China's Growing Spy Threat

Maxim Worcester

January 2014

Executive Summary

Beijing denies it. Much of the world ignores it. But according to officials familiar with the matter, the People's Republic of China (PRC) operates the single largest intelligence-gathering apparatus in the world. While the current debate regarding espionage is firmly focused on the NSA, the public and some companies have forgotten that China and Russia are the real threat to companies and not the intelligence agencies of the West who are mainly focused on the fight against international terrorism and organized crime. China, on the other hand, can devote much greater resources to spying on the private sector and is not hindered by the same laws and public controls that govern the activities of Western intelligence agencies. It is becoming ever clearer that China reverts to corporate espionage when it is unable to buy or license technology from Western companies or Governments.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented and is above party politics.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, bringing major opportunities but also risks, decision-makers in enterprises and politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, economy, international relations, and security/ defense. ISPSW network experts have worked – in some cases for decades – in executive positions and possess a wide range of experience in their respective specialist areas.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

ANALYSIS

The Sheer Size of the Problem

Determining the size and strength of China's intelligence services is no easy task. The byzantine nature of the Chinese government and the penchant for secrecy in the intelligence community in general virtually assure that news about Chinese intelligence services are frequently inspired as much by fiction as by fact. Still, it is widely accepted that the Ministry of State Security (MSS), the main agency tasked with foreign and counter-espionage, employs around one million people. Additionally, the Domestic Security Department (DSD), a branch of the Ministry of Public Security (MPS), has developed a network of informal agents throughout China that *the Telegraph* estimates to be 39 million strong. Finally, the People's Liberation Army (PLA) has considerable intelligence capabilities in its four service branches, seven military regions as well as in some of its general departments.

Admittedly, opinions differ about how well the size of China's intelligence services translates into strength. A lack of central coordination and parallel structures in civilian and the military intelligence are one source of inefficiency. Another is the fact that lean management structures are still an anathema to much of the Chinese bureaucracy. Finally, extracting actionable intelligence from raw data has to be complicated by the amount of data generated by these extensive intelligence networks. However, these inefficiencies and challenges pale in comparison to the sheer vastness of the abundance of resources that are available to the Chinese intelligence services. As General Michael Hayden, the former head of the CIA and the NSA, stated in a recent interview 'As an intelligence professional, I stand in awe at the breadth, depth, sophistication and persistence of the Chinese espionage campaign against the West'. Moreover, China's intelligence capability is arguably augmented by the greater freedom it enjoys in its use. Aside from the lack of democratic accountability, one important factor is that international terrorism, which has dominated the agenda of intelligence services in the USA, Russia, the UK and France and tied up their resources, has yet to have a significant impact on China.

This has one important implication for European companies operating in China: While corporate espionage ranks fairly low on the list of priorities for most other intelligence services, Chinese intelligence service can devote much greater resources to spying in the private sector.

The Chinese Rationale for Corporate Espionage

Three reasons make the proposed allocation of resource within the Chinese intelligence services likely. First, there is a tradition of lax intellectual property rights (IPRs) in China. While economists disagree about the current net-effect of China's treatment of IPRs, the important role corporate espionage in particular has played in the economy's success in recent decades makes it unlikely that the Chinese government and, by extension, its intelligence services will abandon their activities in this field. Secondly, while it is true that China is currently shifting from copying innovation to becoming truly innovative, the slowing economic growth in China makes leapfrogging expensive development steps by "acquiring" the necessary technology all the more tempting. Here, the availability of a wide and sophisticated network of agents within and beyond the borders of China is an important asset. Finally, as Chinese economic growth is slowing, government austerity becomes a looming prospect. One way for the intelligence services to fend off unwanted budgetary scrutiny is to make a genuine contribution to economic prosperity – through the use of corporate espionage.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Thus, General Hayden's conclusion that '[in China] industrial espionage by the state against relatively vulnerable private enterprise is a commonly accepted state practice' seems valid. The coincidence of means and motive for corporate espionage in China is particularly problematic for European companies, as they generally tend to produce highly sophisticated products. Not only does the resulting reliance on innovation make them a target for corporate espionage. The successful production of said products also requires a greater transfer of knowledge to the producing country, i.e. China, which greatly facilitates corporate espionage.

The Chinese Aviation Industry – A Case Study

While the aforementioned arguments apply to most innovation-led businesses, the aviation industry is arguably most at risk when it comes to corporate espionage. The main reason for this is the Chinese government's plans for its domestic aviation industry.

According to the *China Daily*, the government has set itself the goal of breaking the duopoly of *Airbus* and *Boeing* by securing at least 5% of the domestic market by 2020. The two aircraft that are meant to meet this target, the *Comac* ARJ21 and *Comac* C919, have both been plagued by set-backs. To start with, a host of design flaws have delayed approval by the *Civil Aviation Administration* (CAA) for the AJ21, caused mainly by flaws in the wing design. Recent reports by *Aviation Week* also suggest that *Comac* has largely abandoned the use of composite structures in the C919, which would make the C919 airframe little more advanced than that of the Airbus A320 or Boeing 737. Similar delays and difficulties are expected with *Comac`s* larger ambition: to start delivering a 160-seat narrow-body aircraft by 2016. From a Chinese perspective, there is thus a very real risk that, by the time the aforementioned aircraft enter service, Airbus and Boeing will offer products that make them look obsolete.

