Chapter 91
Cyber Espionage and Illegitimate Information Retrieval

Roland Heickerö
Royal Institute of Technology (KTH), Sweden

ABSTRACT

One of the most serious threats to a modern country's trade, industry and long-term economic development is cyber espionage and insiders. The activities are directed against high-technological industries and companies with advanced basic research. The defence and telecoms sectors are of particular interest, just as biotechnics, medical and material technology. Behind this kind of espionage there may be individual states and security services as well as competing companies. One trend is that criminal players are getting involved both as thieves and fences of information. Computerisation and the development of the Internet drastically increase the possibility of procuring sensitive information through illegal means. This can be done in different ways. In the paper the convergence between industrial- and cyber espionage are discussed. A number of examples are provided of different kinds of espionage as well as some of the methods that is used to collect information over the Internet – such as signals intelligence, monitoring of traffic, penetration and overtaking of computers with the aid of trojans. Examples are given on succesful cybertheft operations such as the operation Buckshot Yankee and the Chinese Ghostnet. The paper ends with a discussion on how to improve information security in organisations in order to reduce the risks for illegitimate information drainage.

The difference between espionage in the traditional sense and industrial espionage is marginal. Both are conducted in similar ways and with the same methods, although targets may differ. In principle, this is the world of organised theft of information. Most countries and companies look for information on their opponents and competitors. Even friendly nations and companies can be of interest. Using open source information is legal and in no way controversial. It is part of the game. The problem lies in the transition from what is legally acceptable to criminal behaviour. The dividing line can be related to what methods are used, whether ethical guidelines are broken in order to acquire information and whether the

DOI: 10.4018/978-1-5225-7909-0.ch091

measures violate the laws of a country or not. Different nations have different legal systems; an activity can be viewed as criminal in one country, but be legal in another.

This paper discuss the development of cyber espionage in a broad sense, examples are given on methods to be used in order to collect information. The paper ends with a short discussion on how to protect an organisation from illegitimate information gathering.

GENERAL

Industrial espionage is relatively cheap compared to investments in advanced research and development. According to an estimate by the FBI, industrial espionage in 1992–1993 cost more than 120 billion U.S. dollars in lost contracts and R&D expenses. The number of lost jobs was assessed to be 6 million (Lyle, 1999). Later estimates have figures of more than 200 billion U.S. dollars annually, in the United States alone. In Canada the cost of illegal information collection is estimated at more than 12 billion dollars per year (CBC News, 2005).

In 2009 the information security company Symantec conducted a survey in order to analyse the amount of information stolen, and the cost of it. A total of 2,100 companies in 27 countries participated in the study. The result showed that all the companies that participated had lost important information; in 92 percent of the cases it had led to great costs. Each information theft cost an average of nearly 2 million dollars (Danielsson, 2010).

Espionage can be sanctioned at national level and/or be part of an individual company's strategy to gain competitive advantages. In some cases third parties are used for the actual information collection, for instance a criminal organisation or a company. One of the most serious threats comes from insiders. They may be planted in an organisation by a security service or the like. An insider can also be an employee who has been recruited to conduct a specific task. His or her motivation may be financial or personal, such as dissatisfaction with the work situation and a desire to cause the company harm. People can also be bought, bribed, blackmailed or forced to hand over vital information. A player can manipulate a person into handing over secret information without understanding the consequences his/her actions, who is actually behind the operation or why it is conducted. Referring to ideology, patriotic, ethical and/or sentimental reasons are viable tools for recruitment.

After the end of the Cold War there was a drastic increase in industrial espionage. One reason may be that many security services were forced to change concentration after the fall of the Berlin Wall and adjusted to a new situation. Today it is not necessarily military capacity that is the decisive means of pressure between regions and states; economic strength is just as important. Industrial espionage is also very lucrative with great payback on invested capital. It is a tempting activity. If an operation is discovered it is often legally very hard to tie the actions of individuals to a security service from a specific country, for example. In some cases the interests of a regime coincide with those of a company, in other cases a company may act as a proxy and a cover for an operation. It is important to stress that industrial espionage is in no way limited to enemies; it can also be conducted between friendly nations and companies that are not seen as competitors.

Advanced technology can be acquired through industrial espionage, technology that can be used to build up industrial capacity and speed up development of products. A country that is technologically less developed can use a structured and conscious long-term collection campaign for sensitive informa-