University of Wales

Robert Kennedy College

Master of Business Administration

INDUSTRIAL ESPIONAGE – A MANAGEMENT PERSPECTIVE

EYSTEIN HANSSEN

September 2008

DECLARATION

This dissertation has not previously been accepted, nor is being concurrently submitted in candidature for any degree. It is being submitted in partial fulfilment of the requirements for the degree of MBA.

It is the result of my own independent investigation, except where otherwise stated. Sources are acknowledged by explicit references.

I hereby give my consent for this dissertation, if accepted, to be available for photocopying, inter-library loans and for electronic access, and for the title and summary to be made available to outside organisations.

Date 13.09.2008

Acknowledgements

The process of writing this piece has been, I suppose, like most other dissertations: challenging and fulfilling – but at times a lonely journey. I owe three individuals a sincere thank you for their support. First and foremost Gabriel Jacobs, my supervisor, for his constructive criticism and help to stay on track. Secondly my dad, Asbjørn Hanssen, for reading through the piece at an early stage and giving me valuable feedback from a retired academic's perspective. Finally, all my love and thanks to my partner Tonje Bentzen, for her read-throughs and critical opposition from a social anthropologist's view, and for putting up with endless nights with me incommunicado in front of the MacBook.

CONTENTS

1. ABSTRACT

This thesis develops an understanding of the main leadership and strategic challenges resulting from the threat of industrial espionage.

The research has been carried out as a desk study. Arguments build on academic writing on industrial espionage and related topics, literary accounts of former spies, reports and news articles from the public record. My angle has been to extract and present a management perspective.

The *raison d'être* for industrial spies is finding and obtaining information. The drivers for industrial espionage are different for a business, a state or an individual. Businesses spying on other businesses will have competitive or economic motivations; an individual can have cultural, personal, as well as economic motivations; a state often has political- or security-related motivations (chapter 4).

Foreign intelligence agencies pose a real and continuous threat to high-tech companies. France, for instance, openly admits, essentially, to spying. Other countries known to be active are all EU-countries, plus Russia, China, Taiwan, South-Korea, Israel, Japan and the US (chapter 4).

The USA is a prime target for industrial espionage because it is the technology leader in most fields. The Anglo-Saxon intelligence system *Echelon* sweeps for transmissions globally, providing the member states with huge amounts of information which can be utilised to acquire trade secrets and strategic information for commercial purposes (chapter 4).

A proper and realistic evaluation of the risk of becoming a target of industrial espionage is instrumental in assessing the threat level, the level of vulnerability and the potential consequences for a targeted organisation (chapter 5).

Company culture has a considerable impact on a business's ability to avoid becoming a target. Managers need to acquaint themselves with that risk, the companies' vulnerabilities, and the methods used by industrial spies, and consequently implement

preventive approaches within the company culture. Leaders must communicate clearly; contextual ambiguity can create huge strategic losses caused by unaware employees, and an insecure working environment (chapter 6).

The line between legally collected business intelligence and illegally obtained information can be blurred, but once the information is at hand, most businesses are likely to use it regardless of its origin and draw benefits from its strategic value (chapter 6).

The threat of industrial espionage is constantly changing, and handling this continuously changing environment effectively calls for contingency-based leadership. Successful industrial espionage attacks leave an organisation in a state of crisis; here crisis leadership-theories present relevant approaches (chapter 7).

Entrepreneurs are particularly vulnerable as their technology might not be patented, but they still need to show or publicise parts of their inventions in order to attract funding (chapter 7).

The cyber sphere has grown into one of the most important areas of information collection for spies. Focus on information security is therefore a key priority. Organisations will also benefit from analytical organisational approaches allowing for adequate risk assessments, raising cross-organisational awareness about the threat level (chapter 8).

Leaders must acknowledge that the threat of industrial espionage is a constant factor in contemporary business life. The openness of the globalised information age creates new opportunities for industrial spies. Intelligence operators performing acts of industrial espionage are highly skilled professionals (chapter 9).

2. METHODOLOGY

The subject of this thesis is industrial espionage; specifically how industrial espionage influences the management of an organisation. My main research question is:

What are the main leadership and strategic challenges resulting from the threat of industrial espionage?

In order to present a useful, current perspective, I believe the following questions will help clarify my main research question:

What are the principle characteristics of industrial espionage?

What constructive approaches are available for companies towards the threat of industrial espionage?

The main research question and the two sub-questions will cover the most important problem areas when facing the threat of industrial espionage; prevalence, who are the important players, the methods of industrial spies, the key leadership implications and how to approach the threat effectively.

I am aware that the standard way of approaching an MBA thesis is to gather primary data, for example by questionnaires or interviews. For this thesis, however, I decided to opt for a traditional desk-based research approach. There are two principal reasons for this decision. First, the subject is by its very nature a secretive one, such that questionnaires or interviews would not have yielded a great deal of useful information. Second, and on a related point, in order to gather primary data for a subject such as this one, it would have been necessary to have a series of close contacts, which I do not have, willing to share perhaps sensitive information. On the other hand, while in business literature as well as within the academic world there has been less focus on industrial espionage as opposed to the traditional economic, organisational and strategic areas, there

is a reasonable selection of literature that altogether makes for an adequate academic platform suitable for discussion. Relevant works are listed in the bibliography, and have been my primary source of information. In addition, the financial press writes continuously about industrial espionage, although the angle here is often the crime spectacular or the potential financial loss and subsequent law suits, rather than in-depth debate. Relevant sources are nevertheless, once again, listed as web sites in the bibliography. The Robert Kennedy College online library facilities have also been a useful resource. In terms of methods of searching information in the Internet, I have used several search-engines and cross-checked the respective findings.

3. LITERATURE REVIEW

Private businesses as well as government intelligence organisations have been involved in acts of industrial espionage for several hundred years. In the 1780s, during the early textile industry upswing in Britain, rigorous patent laws were passed to fight competitors from snatching each other's production secrets (Ferdinand and Simm, 2007). Mendell (2003, pp. 45-47) in his book portrays how the Union States managed to place a female observer, Mrs. E. H. Baker, inside one of the Confederate States' submarines, taking mental notes on firepower and technology. Later she sketched what she saw and conveyed it to the South States' Navy, providing key technological information. In another example, the much-used Sun Tzu's *The Art of War*, probably written more than 2,500 years ago in China, is a very early account of the importance of espionage. This book, now basic knowledge at military colleges, business schools or for anybody studying international politics, provides a whole chapter on *The Use of Spies*.

> "Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge." (Clavell, 1981: Sun Tzu, 500 BC, Chapter XIII, Section 4.)

Herring (1992, 13 (March/April) A) presents more recent examples of business intelligence gathering. In 1903 the Swedish banker Marcus Wallenberg hired the young Rolf Jolin to secretly gather information about the bank's customers and clients. In France, Jolin noticed the tight connections between French banks at its government intelligence services – and brought this idea home with him. In another parallel account from Japan, Herring (1992a) describes how the business intelligence operation run by Japanese corporation Mitsui before World War II was so effective it was actually used by the Japanese government for military purposes.

3.1. CORPORATE CRIME

'Corporate crime' – crime committed by corporations – is portrayed and discussed widely in business literature. Discussions about the driving mechanisms behind corporate crime are relevant when discussing industrial espionage, as the latter is a criminal act often committed by one corporation against another. In Clinard and Yeager's *Corporate Crime* (1980), an in-depth analysis of the prevalence of corporate crime among Fortune 500 companies is carried out. The authors present evidence of how corporate crime infiltrates interfaces between private businesses and public servants, examine ties between corporations and governments and furthermore discuss the ethical problems arising when capitalist interests collide with public interests. Clinard and Yeager define 'corporate crime' as "…any act committed by corporations that is punished by the state, regardless of whether it is punished under administrative, civil, or criminal law." (p. 16) This definition encompasses industrial espionage.

Corporations are entities of considerable economic, positional and political power. However, the drivers for corporate crime – or 'white-collar crime' – need not be entirely economic. Gobert and Punch (2007) discuss the motivations and intent of white-collar criminals. They point to positional power and corporate culture as key drivers for why individuals engage in white-collar crime. Three typologies of behaviour are described; white-collar crime committed with

> "I) an ostensible awareness of the criminal implications, II) an ostensible un-awareness of the criminal implications and III) where the contextual ambiguity in the law encourage offenders to believe or rationalise to themselves they are not engaged in illegal activities." (pp. 98-119)

This puts forward evidence that organisational and behavioural factors contribute to the likeliness of individuals engaging in corporate criminal activities. Furthermore, this is consistent with the finds published in a PriceWaterhouseCoopers survey (PWC 2007, p. 13): "an individual's opportunity, incentive and ability to rationalise his or her own actions are personal drivers for getting involved in economic crime activity."

