



## IRIS Report

# Commercial Espionage: The Threat from Chinese Cyber Attacks

## Executive Summary

---

Intelligence-led, business-driven

## Invictis Risk Intelligence Service Report

# Commercial Espionage: The Threat from Chinese Cyber Attacks

## Executive Summary

The following is an executive summary of the full IRIS report which contains an assessment and analysis of the threat from Chinese cyber attack including details on key organisations and target sets, together with recent summaries of assessments from both the FBI and MI5. The full report contains information on specific vulnerabilities and security issues together with recommendations and conclusions.

### **Invictis Risk Intelligence Service – IRIS**

The Invictis Risk Intelligence Service - IRIS - provides sector specific commercial, geo-political and cyber threat insights that inform information security and risk management strategy. The service comprises three elements and equally applies to organisations seeking to understand the threat and risk landscape faced by existing business units as well as to planned operations in new territories prior to market entry.

---

## Intelligence-led, business-driven

---

# Commercial Espionage: The Threat from Chinese Cyber Attacks

## Executive Summary

- Despite denials by Beijing, Chinese commercial espionage is as much a state-sponsored activity as their military and civilian operations.
- The Chinese government supports commercial espionage as a necessary economic activity to help create Chinese commercial advantage and strategic success in the 21<sup>st</sup> century.
- As a result, the Chinese commercial espionage effort is targeted, well-funded, aggressive and overt.
- It is estimated that in excess of 2M people are either direct or indirect employees of the Chinese intelligence services.
- Beijing has at its disposal an army of computer hackers, immigrants (resident in target countries), intelligence operatives, scientists and students.
- In 2010 China had an estimated 457M Internet users, according to the China Internet Network Information Centre, more than the combined populations of the US and Japan.
- This army operates in an integrated intelligence architecture carrying out systematic targeting of operations against carefully defined commercial, government, industrial and military information.
- It is therefore no surprise that in the US, the FBI now regards China as the primary threat to security from electronic espionage.
- The Chinese commercial espionage attack uses a multitude of techniques:
  - Human intelligence assets, including placing interns in target companies
  - Corporate entities and front companies established and controlled by the Chinese government
  - Open-source intelligence collection operations
  - Carefully targeted cyber-attacks that involve data theft of intellectual property
- On Mainland China there is a concerted effort to collect intelligence involving thousands of full time government employees operating from numerous departments, offices and provinces.
- Cyber intelligence collection is managed in China by two government entities - the State Council and the People's Liberation Army (PLA) - operating under the control of Beijing.

---

## Intelligence-led, business-driven

- 
- China also has a non-traditional intelligence capability, allowing clandestine operations to be conducted (by definition deniably) outside the envelope of the official intelligence services.
  - The two intelligence services (which target intellectual property and technology) are the Ministry of State Security (MSS) and the Military Intelligence Department (MID), also known as the Second Department of the PLA General Staff.
  - However, much of China's clandestine 'unofficial' intelligence collection is independent of these services.
  - China supports a widespread and comprehensive clandestine intelligence collection attack through numerous government-controlled research institutes and military-industrial companies.
  - The State Council directs technology acquisition efforts through the Ministry of Science and Technology (MST).
  - The PLA's military research and collection effort is channelled through the International Studies Research Centre (ISRC).
  - The clandestine state-sponsored attacks are much more comprehensive than those directly operated by the intelligence services – permitting state deniability.
  - It is through these clandestine 'unofficial' operations that many Chinese hacking groups are directed at specific targets and subsequently rewarded or paid for stolen information.
  - The PLA actively recruits nerds and geeks to create their cyber-army and since 2000 has been rapidly developing its computer network exploitation and attack (CNE/CNA) capabilities.
  - By 2007, Jonathan Evans, the Director-General of the UK Security Service, MI5, warned the CEOs of banks and legal firms that the Chinese government was targeting them with cyber-attacks over the Internet.
  - The Chinese have developed advanced and custom exploitation software to hack into financial and legal companies' networks to steal confidential information. Such attacks are coupled with social engineering techniques.
  - In the case of external cyber attacks, the techniques and tools used are fairly consistent. There are however numerous variations in both payload and the vulnerabilities exploited.
  - Law firms are a very attractive target for cyber attack by anyone seeking sensitive information, according to the Cyber National Security Section in the FBI's Cyber Division: "Law firms have tremendous concentrations of really critical private information," and breaking into a firm's computer system "is a really optimal way to obtain economic and personal security information."
  - Targeted online attacks have increased significantly for Hong Kong's retail sector with more than 40% of Hong Kong-based retail industry respondents admitting their firms had experienced a cyber attack.

---

## Intelligence-led, business-driven

- The severity of the impact according to the respondents ranged from very inconvenient and financially damaging (36.2%), to extremely inconvenient and financially damaging (10.5%).
- According to the survey: "Only 7% of respondents expressed a high level of confidence that their current security solutions are capable of coping with new e-mail and Web threats. What is more alarming is that fully 43% were only moderately confident and 6.4% had no confidence at all."
- On Nov. 17, 2009, the FBI issued an alert warning that law firms and public relations firms were being targeted in a new round of organised cyber attacks. According to the FBI, the attackers were intruding into individual computers using a tactic known as "spear-phishing."
- The threat to a law firm in Hong Kong dealing with confidential issues of IP is therefore likely to be of considerable commercial interest to the cyber-army of China.
- Cyber-attacks on law firms without adequate security procedures and protocols are likely to give rise to issues of legal liability.

---

## Intelligence-led, business-driven

### **Informed Security**

Invictis take an objective intelligence-led, business-driven approach to Information Security, delivering comprehensive product-agnostic services that identify, orientate, benchmark and manage risk.

Invictis understand both the challenges and opportunities that come with the effective storage, transmission and use of an enterprise's key asset - its information. And with a threat spectrum that is constantly evolving, the importance of securing information without impact to legitimate operations.

### **Confidential Proprietary Information**

This document contains proprietary and confidential information of Invictis Information Security Limited protected by law. It is made available only under the terms of a signed agreement to business partners and clients of Invictis Information Security Limited. A person viewing this document must be authorised within the scope of such an agreement to do so and accepts that:

- Other than for the expressly permitted purposes covered by such an agreement, no part of this document may in any form or manner be reproduced, displayed, distributed or the confidential proprietary information contained in it disclosed or made available to unauthorised parties without the written permission of Invictis Information Security Limited.
- Use of this document other than for the purposes described in the agreement is prohibited.

Return of any copy of the whole or part of this document may be required at the request of Invictis Information Security Limited and any unauthorised use or disclosure of the information contained in it restrained by law.

The information contained within this report has been obtained from sources believed to be reliable, however, Invictis disclaims all warranties to the accuracy, adequacy or comprehensiveness of this information. Invictis shall have no liability for errors, omissions or inadequacies of the information contained within this report or for interpretations thereof. The opinions expressed within the report are subject to change at any time and without notice.

---

## Intelligence-led, business-driven

### **Invictis Information Security Limited**

Southgate Chambers, 37-39 Southgate St, Winchester, SO23 9EH United Kingdom

**Telephone:** +44 (0)845 177 0654 **eMail:** [info@invictis.com](mailto:info@invictis.com) **Web:** [www.invictis.com](http://www.invictis.com)