How will China react to this set back? Li Xiaojin, professor at the Civil Aviation University of China, provides a revealing answer: 'Chinese manufacturers have no experience of building such commercial aircraft and they have to look for new solutions to every problem they meet'. In other industries, the Chinese learned first-hand from the actual OEMs: Volkswagen for automobiles, Cisco for telecommunications, Bombardier for high-speed trains. Through joint ventures they trained, learned and copied their way to innovation. Since *Comac* is not receiving the same "help" from Airbus or Boeing, Li Xiaojin seem to suggest that they should rely on corporate espionage instead.

The Chinese Way of Corporate Espionage

The Chinese intelligence services rely on a mixture of signal and human intelligence (SigInt/HumInt) – much like their counterparts in the western world. What makes them unique, however, is their approach to intelligence gathering: Chinese intelligence services complement their cadre of professional agents with a vast network of informal contacts. Abroad, sources are recruited among the often sizable Chinese expat community. Also, the students, workers, businessmen and academics that live temporarily outside of China are frequently contacted during their stay or interviewed upon their return to China. Domestically, the DSD and the MSS maintain extensive networks that reach down to virtually every hamlet and, more importantly, into every aspect of a foreign company's presence in China.

Another important difference, at least with respect to its western counterparts, are the vast powers granted to the security services and the poor protections of individual freedoms in China. These powers allow the Chinese

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

intelligence service to use aspects of tradecraft more freely that would be heavily curtailed elsewhere: bribes, blackmail, venus traps, etc. Yet, the most important distinguishing feature of the Chinese way of corporate espionage is the way in which means of gathering HumInt is combined with cyber-attacks – a technique generally called Social Engineering.

Social Engineering in China

Social engineering, in essence, involves tricking people to subvert a network`s security, for example by clicking on to a link, opening an infected document or plugging a USB stick into their computer. The social engineer will spend a great deal of time and effort in designing said link, document or USB stick to appear perfectly genuine. Moreover, he or she will use all available information to create a pretext to allay any suspicions the victim may have. For example, he or she may engage in dumpster diving, going through a person's garbage to collect information, or create false profiles and befriending the victim on social media sites like Facebook.

Of course, social engineering is not unique to China. Yet, the resources available to the country's intelligence service and their extensive networks at home and abroad allow them to make much greater use of the technique – with considerable success. What makes social engineering so appealing for the Chinese intelligence service and so dangerous for its targets is the fact that, compared to SigInt, it is relatively cheap and does not require great technological sophistication. More importantly, targets often do not realize that they have been the victim of an attack. Sources generated through social engineering, therefore, tend to be very valuable for the intelligence services, but all the more devastating for the affected companies: The sustained loss of information crucial to a company`s competitiveness eventually endangers its survival. Thus, social engineering not only helps Chinese companies by providing them with vital information on their competitors, in the long term, it also eliminates said competition.

What Can Companies Do Against the Threat of Social Engineering?

Before addressing any specific countermeasures, it is important to acknowledge two "truths" about corporate espionage in China:

<u>It is very important to be judicial in determining what information needs to be kept secret.</u>

The resources used to protect information are scarce and, when spread too thinly, their overall effect is negligible. Most people accept this argument with respect to financial resources but tend to overlook that it also applies elsewhere. For example, employees are less likely to follow strenuous data protection regimes if the information in question does not seem to merit such measures. A measured approach to the classification of information also seems to be warranted due to the resources and reach of the Chinese intelligence services.

<u>Social engineering is not a problem that can be addressed by technological means.</u>

Most of the time, agents do not target IT systems but rather their users to gain access to a company's information. Indeed, many companies are so focused on their IT systems and processes that they overlook the human factor involved in information protection. Faced with overly complex and over-reaching IT regulations, employees are more receptive to outsiders offering them "solutions". Thus, it is unfortunately true that computers do not reveal secrets, their users do and no technical solution can protect an employee from being duped by a professional social engineer.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

So, what can a company do to meet the challenges posed by social engineering?

1. **Training**
   Any successful approach has to start with its employees, specifically their training! Workshops teaching how to recognize and avert social engineering attacks are an excellent first step. These workshops should take place regularly and should not be limited to managerial staff and employees send to China should receive intensive training prior to their deployment.

2. **Information**
   Those responsible for information security or tasked with handling such information need to be up-to-date on new developments and emerging risks.

3. **Policies**
   Another essential step is a thorough review on the existing policies aimed at protecting information. Here, it is more important to cut unnecessary, overly burdensome and over-reaching processes than to add new ones. Without employees "embracing" and "living" the processes codified in it, a company's information protection policy is not worth the paper it is written on.

4. **Structure**
   An important tool in defending companies against social engineering attacks is the use of a whistleblower system. Employees have to be able to voice concerns about information security – anonymous if necessary – outside of the usual chain of command.

5. **Technology**
   While technology alone cannot meet the challenges posed by social engineering attacks, it has a role to play in making a company more resilient against them. Vital information, for example, should always be kept on stand-alone systems, encryption software should be readily available and easy to use and defense mechanisms like firewalls need to be kept up to date.

6. **Countermeasures**
   At times, employing countermeasures can be a very effective way of detecting ongoing and preventing future social engineering attacks. Such countermeasures can include the use of disinformation which is leaked in order to confuse the attacker and sow doubt as to the reliability of intelligence and agents.

***

Remarks: Opinions expressed in this contribution are those of the author.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

About the Author of this Issue

Maxim Worcester is Managing Director of German Business Protection GmbH (GBP), a Berlin based Security Consultancy. GBP is a subsidiary company of KÖTTER Security. In the past he worked, amongst others, for the Economist Intelligence Unit, Frankfurter Allgemeine Zeitung, Control Risks and KPMG.

Maxim Worcester

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de