Nasheri (2005, p. 7) argues there are two scenarios of motivation; disgruntled employees misappropriating trade secrets for their own financial benefit, or a competitor or foreign nation misappropriating trade secrets for its own financial interest (p. 7).

A further exploration of the mechanisms behind corporate crime argues that most capitalist societies consider it to be a regulatory crime, established by the society's elite as a less serious crime than street crimes (Michalowski and Kramer, 2006). Consequently leaders within elite circles of society are able to challenge regulatory laws with minimal – or at least less – risk of being prosecuted because there are strong ties between the economic and political powers.

The literature discussing corporate crime provides a coherent management perspective on the mechanisms relating to corporate crime, with emphasis on typical regulatory and financial crime, but less has been written about the managerial challenges stemming from industrial espionage. However, Ferdinand and Simm (2007) do focus on an organisation's external learning – what it acquires in the way of 'informational input' – and to what extent this can be derived from illegal sources. As we have established, some of the drivers for corporate crime will be identical to the drivers for industrial espionage, and there are other perspectives around motivation for, and how to relate to industrial espionage in an organisational and societal context that would benefit from further discussion. This dissertation will build its arguments on the observation than within a business perspective, the drivers and motivators for corporate crime are similar to the drivers for corporate espionage.

3.2. ESPIONAGE

The methods applied in industrial espionage are no different from those used by government intelligence agencies. Nasheri (2005, p. 32) discusses the shift in espionage-methods brought about by the information age and the globalisation of economies. Furthermore, the judicial aspects of the US Economic Espionage Act are discussed, exemplified by the continuous dilemma between increased global openness and the need to keep trade secrets. Nasheri also provides a useful, analytic coverage of the strategic ties between a nation's businesses and its government intelligence outfits.

The threat imposed by industrial spies is extensively covered in the current literature. Winkler (1997) focuses on risk and vulnerability aspects, emphasising the variety in which 'information' can occur, and subsequently the many avenues of attack available to industrial spies; a discussion of hands-on countermeasures is also presented. Cornwall (1992) focuses further on the craft and techniques of industrial espionage, providing a 'how-to' approach for anybody wishing to use industrial espionage techniques when collecting business intelligence. Contrasting the civil approach presented by Cornwall, a wide selection of rougher, professional espionage techniques is presented by Rustmann (2002) who portrays the operators originating from outfits like the CIA as more cynical, target-oriented and with less concern about ethics or human costs.

Penenberg and Barry (2000) describe in colourful detail industrial spies formerly employed by government spy organisations. They also put forward evidence of the particular vulnerability of entrepreneurs, while Perman (2005) draws the connection to professional espionage outfits, but with an overall focus on previous operator's commercial success in utilising Israeli military espionage inventions in technological start-ups. Mendell (2003), also with a threat-focus, centres on the practical sides of the security operative's challenges to limit the risk of industrial espionage attacks. He adds a further perspective of 'internal intelligence' – a system of surveillance of an organisation's own employees and activities (pp. 111-125).

A common categorisation of collection methods among the authors is, at a top level, overt and covert sources, and on the next level human intelligence – HUMINT, signals (communications) intelligence – SIGINT or ELINT and image intelligence – IMINT, (Cornwall, 1992, pp. 52-60; Rustmann, 2002, pp. 206 and 208; Nasheri, 2005, p. 23).

The literature covered in this segment can be categorised as 'spy-literature', with an operative focus on threat and countermeasures. The practical security advice offered is plenty, but it is aimed at security professionals rather than managers. Furthermore, there is less focus on organisational culture or ethics, and how these influence threat or vulnerability.

Overall a number of news-articles mainly from the *Financial Times* and the BBC, but also the *Wall Street Journal,* the *New York Times, The Economist* and *Aftenposten* are cited in this thesis as they provide valuable contextual references on current and previous incidents of industrial espionage, as well as insight into the perceived threat and ongoing debate in the global business community.

3.3. INFORMATION SECURITY

Within the scope of this dissertation, information security – subsequently information technology security (IT-security) – is a central area of discussion. SIGINT could by definition include interception of Internet traffic or theft of information from computers as these are digital signal streams; however the term 'computer hacking' or just 'hacking' is commonly used in the relevant literature (Cornwall, 1992, pp. 61-67, Nasheri, 2005, pp. 77-78, Rustmann, 2002, pp. 155, Winkler, 1997, pp. 83-87) as a separate method of intelligence gathering referring to the snatching of information via computers directly or through Internet connections.

An information security management system (ISMS)[1] represents an organisational, systematic approach to meet the threats to the availability, integrity and the confidentiality of an organisation's information (Calder and Watkins, 2006, p. 9). How information travels, and in what form, greatly influence the level of vulnerability: the risk of successful interceptions of strategic information. However, an opposite perspective on vulnerability is equally important: "What concerns us is the lifeblood of modern commerce: the free flow of information." (Mendell, 2007, p. 44). Information security involves the dilemma of imposing reasonable constraints upon business channels, without interfering with the business created by the free flow of information.

A further perspective is how the information age and the globalisation of business create new channels of industrial espionage opportunities. Nasheri (2005, p. 32), again, points to how the recent developments in information technology have created new and unprecedented methods of industrial espionage. Moreover, the term 'hacking' is closely

[1] The ISO/IEC 27001 standard provides a specification for an ISMS

associated with computer break-ins via Internet-connections. To fully understand hackers one needs to talk to and cooperate with the hackers themselves. Hiring criminals presents an ethical problem for businesses, but one that several businesses have set aside and have hired former hackers in order to pick their minds for information security reasons (Penenberg and Barry, 2000, chapter 9).

Literature published after the introduction of the Internet emphasises the threat-level of cyber-related industrial espionage. However, as strategic thinking and development as well as product development is entangled with the IT system of a business, there is a need to develop this discussion further onto a strategic management level.

3.4. CONCLUSION

I find little discussion among authors about the possible serious consequences of becoming a target of industrial espionage. The literature also portrays a unison picture of the threat level, both with respect to information security, globalisation and the different espionage operators. Winkler (1997) and Mendell (2003), offer concrete advice on how to continuously evaluate the threat. The approach of both sources is hands-on – Winkler with a systematic threat-based approach, Mendell with an investigative approach. Neither of these authors, however, presents a full leadership perspective; how should leaders address the challenge and threat presented by industrial espionage? Nevertheless, the adaptive, vigilant leadership approaches described by Fink (1986/2002, p. 138) when dealing with crisis management could provide an interesting approach here, worthy of further scrutiny. A threat of industrial espionage can be viewed as a warning stage for a crisis, “the prodromal stage” (Fink, 1986/2002, pp. 21-22), subsequently applying contingency-based leadership techniques.

Yet another relevant leadership perspective is debated by Ferdinand and Simm (2007) who maintain that an organisation needs to address the ethical sides of its external learning as this can be larcenously as well as legally obtained.

It is worth reiterating that this dissertation, based on a traditional desk-study, firstly presents evidence of the magnitude of the problem of industrial espionage, as well as the

motives behind it. Based on these findings, it seeks to compile and present relevant information for leaders to adapt effective strategies to face the threat of industrial espionage. Such strategies should include organisational, ethical as well as technological approaches. A further development of the discussion should point towards a higher awareness among managers. The research here aims to provide the concrete, strategic advice needed to heighten such awareness.

Concluding my literature investigations, I find that some of the advice and strategic knowledge relevant for managers is to be found in bits and pieces, spread out among very different literature sources. It is to a little degree presented as coherent, hands-on management advice, which, again, is my aim here.

3.5. DEFINITIONS: INDUSTRIAL ESPIONAGE

The term 'industrial espionage' came into general use during the 1960s (Lawton *et al*, 1988). It attracted increased focus over the following decades, not least after the dotcom wave of the 90s; with the information era came a bundle of new and sophisticated methods of industrial spying. Due to the change in methods used, but also as a result of the different perspectives of the various players in the field of industrial espionage, cultural, corporate, governmental or legislative context influences the meaning of the term 'industrial espionage'. Lawton *et al* emphasise the variations in how industrial espionage is described; "the stealing of secrets, illegitimate intelligence gathering, the unofficial disclosure of information and obtaining sensitive information by dishonourable methods" (p. 4). Winkler (1997, p. 3) states the following: "Economic or industrial espionage is all about the theft of sensitive information," which without further clarification also can pass as a definition of any type of espionage activity. Cornwall (1992, p.1) points out that: "the core of traditional spying is to obtain information that is needed and cannot otherwise be acquired." Furthermore he highlights the ethical aspects on where business activities like market research or due diligence end and industrial espionage begin: "You can find the border wherever your own code of ethics tells you it is" (introductory chapter VII). This view leaves out judicial aspects or regulations of law, which is not entirely the case, as theft of information is illegal in most countries.

