Security Law (CSL) with its Multi-Level Protection Scheme (MLPS 2.0) and the Data Security Law (DSL) are crucial for security strategies in China. Companies must ensure their IT infrastructure meets local regulations, and specific data cannot be transmitted abroad without authorization. Violating these laws can result in high fines, operational bans, or inclusion in the Corporate Social Credit System, causing significant business consequences.

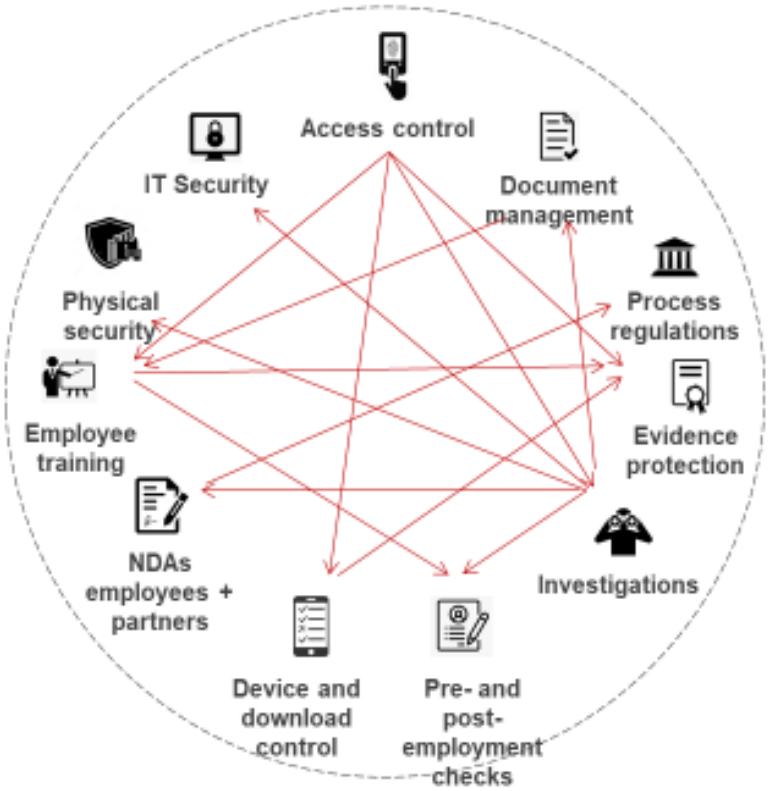
Systematic Espionage Defense

Defending against industrial espionage requires a systematic, integrated approach based on thorough risk analysis. Companies must address key questions:

- Which data and technologies require particular protection?
- Which espionage methods are relevant (digital attacks, personal infiltration, social networks)?
- Where are potential vulnerabilities in IT and organizational structures?
- Which legal and regulatory restrictions must be considered?

A significant portion of espionage activities in China occurs through local networks and clusters. For example, Ningbo is a center for valve production, while Changsha is known for

tunnel drilling technology. Companies in these sectors should expect targeted attempts by Chinese competitors to access their know-how. Espionage often happens in several stages, beginning with the acquisition of business information and supplier relationships, followed by targeted extraction of technological details. Effective defense strategies must therefore consider all stages of information procurement.



Integrated Know-how Protection System

Implementation of a Defense System

A comprehensive espionage defense system consists of several elements:

- **Technical Protective Measures:** Identity & Access Management (IAM) systems for data access control, multi-layered encryption technologies, and data movement logging. However, companies must note that certain encryption technologies are restricted under Chinese Encryption Law, prohibiting full encryption of some security-critical data.

- **Organizational Measures:** Companies should strictly regulate internal information flow, especially concerning external business partners and employees. Critical technologies should ideally not be fully accessible in China but divided into individual components that are worthless without central control.

- **Physical Security Measures:** Many espionage activities occur through physical access. Strictly controlled access and authorization systems are essential, especially in research facilities and production sites, where tamper-proof areas should prevent unauthorized access to sensitive components.

- **Strategic Compliance Adjustments:** Adjusting the Information Security

  Management System (ISMS) to Chinese regulations is vital. This requires close coordination between IT security, corporate management, and compliance departments both locally and at headquarters.

Future-Proof Security Strategies

To remain resilient against industrial espionage, companies must embed security measures into an integrated overall concept rather than viewing them in isolation. A key aspect is the global compliance strategy: Companies must ensure their security frameworks comply not only with Chinese but also with European and international regulations, necessitating close collaboration across various locations and departments.

Another crucial element is employee training. Many espionage attacks use social engineering or covert recruitment within companies. Regular employee awareness and training significantly reduce this risk.

Increasing the use of artificial intelligence in espionage defense is gaining importance. AI-driven anomaly detection can help companies proactively identify potential attacks and implement countermeasures early, particularly valuable in defending against cyber-attacks.

China remains an attractive market, but the risks of industrial espionage require high vigilance and adaptability. Companies acting proactively and continuously optimizing their security strategies can effectively safeguard themselves from espionage impacts without violating Chinese regulations. Close integration of technical innovation, organizational security, and legally compliant implementation is critical to effectively protecting the company and maintaining competitiveness.

For Further Informations

For more Informations about our services, please visit:

www.chinabrand.de

Contakt und Feedback

info@chinabrand.de

Blog | LinkedIn

Grashofstraße 3, 80995 München - +49 89 321212800 - www.chinabrand.de