However, it points to an important grey zone; in the globalised information society, information can be obtained, or perhaps accidentally presented, in a number of ways. Which methods are legal and not might be entirely circumstantial. This grey-zone view is supported by Lawton *et al* (1988, p. 4) who state, "the point at which legitimate intelligence gathering crosses over to industrial espionage [is] a matter of debate." Cornwall (1992), on a macro level, emphasise further that the technique used to obtain information decides whether the collector engages in ethically acceptable research, or industrial espionage. He divides information into overt and covert sources. This is a continued line of thinking from his description of ethical dilemmas; if the information comes from a covert source, the information gathering is espionage, if it is an overt source it is an ethically acceptable method of gathering business intelligence. However, this subjective definition allows for interpretation.

Nasheri (2005) defines a difference between 'economic espionage' and 'industrial espionage': the first requires a government to be active in the process; the latter is an organisational activity, without government effort (p.12). The same differentiation between the two is also used by Ferdinand and Simm (2007), while Fink (2003, introduction) recites FBI-definitions "The Bureau defines *economic espionage* as that which is carried out by foreign government agents against a U.S. business, *industrial espionage* as theft of trade secrets carried out by foreign or domestic companies against other businesses." Furthermore, for the Canadian Security Intelligence Service (CSIS, 2008),

> "Illegal, clandestine, coercive or deceptive activity engaged in or facilitated by a foreign government designed to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage."

Here too the participation of a foreign government is emphasised. A few other relevant definitions of industrial espionage cast further light on the different nuances. "Spying on one's competitors to gain a competitive advantage" (Investor Words, 2008) includes any organisation, corporation, business or state to spy on any of its competitors. "When one company steals secrets from another company with which it is competing" (Cambridge

Dicitonary, 2008) narrows the description to espionage between companies. "Industrial espionage or corporate espionage is espionage conducted for commercial purposes" (Wikipedia, 2008a) describes any espionage acts where the end result is of commercial value; the spying operators could come from any organisation – private or state run.

The terms 'industrial espionage', 'economic espionage' and 'corporate espionage' are used inconsistently among governments, intelligence operators, academics, journalists and business or legal professionals. However, in this dissertation I will use the term 'industrial espionage' to include economic espionage as one state's economic espionage against another. Both terms are relevant whether a government or a corporation is behind the idea. The term 'corporate espionage implies the involvement of a corporation. Usually the term is used when describing one corporation's espionage against another corporation. However, state intelligence agencies often hide behind a business – a front company – in a different country than their own. In other situations big corporations operating globally are wholly or partly owned by sovereign states. In the example when a state owned corporation performs acts of espionage against a privately owned peer in a different country, all three definitions – industrial, economic, and corporate espionage – could be used.

In all, then, my understanding of the term 'industrial espionage' is as follows:

> ***Any acts performed by one company, organisation or state to illegally search and obtain sensitive industrial information from another company, organisation or state.***

Importantly, this definition does not describe the characteristics of the target information, whether technical, financial or strategic. Furthermore, I have used the terms 'target organisation' or 'victim organisation' to describe the company targeted by industrial espionage, whereas I use the terms 'spying organisation' or 'hostile organisation' when referring to the company behind the acts of spying.

4. STRATEGIC AND LEADERSHIP CHALLENGES

A key strategic challenge presented by industrial espionage is the sheer level of activity. Professional industrial spies, foreign intelligence units, competitors' internal business intelligence units and disgruntled employees contribute to the risk-scenario. Furthermore, inadequate information management routines – in fact the whole company culture – are also important contributors to the threat scenario. In order to approach industrial espionage with the appropriate means, managers in any field should first acknowledge the fact that it is a constant factor in contemporary business life. The threat of becoming a target should influence strategic thinking and planning, in fact all levels of an organisation. There are no indicators of a decrease in espionage activity; hence all activities relating to preventing industrial espionage should be continuous. Countries with the most powerful intelligence outfits are the most active in industrial espionage, corporations with the biggest intelligence staffing levels are the best equipped to gather competitive intelligence. Furthermore, managers must realise that their adversaries are not simple backyard detectives, but technologically advanced and highly skilled professional spies. The espionage techniques and methods utilised are the same as for government intelligence agencies.

The *raison d'être* for industrial spies is finding and obtaining information. Given the complexity of today's globalised, information-driven world, there is ample chance of becoming a victim of industrial espionage, as well as the opportunity to be involved in acts of industrial spying. Consequently, there is an increased focus on the subject from governments, academics, journalists and business professionals.

As I will debate later, the reasons for the increase in focus are several; technological developments, the Internet, globalisation of economies and political shifts toward market liberalism all contribute to the increase. However, first an introduction to the principal characteristics, scope and current prevalence of industrial espionage will be useful as a theoretical platform to grasp the full potential of the risk and vulnerability involved.

On a macro-level, industrial espionage can be divided into two main sectors of activity; 1) industrial espionage conducted by one business or corporation against another, and 2) industrial espionage conducted by a government intelligence agency against a business or corporation.

4.1. INFORMATION

The object of espionage is to obtain information, and industrial espionage is all about "the theft of sensitive information" (Winkler, 1997, p. 3). Nasheri (2005) divides this further into two general types of sensitive business information: Intellectual property is one, operational information the other. The first consists of patents, manuscripts, inventions, formulas etc., the latter of production details, strategic details, financial and marketing details and so forth (p. 73). For the purpose of this dissertation, this categorisation is useful as it covers the main problem areas.

Given the characteristics of the information age, it is a reasonable assumption that probably all relevant technical, financial, political, strategic, creative, artistic or personal information is stored digitally somewhere. Industrial spying, then, becomes a question first of locating the digital storage containing the desired piece of information (disc, server, portable storage unit etc.), second of gaining access to it. Furthermore, the information age has brought about the possibility of collecting sensitive information from the other side of the world, provided that the collector knows what to look for, where to look and manages to obtain access. The ability to do so will in some cases strengthen the position of the spy, as he or she could be operating under a completely different judicial regime than that which the target company is subject to; hence the spy is not liable for prosecution from the target company's legal sphere. Even worse: the spy could carry out operations under the blessing of a hostile regime.

Information is stored and made public at enormous speed. Public sources, corporate web pages, news pages, and financial statements from stock exchanges all present collectors with information which, when put together, can provide good intelligence. In principle, competitive intelligence is a digital exercise, a true child of the Internet. This global-scale openness is driven by the need for businesses to present themselves in the

digital sphere – to be players on the Internet. For managers this also presents a wide spectrum of information challenges (debated later in chapter 9). Cornwall (1992, pp. 17-24), Rustmann (2002, pp. 80-90) as well as Nasheri (2005, pp. 30-38) point out that the increased openness and transparency in societies, combined with the technological developments provided by the information age, have created new and simpler opportunities for gathering competitive business intelligence. As a consequence, creating an analysis of information relating to competing businesses has been made much more accessible, at a fraction of previous costs.

4.2. DRIVERS FOR INDUSTRIAL ESPIONAGE

A key condition for acts of industrial espionage to take place is that somebody – an individual, a company, an organisation or a state – wants sensitive information that somebody else has. The reasons for wanting such information are many.

Criminologists and fraud investigators generally point to three key conditions that must be present before a person is likely to commit an economic crime like industrial espionage against his or her own company, namely the opportunity, the incentive and the ability to commit such crimes (Bussman, 2007, p. 13). Often insiders are involved in acts of industrial espionage. A typical incentive is money, driven by personal wants or needs, or simply greed. A lesser sense of belonging in the organisation, with a low level of commitment, or perhaps the impression of being overlooked, can act as motivation to rationalise for him/herself that given the circumstances, the illegal or disloyal actions involved are acceptable. Fink (2003, p. 105) argues that individuals often are motivated by revenge – for instance after lay-offs. Nasheri (2002. p. 7) confirms this view. As Fink puts it: " With the right motivation, anyone can be inspired to become a spy" (2003, p.103). Former intelligence agents describe how intelligence organisations, when approaching individuals in the process of recruiting new agents, actively use the opportunity, incentive and ability perspectives in an individual in their recruitment strategy (Rustmann, 2002, p.29).

For companies involved in business-to-business espionage, a central driver is profit; it is cheaper to copy than create. Looking at the numbers only, illegal acquisition of

technological knowledge will shorten time to market for a new product, leapfrogging a potentially costly development process.

Stealing information to copy something can prove enormously profitable. Strategic reasons can be more complex. The spying company might seek to financially hurt the target company; it might have a long-term strategic goal of better market positioning or better technological understanding of a particular problem, or it could be spying as part of the groundwork for mergers or acquisitions. Lawton *et al* (1988) describe a number of purposes for industrial espionage: "as to gain unfair economic advantage over a competitor, to establish bona fides prior to business deals, as a precursor to forgery or personal gains, to counter business fraud, as first step of planned sabotage, personal vendetta after major disappointment in business deals, as revenge by disgruntled staff, investigative journalism, as means of earning a living, for enjoyment (computer hacking)".

Furthermore, two purposes described by Lawton *et al* point to the government intelligence sphere: "power seeking and to enhance military capabilities". For a fuller picture it is necessary to establish the drivers – interests – for government intelligence agencies to engage in acts of industrial espionage. It is at any nation's discretion to define what its matters of national security are, and any acts thereof are performed in the accepted grey-zone of intelligence activity, illegal in civil terms, but acceptable under the umbrella of national security. Internal political and macro-economic factors in one country are likely to be drivers of industrial espionage towards a business in another country. For instance, if the government of one state seeks to secure and increase workplaces within its own territory, it will benefit from strategic intelligence about other nations' competitive industry. Or if a government regards a particular business segment to be of strategic importance, as the oil industry is for Norway (my own country), Russia, Great Britain or Saudi-Arabia, strategic information about competing businesses in other countries become matters of national stability and prosperity. As an example, MI6 (British Secret Intelligence Service) states on its webpage (MI6, 2008) that the

> *SIS collects secret intelligence and mounts covert operations overseas. The Intelligence Services Act 1994 directs SIS to obtain and provide information*

relating to the acts and intentions of persons overseas.

- *in the fields of national security with particular reference to the government's defence and foreign policies;*
- *in the interests of the economic well-being of the UK; and*
- *in support of the prevention or detection of serious crime.*

Bullet point two provides a political argument for an intelligence outfit to engage in industrial espionage on behalf of, in this case, the UK. However, such acts of industrial espionage need not always be the result of target-specific activities, but could also be sifted out through the general sweep of information gathered via routine interceptions of communication, debated more in more detail later in this chapter. Herring (1992a) gives supporting evidence to this when debating Sweden's role in early developments of effective business intelligence systems: "Swedish embassies abroad often provide direct intelligence support to Swedish companies." Again, the lines between business intelligence, industrial espionage or economic espionage become blurred.

Organised crime groups are also likely to conduct industrial espionage. An indication of the form such activities might take, is the massive computer attacks experienced by key European institutions and businesses in 2005 where "Close to 300 government departments and businesses considered part of the country's critical national infrastructure have been bombarded with a sophisticated electronic attack for several months", according to the British National Infrastructure Co-ordination Centre (Pesola, 2005). Moreover, Winkler debates the phenomenon of cyber-cartels (1997, pp.74-78). Here, Eastern Bloc criminal organisations are believed to have attracted the talent of former Soviet Union intelligence operatives in order to "provide their employers with information about companies entering markets controlled by the criminal organisation" (p.74). This information is valuable in order to optimise the extortion demands. A significant part of this industrial espionage activity is concentrated around computer hacking techniques.

The drivers for crime are similar to those of legal business: profit, influence, and strategic positions. However the means with which profit, influence and strategic positions are acquired, are illegal. There is no moral threshold involved, simply pure

pragmatism on what methods produce the best results. Their reason to engage is possibility. An organisation's vulnerability will be used for the simple logic that criminal groups search for weaknesses to exploit.

4.3. FOREIGN INTELLIGENCE

When businesses are owned by the state, their wellbeing and prosperity becomes a state matter. There is a consensus among intelligence writers and commentators that some countries are more active in state-initiated industrial espionage than others (Winkler, 1997, pp. 54-74, Rustman, 2002, pp. 113-119, Fink, 2003, pp. 46-51, Nasheri, 2005. P. 8,). Russia, China, Israel, France, Japan, South-Korea, Taiwan, UK and Iran are known to conduct massive, continuous industrial espionage operations against each other and their allies. For instance, Israel, France and China are considered to be among the most active industrial spies against the US (Nasheri, 2005, p. 8) Even between allies economic and industrial espionage is inevitable.

The former Soviet states and China are examples of countries where most businesses of strategic importance or considerable size are owned fully or partly by the government. In other words there is a clear interest for the state to better the competitive strength of these companies via its intelligence services' operations. However this is also a likely scenario in the Scandinavian countries, where state ownership in private sector is common (Nasheri, 2002, p. 8)

Furthermore, when private companies produce weapons, defence systems or key communication infrastructure, these companies' success and activity also become a matter of state security. Yet another aspect is the fact that when the Cold War ended, substantial intelligence capabilities slid from traditional military espionage and into economic espionage (Fink, 2003, p. 37, Nasheri, 2002, p. 53). Industrial espionage has become the new niche for government spies.

4.3.1. SPYING ON YOUR FRIENDS

France's industrial espionage against its ally USA is perhaps the widest publicised incident of a continuous industrial espionage effort from one government's security service against another. A former director of the Direction Générale de la Sécurité Extérieure (DGSE), Claude Silberzahn, affirmed in 1996 that (Rustmann, 2002, p. 107) "the state [France] is not just responsible for law making, it is in business as well. […] For decades, the French state regulated the markets to some extent with its left hand while its right hand used the secret services to procure information for its own firms." It cannot get much clearer; France's secret service conducts industrial espionage on behalf of the French government. It has also been documented that the DGSE routinely bugged Air France flights between New York and Paris, as well as five star hotels in Paris (Rustmann, 2002, p. 107, Fink, 2003, p. 46, Nasheri, 2005, p. 16) to obtain technological, economic or strategic information.

Private manufacturers of defence systems are among the most likely targets of industrial espionage. Defence systems are a matter of national security, and collecting other nations' defence secrets will by nature involve industrial espionage. The motives behind industrial espionage carried out by a foreign state, or their representatives, may not be commercial but rather based on strategic needs originating from arguments of national security. When a company's product becomes important in such international political games, the rules change.

China is well aware of the vast amount of technological know-how to be found in the US. Its secret service Guojia Anquan Bu [Guoanbu], English name Ministry of State Security (MSS), operates a vast number of foreign agents via case officers attached to embassies, consulates, trade offices etc. This is no different from other nation's spy organisations. However China being a strictly controlled state, the MSS has the clout and the means to routinely contact a quite big portion of its citizens living abroad (Rustman, page 117). Chinese expatriates who successfully develop access to interesting information quickly become candidates for MSS recruitment. Not that the Chinese level

of activity should come as a surprise. The late Deng Xiaoping made the following clear when visiting the USA under President Carter in 1979: “We want your most up-do-date technology. Not that of the early 70s, but the very latest. Do you understand?” (Rustmann, 2002, p. 114).

One early example from 1986 was the CIA translator Larry Wu-tai Chin who had been passing on restricted and top-secret material to Chinese intelligence for more than thirty years (Wikipedia, 2008b). Also in 1986, it was discovered that the Chinese had illegally purchased information from Israel that was initially transferred to help the Israelis built their Lavi fighter jet. This information helped the Chinese develop their J-10 fighter jet, which was largely based on the same principles and aviatronics as the F-16 fighter jet (Rustmann, 2002, page 114).

Lavi

J-10

F16

The same technological and avionic principles are used in the three fighter jet designs.

Another example is the repeated stories of information leakage at The Los Alamos National Laboratory (LANL, 2008), the premier national security research institute in the US. Here high-tech research is carried out in a number of areas of interest also for foreign nations, and several alleged spies have passed on information from this outfit to China.

Notably the best known is perhaps Wen Ho Lee, who was arrested in 1999 on charges on having provided the Chinese intelligence with laser- and nuclear secrets. However he was later, after nine months in solitary confinement, released and reached a settlement of $1.6 million with the US state together and a group of newspapers.

There can be little doubt that all countries have intelligence operatives spying on other nations' strategic businesses. Activity levels most likely vary, but countries like Israel, France, Russia and China almost certainly have powerful intelligence capabilities. Of course this is also the case for the USA and Britain, since it would be naïve to think they were not spying back. However, with regard to industrial espionage, the US is the most interesting target because it has the most advanced level of technological innovation. China, Russia, Korea, Japan, Iran, India, Germany and Sweden will all be very interested in US technological know-how. One should expect that other countries spy on technologically advanced countries in the areas where they excel. It is, for instance, widely believed Russia has increased considerably its industrial espionage against Norway since the Russians started to plan advanced subsea oil extraction programmes in the Barents region. Much of the world's advanced subsea oil-extraction technology know-how is concentrated in Norway. Norwegian subsea entrepreneurs have reported a considerable increase in suspicious activity (Jonassen and Aale, 2007). And again, the Norwegians are in all probability spying back on the Russians.

4.3.2. ECHELON

The perhaps most powerful intelligence-gathering system is Echelon (Schmid/EU, 2001, Rustmann, 2002, p. 126, Fink, 2003, pp. 52-55, Nasheri, 2005, pp. 23-24, Perman, 2005, p. 107), a highly advanced eavesdropping system run by the intelligence bureaux of the USA, UK, Canada, Australia and New Zealand. This network gathers as much electronic traffic it can – emails, faxes, phone conversations, text messages – and sifts all this information through digitals filters in search of information. The filters are presumably set up to recognise specific words – like *Bin Laden* – or combinations of wanted information – like *Hezbollah, weapon, money* – or specific phrases – in order to filter out interesting intelligence. It is believed the system is capable of intercepting three

billion communications every day (Nasheri, 2005, p. 24). The Echelon utilises a spectrum of techniques – designated satellites intercept other satellites as well as performing routine dips into communication between metropolitan areas, sniffing devices are believed to be installed at Internet routing points (BBC, 2008). Even deep sea fibre-optic cables are now thought to be unsafe; there are reports of devices developed by the USA that are able to sniff information from the outside of such cables. One Norwegian offshore ROV technician, Andreas Fredriksen, employed by one of the major Norwegian subsea service company, told me that on one of his deep sea assignments in the North Sea a group of anonymous Americans operated a top-secret ROV (Remote Operated Vehicle) out of the same vessel as Fredriksen was assigned to. Their operation was completely unrelated to the subsea service company's assignment. The American group were only interested in where to find deep sea communication cables, utilising the subsea service ship's advanced radars, maps and seismic equipment to locate fibre-optic cables running between European countries and the USA. Their top-secret ROV was kept in a restricted area of the vessel, only accessible to the Americans and a few select crewmembers. However the Norwegian ROV technicians could monitor the American top-secret ROV's movements down to a certain depth (it could dive deeper than any civilian ROV) from their own ROV equipment's control room. According to Fredriksen and his peers, the top secret ROV no doubt deployed advanced and heavy equipment on its ventures to the seabed. Combined with a strong rumour on board, the Norwegian crewmembers resolved top-secret ROV was used to deploy a listening device on a fibre-optic cable.

4.3.3. FROM ECHELON TO PRIVATE ENTERPRISES

Given the scope of the economic implications for the benefiting nation of a multinational industrial contract, it is very likely information filtered through the Echelon system has found its way to private enterprises. Allegedly, in a 1994 incident, the US used information obtained from communication intercepted via the Echelon system when the French communication giant Thomson-CSF negotiated a 1.3$ billion radar contract with Brazil. This knowledge was used to swing the contract over to US company Raytheon. In another example from 1990 the NSA (National Security Agency) allegedly

intercepted communication between Indonesian authorities and Japanese satellite manufacturer NEC negotiating a $200 million telecommunications contract. US company AT&T was also a bidder for this contract. In this case president George W. Bush intervened directly with the Indonesian authorities, managing to split the deliverables between AT&T and NEC (Rustmann, 2002, p. 126).

Another intelligence incident sheds further light onto the importance of the Echelon system, and how, again, the US have utilised this information for commercial positioning. During the delicate and critical automobile negotiations between the US and Japan in 1995, handling the question of tariffs on Japanese luxury cars Lexus and Infinity versus better access to the Japanese market for American automakers, the US negotiating team lead by Mickey Kantor had access to background information from CIA and NSA eavesdropping operations targeting the Japanese delegation. Consequently the US team knew what the Nissan and Toyota executives' position would be every next morning. Surveillance under such circumstances is in fact legal under US law (Nasheri, 2005, p. 22).

Listening in on commercial communication is by no means restricted to Anglo-Saxon countries. The EU report on the existence of Echelon (Schmid, 2001) states that the intelligence services of all but a few EU-countries (Austria, Belgium, Greece, Ireland, Luxembourg, Portugal) engage in interceptions of civilian communications.

Echelon, as well as any other intelligence-monitoring of civil communications, presents a considerable strategic challenge for a manager. It means, as exemplified above in this section, that strategic financial, commercial, technological or negotiation positions can be revealed to either adversaries or business partners in other countries via close ties between intelligence services and corporations. Drawing further on the findings presented by Herring (1992a), where such ties between government intelligence operations and the private sector are institutionalised over decades in countries like Sweden and Japan, it is clear the challenge of keeping sensitive business information from leaking is a considerable challenge.

4.3.4. CASE: THE SILOVIKI, RUSSIA

Developments in Russia under President Putin are of particular interest. The Russian sociologist Olga Kryshtanovskaya (Ostrovsky, 2003) points to the arrest of Mikhail Khodorkovsky, with the subsequent state-seizure of Yukos shares, as an historic shift in power from the liberals in the 1990s to *siloviki* under Mr. Putin.

The siloviki are made up of former KGB and FSB acquaintances of Putin, whome he has presented with powerful and strategic positions in the Russian business sphere. According to Bremmer and Charap (2006), the siloviki take up top positions in the oil company Resnoft, military companies Rosoboronexport and Almaz-Antei; Aeroflot, the Russian Railroads, and banks Vneshekonombank, Mezhprombank, and Rossiya. In addition the siloviki apparently control ten important ministries, and through these control developments in telecommunication, oil extraction and the economic development.

The developments under the siloviki-influence have resulted in a shift in Russian policy. Considering their background, and the strong position of the state in Russia, Kryshtanovskaya says "We are witnessing the restoration of the power of the KGB in the country from the regions to the top of the Kremlin" (Ostrovsky, 2003). Yukos, now Gazprom, is still one of the biggest employers of former officers of the KGB and its successor FSB. Their jobs range from traditional bodyguard/driver assignments to business intelligence tasks. Kryshtanovskaya estimates in excess of 20,000 former KGB professionals ended up working for the oligarchs of the new Russia. Furthermore, between 1991 and 1993 an estimated 300,000 KGB officers had to look for a private job outside the security organisation (Ostrovsky, 2003).

Putin and his associates obviously want Russia to prosper. Bremmer and Charap (2006) describe the group's aim: "The Siloviki are economic rationalists that seek to restore Russia's international greatness." With the intrinsic intelligence capacity described in the current Russian, state-influenced business life, it is a reasonable assumption that Russian corporations have advanced intelligence operations, furthermore that there is a continuous cooperative intelligence effort between corporations and the state. Facing such intelligence capacities where managers and other key operators might

even be former intelligence people, finding effective counter-measures becomes very difficult. Managers operating on this level cannot expect to be better, more savvy game players than ex-KGB professionals.

4.4. BUSINESS INTELLIGENCE

The former CIA agent F. W. Rustmann Jr. states that "Business is war" (Rustmann, 2002, p. 4); Though perhaps a simplistic view, the highly competitive situation of today's globalised economy – the war in the Sun Tzu universe – creates a market niche for professional business intelligence outfits, which provide business intelligence services, with adjacent analysis to their finds. Companies will want to gather intelligence about their competitors – business intelligence – and use this information in order to compete more effectively. Information-gathering from legal sources like public registers, company web-pages, news archives, marketing brochures, trade fairs, etc. is a common way to collect and compile information in order to construct a competitive dossier on adversaries. Competitive intelligence is described by Nasheri (2005, p. 73) as "a systematic and ethical program for gathering, analysing and managing information that can affect a company's plans, decisions, and operations". Many companies also have their own business intelligence operations working solely with information gathering on competitors. An interesting example of the possible strategic importance an internal intelligence unit is presented by Penenberg and Barry (2000, pp. 28-35), in the Motorola case described later in this chapter.

4.4.1. PRIVATE SECURITY FIRMS

A significant part of the industrial espionage scene is made up of private security firms. Their clients are businesses and corporations in need of competitive intelligence (CI) about competing businesses and corporations. In the US, the Operational Security Professional Society is a membership organisation for security professionals (OPSEC, 2008). The USA is – it needs not be stressed – a big country, but the fact that private

intelligence operators have their own society gives indications in any event on the scale of the market. One well-known provider of business intelligence services is the American company Kroll, the de facto business leader, established some 35 years ago by Jules Kroll. On their website, services like "Investigations, Financial Advisory & Intelligence, Background Screening Services, International Backgrounds, Business Intelligence, Security Services" and more are offered (Kroll, 2008). The company sports 65 offices in the US and abroad. The use of such services has increased considerably over the last few years. According to Barker, (2007), "In many areas of business – from due diligence to litigation to background checks for prospective employees – it has almost become routine." Other international players in this market, offering similar and complementary security services are British Control-Risks (BCR, 2008), The Risk Advisory Group (Risk, 2008), Hakluyt & Company (Hakluyt, 2008 – in tune with secrecy, their one-page website simply states their London address and phone number), GPW (GPW, 2008) and a string more.

Given the fact that many of the founders of such companies, as well as their employees, have a military and government intelligence backgrounds, their operators will certainly be well acquainted with a spectrum of intelligence collection methods. For managers facing critical decisions, but at the same time experiencing information vacuums, such intelligence abilities might seem quite tempting to acquire, but a fine line of ethics runs here between acceptable business intelligence methods and unacceptable industrial espionage methods.

4.4.2. CORPORATE BUSINESS INTELLIGENCE UNITS

Competing companies are faced with a continuous strategic challenge of collecting business intelligence from legal, overt sources, but knowing competitors are doing exactly the same, or might even be using illegal methods, crossing the line into industrial espionage. McQueen (2008) confirms that illegal activities are on the rise, exemplified here by the disclosure of the illegal wiretapping of actor Sylvester Stallone in a celebrity business dispute, or the hotel room of Porsche executive Wendelin Wiedekin during negotiations with Volkswagen.

As a response to the increased importance of competitive intelligence in the strategic formulation process of companies, it has become the standard per se for big companies and international corporations to have business intelligence units. Such units are involved in both for both intelligence gathering as well as counter intelligence operations. Herring (1992a) points to the common practice of Japanese and Swedish companies involved in international business to have their own business intelligence units.

4.4.3. CASE: GALVIN AND MOTOROLA

A relevant example on the strategic significance of competitive intelligence (CI) is the story of Motorola presented by Penenberg and Barry (2000), since it provides evidence of strategic achievements as a direct result of business intelligence. Motorola is considered one of the pioneers in corporate business intelligence. Its CEO from 1959 to 1990, Robert W. Galvin, was well acquainted, as a result of his background as a member of the US President's Foreign Intelligence Advisory Board, with the effort foreign states put into spying on American companies. In 1979 he hired the former CIA operative Jan Herring to head an in-house Corporate Intelligence unit at Motorola.

In 1985, Motorola found itself in a bidding war over Danish land mobile systems producer Storno A/S, together with NEC, Bosch, Siemens, Ericsson and others. If Motorola successfully managed to acquire Storno, it could push their mobile systems market share from 20% to as high as 60%. But the other bidders were tough ones, and Motorola was about to lose the bidding. However, a turning point occurred as Motorola executives became aware that negotiations between Bosch and GE over Storno A/S had broken down. Motorola wished to know why in order to take advantage of the situation. Jan Herring and his group of people encouraged any Motorola employee with information relevant as to understand the stalled negotiations to report to Herring's team. The tactics proved successful. A local Motorola manager in France reported back with "a treasure trove of business and government contacts within France and Germany" (Penenberg and Barry, 2000, p. 34). According to this well-informed manager, negotiations had broken down over Storno's value. He also provided information that

Swedish Ericsson seemed not to understand the significance of Storno A/S, and that the French were not interested. Herring and his team's report concluded that Storno could be Motorola's, provided the offer was right. Motorola drafted a new offer for GE, based on the information provided by Herring, and presented this to GE within a week of Herring providing his memo. The deal went through.

What can we learn from this story? Could Motorola have reached the same result without an internal business intelligence unit? Were the methods used here fully legal? The rapid input of reliable information in fact changed Motorola's position from a dead end to a new and positive angle. The foreknowledge obtained told Motorola that the evaluation of Storno was the Achilles heel. Without this knowledge, Motorola would not have succeeded. Moreover, it was all done using fully legal methods within its own organisation. However, Penenberg and Barry (2000) give no evidence of the origin of the first piece of information, namely the fact that the negotiations between Bosch and GE had broken down. Was this information collected provided legally, for instance via the media, or was it intercepted via illegal sources? Perhaps a 'deep throat' within GE? If so, the whole operation was instigated based on one illegally obtained piece of information. This is now purely speculative, but points to an important aspect: one little piece of information – legally obtained or not - can have tremendous impact on a business's strategic choices. Cornwall's (1992) perspective leaves it up to our own code of ethics to define whether or not we are engaging in acceptable business intelligence activities, or industrial espionage (1992, introductory chapter). But as Ferdinand and Simm (2007) maintain, it has become "a normative assumption that an organisation's learning [its information input] is an entirely legitimate activity." Nasheri (2005, p. 76) offers a more clear-cut perspective: "Competitive intelligence or corporate intelligence becomes illegal espionage when it involves the theft of proprietary information, materials or trade secrets."

4.4.4. STRATEGIC LEARNING FROM BUSINESS INTELLIGENCE

Whether acquired within acceptable ethical guidelines from open sources, or as a result of industrial spying via covert sources, good business intelligence provides opportunity for a business to adjust its strategies. But as Herring (1992b) points out, "…successful strategies are derived from good intelligence concerning a company's total business environment, including the competition." Herring points to several categories of information where competitive intelligence influences both the formulation and implementation processes of a business' strategic planning. For instance, the analysis of intelligence provides a valuable opportunity to describe the competitive environment. Furthermore, it can be used to forecast the future competitive environment. However, when analysing intelligence, an organisation must challenge underlying technological, economic or political assumptions to avoid new information to be coloured by 'old truths'. The analysis can also provide an opportunity to identify and compensate for exposed weaknesses. Finally, Herring emphasises the importance of using the intelligence to implement and adjust strategies, as well as to determine when a chosen strategy is no longer sustainable.

The opposite perspective reveals the vulnerability of organisations targeted by business intelligence professionals, or industrial spies. Even small pieces of information gathered from covert or overt sources can prove sufficient for the organisation gathering the intelligence to successfully alter its strategy. Consequently managers need to realise any output of strategic information is likely to work its way into the corresponding strategic approaches from competitors. Herring (1992a) identifies two countries in particular as prime examples of having an effective business intelligence culture: Sweden and Japan. Sweden's effective business intelligence cooperation between banks, industrial giants, universities and foreign intelligence services has provided Swedish businesses with solid intelligence for decades. Similarly, the Japanese government's focus on intelligence collection through the government organisation Japan External Trade Organization (JETRO) and other similar organisations has provided Japanese businesses with prime business intelligence since the 1960s. Again, the link between government and private sector is clear, as in the previous example about the siloviki

culture in current Russia. With this is in mind, it becomes relevant for managers to know the principal methods of industrial espionage.

4.5. PRINCIPAL METHODS OF INDUSTRIAL ESPIONAGE

To fully grasp the potential threat of industrial espionage, managers need a fair knowledge of the methods used to obtain information. Cornwall (1992) divides information sources into overt and covert sources. Information derived from overt sources will be legally obtained, as opposed to information obtained from covert sources. As already discussed, the increased openness of modern societies creates ample possibility to legally collect strategic information about a business. Simply cross-referencing such information might provide formidable intelligence. Economic records of companies are readily available in the EU, authorities are required to have public records on the lay-out of laboratories or chemical plants, architectural information is stored in municipal archives, media records from financial press might provide hints on R & D activity.

However, the methods used to find and compile illegal information are more advanced. For instance, travelling executives can be bugged, exemplified by the Air France bugging routine in first class (see next chapter for details). Hotels are also considered typical 'bag ops' (snatching bags), where document folders can be taken away for copying, or worse, the whole hard drive of a computer can be copied onto a portable disc. In many incidents operators snatch the whole computer.

Another cheap and effective technique is to request a quote from a competing business, perhaps to a front company or cooperating third party, in order to obtain information about prices or technological solutions. Further down that track there are techniques where collectors pose as representatives of marketing survey companies, asking a wide range of questions to targeted people in organisations – often the CEO, CTO, CFO or at managerial level.

Yet another approach is acquisitions of export-controlled technology via front companies in a third country. And a further development is that of joint ventures, where

guest workers under the joint venture programme become effective spies for a foreign company or organisation.

Mergers or acquisitions can be tools for acquiring intelligence. A resourceful company A might opt to buy the smaller company B entirely to gain access to the information company B is privy to via its joint venture with company C. Nasheri (2005, p. 86) mentions an attempt by French companies together with Airbus to acquire a subcontractor to Boeing.

Former employees may have known, and might still have essential information about, technology, production processes, and financial or strategic situations. If they still have access to information via personal networks or via the current position they are possible targets of co-opting.

Trade fairs, conferences and seminars attract key people with cutting edge knowledge. Leading scientists are often present. Here subtle approaches, the smallest corner chitchats, can provide essential information for a skilled collector.

Finally, computer break-ins and surveillance of Internet traffic can provide big chunks of strategic information.

4.5.1. THE INTELLIGENCE PROCESS

Industrial espionage is to a large extent carried out with the same methods as used by intelligence organisations like the CIA, MI6 or other national equivalents. In fact many of the people performing acts of industrial espionage are former spies (Nasheri, 2005, p.19, Fink, 2003, p. 37) In many cases they still are spies. The CIA definition of the intelligence process (cited from Rustmann, 2002, p. 11), meaning the process of gathering and analysing information, is:

1. *defining the requirement;*
2. *collecting information on the requirement from all available overt sources (databases, library research, and so forth);* [Internet research, media research]

3. *analyzing the overtly available information and organising it into a cogent preliminary report on the subject;*
4. *identifying the gaps in the information and filling them through the use of more targeted covert collection techniques, and writing the final, comprehensive report.*

It is a simple, logical list laying out a step-by-step approach. Illicit methods first come into play where open sources of information fail to deliver the wanted results. If one business, Hightech Inc., fails to collect the wanted information about its competitor Highertech Gmbh. through open sources of information, it might resolve to proceed to point 4 on the CIA list, describing the covert part of the intelligence process. Depending on the type of information Highertech wishes to obtain – and provided that the company is willing to use illegal methods to get this information – more or less the whole range of clandestine operations and illegal techniques could prove viable options. Cornwall (1992, p. 6) describes a similar overview of the intelligence cycle:

1. *Set objectives*
2. *Collection/acquisition*
3. *Analysis*
4. *Report/dissemination*

Finally, categorising the civil as well as government methods described in the literature we are left with two main methods of intelligence gathering – 1) Technological Methods, herein Signal Intelligence (SIGINT) and 2) Human Intelligence (HUMINT).

4.5.2. TECHNOLOGICAL METHODS

The information age has provided an array of new methods of obtaining information. In great contrast to the wiretap operations of 70s and 80s, when the secret police would connect cables to the target's phone line, or drill holes to insert mini microphones in the wall, audio operations of today to a large extent mean the interception

of un-encrypted communication between two parties. The necessary digital equipment to do so is within reach for almost anybody, resulting in a considerable increase in such activities over the last decade. Security companies report, for instance, a 25% annual increase in the request for sweeps to detect audio listening devices for 2006 and 2007 (McQueen, 2008). Scanners can be bought at an affordable price at any spy-shop to easily eavesdrop GSM phone conversations. More advanced equipment turns any mobile phone into an effective microphone, without even being turned on. GSM phones with remotely operated built-in listening devices are sold online (GSMSpy (2008). More advanced solutions available online include interceptor software for specific GSM phones where either audio/voice or even SMS-texts are forwarded to another phone (Spycatcher, 2008). Small, quickly installed scripts turn GSM phones into remote microphones. As long as the subject carries his or her mobile phone into a meeting, other people can listen in on confidential conversations from a safe location. And of course, GSM bugs – a GSM version of the classic under-the-table bug – are available as well (GSMBugs, 2008). In short; GSM phones, as well as most other civil mobile phones, are not safe. If one needs to be absolutely certain a conversation is not listened in on, the phones will have to left someplace else.

Another much used method of obtaining information illegally is a traditional computer break-in. Hackers and computer security specialists are engaged in an ever increasing spiral of new security measures in the form of better firewalls, better encryption, biometric identification and so forth, but where the culprits sooner or later always find a way in. The methods of how to get behind a high security firewall amuse hackers no end. Someone with the wrong intentions and the money to back their interests can buy any level of hacking expertise. One of the ironies brought to us by the computer age is that computers are 100% logical; hence, for any security measurement there is a reverse logic. This is what savvy hackers and spies exploit, and why all IT-systems are vulnerable, provided the hacker has the required level of expertise.

The simplest and cleanest method of entering a computer illegally is by getting hold of passwords. Password-theft is big business among hackers. Passwords that gain access to high-profile businesses' or organisations' networks are traded on illegal marketplaces for money. One of the easiest methods to get passwords is to attack a person's home

network to gain access to corporate computers brought home for late-night work. No matter how high the security level is at the business office, if the home network is not secured properly, which represents the company's endpoint security-wise (described later in chapter 9), this is an equal threat for the organisation one works for.

Another method of obtaining access to a company's server is via inserting sleeper software or malicious software. Sleeper software (Altucher, 2007) attaches itself to the very lowest level of a computer, and sits dormant perhaps over years. On a pre-programmed interval the software sniffs out on the Internet to receive orders on how to behave. One of the really clever features of such software is that it is able to rewrite itself, hence antivirus software is fooled. It is used to collect information and monitor the host computer. It is believed that any fresh computer logging on to the Internet via a router with an up-to-date firewall will become infected within thirty minutes. 50 million computers worldwide, and most likely half the Standard & Poor 500 companies' computers are infected (Altucher, 2007).

Computer theft is another effective way of spying. The hard drives on laptops belonging to key personnel, or their portable hard drive units, can contain crucial information. Under lax corporate security schemes disaster can be imminent. Examples are the Hollywood film business, where for instance Star Wars Episode III was leaked as a work print (with time-code imprinted in every frame) for illegal download (Star Wars, 2005). Another example could be engineering companies developing new technology. A laptop used for CAD (Computer Aided Design) work may hold significant traces of its latest designs on its hard drive, or even the complete design if the engineer needs to work outside his office. Snatching the laptop itself is another option, as Brazilian state-controlled oil company Petrobras experienced early in 2008, when two laptops holding sensitive seismic mapping information were lifted from a container onboard a freight vessel (Economist, 2008). The find has been described as the "discovery of the century." In-depth knowledge about the scope and technicalities of the find will of course be of interest for potential buyers of oil, or investors looking to buy Petrobras shares or competitors.

4.5.3. HUMINT METHODS

HUMINT (Human Intelligence) is the spy-world's term for any intelligence-gathering processes by personal contact. Humans are diverse creatures; they watch, listen, read and can memorise enormous quantities of information. We also have amazing capabilities of filtering out irrelevant information on the go. As the methods as well as the people conducting industrial espionage are the same as those who carry out government espionage, HUMINT also plays a role in industrial espionage.

Intelligence outfits use case officers, fully trusted individuals assigned to a specific branch of the organisation, to recruit agents. These case officers have a number of recruitment methods, ranging from long and time-consuming periods of befriending target personnel within an organisation, wining and dining them, finding out bit by bit about their weaknesses, frustrations, unfulfilled dreams, then playing these cards strategically to get the person 'over' to their side. Money, culture, religion or greed, to name a few, are all viable options to 'play' for a recruiter. The 'Recruitment Cycle' (Rustmann, 2002, p. 29) describes further how agents are thought first to "spot new agent talent" (people with access to desired information), "to assess new agent talent's susceptibility to recruitment, how to use their perceived susceptibilities, vulnerabilities and desires to develop them to the point of recruitment and finally how to deliver a recruitment pitch". Motivators for an individual to engage in illegal activities could then be influenced by outside pressure such as financial trouble, child custody cases – aspects that individuals find overwhelmingly problematic – and a recruiting organisation could use to persuade an employee to provide sensitive information. Political, ethical or religious reasons also act as strong motivators and create ability to find rational arguments for spying against your employer. "Inducements of money, recognition and revenge are examples of major motivators; most spies accept recruitment to gain one or more of these things" (Rustmann, 2002, p. 29).

Cornwall divides agents into five categories (Cornwall, 1992, pp. 35-41):

- Unaware
- Covertly Corrupted
- Overtly Corrupted
- Volunteers
- Professionals

Unaware agents provide information without knowing they are doing so. Covertly corrupted agents provide information in return for money or other rewards, but in circumstances where the agent does not fully realise he or she is doing something wrong. As an example people can be recruited as ‘consultants’ for a ‘consultancy fee’ available to them through their job. Overtly corrupted agents are agents collecting information for an agent runner in circumstances where they are fully aware of what they are doing, in return for money or other reward. Volunteer agents are individuals who approach a likely buyer of information with an offer to sell information. Finally, professional agents are simply private detectives or other specialists offering their special skills for customers in need of theses particular services, including dirty work.

Once an agent is recruited within a target business, information can be bought or exchanged for other services. The best agents are of course within the target organisation, indicating what is called ‘direct access’. Once such an agent is operative, providing information, he or she is a ‘penetrating’ agent. If direct access is not possible, recruitment of agents in cooperating businesses or clients of the target business might provide interesting information.

Plain stealing information is another option. Intelligence methods include posing as cleaning or medical personnel to gain access to restricted areas, hotel rooms, wardrobes or air luggage. . But such methods usually require an inside mole for them to be effective. Other methods include, simply, forced break-ins

For as long as there have been intelligence agencies, there have also been double agents. The industrial espionage equivalent to this tactic is to recruit key talent from a competing organisation with the purpose of getting inside, in-depth information. Areas of

interest can be strategic, marketing or economic information as well as information on technological developments, R&D or innovation.

Acquiring information by posing as someone else – for instance market researchers, public servants or journalists – is a technique used successfully time and time again. Executives or other people with access to strategic information will always meet different people with different mindsets. A friendly mindset can prove a great opportunity to obtain sensitive information.

Former intelligence operatives point to the Diaspora of a country as prime recruitment targets for intelligence operatives. Winkler (1997, p.60) and Rustmann (2002, p. 117) focus on how China in particular uses this technique. In particular graduate students doing their doctorate research projects, with access to top-notch technological information, are interesting recruitment objects. On an empirical note, in my numerous phone calls to the Norwegian Police Security Service (Politiets Sikkerhetstjeneste – PST) it would be fair to say I have been met with a reluctance to provide any concrete piece of information. But the only two pieces of information one operative in fact did provide is relevant in this section: 1) there have been incidents also in Norway where R&D departments have disclosed espionage conducted by students working on their doctorate degrees, and 2) there have been front companies set up in friendly third countries, such as Sweden, with the aim of buying restricted technology.

Foreign governments have a much bigger chance of success in recruiting somebody on the inside rather than placing one of their own agents inside. Persuasion techniques involve money, cultural commonalities or pressure against family members left in the home country.

Reverse engineering involves dismantling the target piece of technology and then producing a looks-like-works-like copy via re-engineering and a complete rebuild. However this method has its limitations. The process often requires the engineers involved to understand in detail all principles utilised in the original technological, chemical or digital design. In other words the knowledge gap here is not very wide.

An interesting example of a yet another technique employed by foreign intelligence operatives is how the French Intelligence Service frequently and effectively used its national airline Air France's flights to gather information. Key American business

professionals were logged immediately when booking seats on Air France flights, and their seats were bugged. Some of the flight attendants and members of the aircrew on such flights would be French Intelligence Services operatives (Nasheri, 2005, p. 16).

In addition to the methods of intelligence gathering already discussed, a few methods specific to the business world are worth noting. Recruiting of key personnel from a competitor can provide a business with a heightened knowledge within an area of competition. Quarantine clauses are common in employee contracts, but there are ways to work around this. An individual could stay out of the professional game until the quarantine is over, but still play a vital part for the recruiting company off the record, or, worse, act as a spy from within the company he or she is leaving for the recruiting company. This was the case, when VW recruited the Jose Ignacio Lopez de Arriortua, a purchasing manager, from GM in 1993. Allegedly Mr. Lopez brought with him stacks of sensitive documents very useful in VW's need to cut better deals with sub-suppliers. He also brought along seven co-workers to VW. The case ended in a $100 million court settlement in favour of GM (Meredith, 1997).

Other business-to-business opportunities for industrial espionage include client audits, used for example when bigger companies wish to place orders with smaller, specialised companies. In order to qualify as a supplier, the Little Company must provide the buying Big Company with amounts of technological and financial data, which enables Big Company to extract vital competitive information.

5. RISK

The previous chapter established how the principal characteristics and prevalence of industrial espionage present leaders with a continuous challenge. A manager wanting to meet this challenge effectively and with a complete set of counter-measures might soon find himself or herself in a situation of establishing something similar to a complete intelligence agency. For all but a few businesses, that is not a viable option. However, it is important to acknowledge the threat of industrial espionage, and address this threat adequately in leadership and strategic thinking. The risk of being targeted in industrial espionage is greater than most managers are aware of. Winkler (1997, p. 37) refers to the former CIA director Robert Gates, who stated, "One of the biggest problems companies face in their efforts to secure sensitive information is their lack of awareness of the threats around them." Furthermore, Fink (2003, introduction) reveals that "Virtually *no* company is immune to the risk of economic espionage."

Meeting this threat involves all levels of an organisation; product development, production, innovation, information security, employee policies, finance, mergers & acquisitions, strategy, foreign relations, cultural differences, ethics, technology and information policies.

5.1. CALCULATING RISK

"Is my company at risk from espionage?" This should be a central question for managers, and one that can be asked again and again. The answer often lies within the answer of a complimentary question: "What do we have that others might benefit from?" The risk-equation formula (Winkler, 1997, p. 13), used by statisticians to calculate risk on a general level (see Figure 1), presents a useful approach also when discussing industrial espionage:

$$\text{RISK} = \frac{\text{Threat x Vulnerability}}{\text{Countermeasures}} \text{ x Value}$$

Figure 1: Risk-equation formula (referred to by Winkler, 1997, p. 13)

Here **Threat** represents everyone involved in trying to get information from a company. How much would competitors benefit from information? How far would they go to obtain it? Does your company have, for instance, expert knowledge in the defence area? Who would benefit from this information? The answers to these and related questions of the same nature will help to get some realistic perspective on the threat towards a company.

Vulnerability describes the weaknesses in your organisation spies might take advantage of. Here employees, IT-security, the handling of documents, and even simple things as routines for locking offices or lockers contribute to the overall vulnerability of the company.

Counter-measures are the tools a company uses to address vulnerabilities. Routines, awareness training, security systems and classification of information are examples of activities aimed at counter-measuring vulnerability.

Most companies will be able to define some pieces of technological, strategic or financial information that competitors – known or unknown – will find it useful to have access to. However, not every effort at industrial espionage is initiated as a targeted attack on specific businesses or organisations, but also as the result of information derived from sniffing and intercepting communication (Schmid/EU, 2001).

Referring to the risk-equation model in Figure 1 above, how a company handles its information clearly becomes a contributor to the risk-exposure. Equally important are the routines for communication between offices, subcontractors or clients. A hypothetical example provides further insight: Assuming Engineering Company A develops a particularly versatile and economic valve pack for subsea manifolds. The Subsea Oil Company, the world's biggest subsea operator, commissions it. Subsea well installations

require a number of such valve packs in connection with manifolds which again distribute oil or gas up to sea-level production vessels or platforms. On big installations orders for valve packs quickly reach into the millions of euro level. Considering the fact that many new subsea-projects are under way in the Barents region, in Asia, outside West Africa, in the Mexico gulf and Brazil, the potential market here is considerable.

What is the risk involved for Engineering Company A? It is a twenty-people company. 60% of their engineering capacity is allocated to this project. Vulnerability is high because the company is not developing other substitute products with similar potential. Vulnerability is set to 50%.

The world market for this type of valve pack – over a ten year period – is for the case of this example estimated to €200 million. Engineering Company A might capture 70% of the world market. The market value over ten years is then 70% of €200 million= €140 million. In other words: substantial market value.

Because of the considerable size of the international market, the threat involved is likely to be national spy organisations continuously intercepting communication, or even targeting Engineering Company A specifically with either HUMINT methods or technological methods, as well as professional approaches from competitor's business intelligence units or hired sleuths. The threat is considerable, and set to 40%.

Engineering Company A has no particular routines for secure communication. Technical drawings are emailed to clients as DFW files, documents are Word or PDF. All employees have signed confidentiality contracts, the company's IT-system uses an above average firewall, data is backed up on two external hard drives located on dedicated back-up servers run by professionals. The company does not have a wireless network, but uses traditional cables. The valve pack is patent pending, and the company culture focus on vulnerability and competitiveness. Countermeasure is set to 40% because the risk of spies intercepting communication containing documents and ideas is relatively high.

Using these hypothetical numbers in the risk-equation formula referred by Winkler, we get:

$$\textbf{RISK} = \frac{\textbf{0,5 x 0,4}}{\textbf{0,4}} \textbf{ x €140 million = €70 million}$$

Figure 2: Risk Equation, Example Calculation

The risk of loss here is, to say the least, enormous. This also gives an indicator of how big the chances are somebody would like to steal information making them able to produce copies, or design something close to the original, but work around the patent requirements. €70 million is a huge amount of revenue. In a scenario like this, managers will find good arguments for imposing any counter-measure that could reduce the risk of theft.

5.1.1. VALUE

The process of defining value requires managers to look beyond monetary and other definable assets (Winkler, 1997, pp 30-32). Money, deliverables according to written contracts, machinery, buildings and stocks all have a concrete value. But as the previous example explains, the potential value of a project, or a portfolio of projects, might be something totally different. The potential future earnings of a project, or the company's portfolio of projects, should be taken into account. Which potential is lost if critical information gets into the hands of competitors?

Hidden values are values often not visible on the balance sheet. Hidden values take into account the level of continuous innovation, the strategic importance of knowledge associated with projects, financial records, particularly talented employees, competitor value – how the company is perceived by clients and competitors, and information management. (Winkler, 1997, pp. 30-32). Both Winkler (1997, p. 33) and Calder and

Watkins (2006, pp. 111-116) emphasise that a company's ability to successfully create and maintain an effective information resource management (IRM) system in itself represents great value.

6. COMPANY CULTURE

It is perhaps not obvious whether a company is at risk, or how big that risk is. But as this chapter will show, the risk is entangled with the company culture. Gobert and Punch (2007, pp. 101-119) point out the consistency between organisational culture and how – and to what extent - individuals relate to corporate crime. Three main situations are portrayed: Apparent awareness, apparent unawareness and contextual ambiguity.

6.1.1. APPARENT AWARENESS

(*Corporate Crime Committed with an Ostensible Awareness of the Criminal Implications*)

Some corporate cultures accept illegalities like industrial espionage as SOP (Standard Operating Procedure) because the chances of getting caught are low, the ability to rationalise the need for it is incorporated in the company's culture, the financial up-side is so big the internal corporate rhetoric among 'leagues of gentlemen' at the top systematically justifies tools like fraud or industrial espionage. In the SAS-Braathens vs. Norwegian case (see page 52), the misuse of access to the Norwegian booking system might have started by coincidence, growing into a full-scale industrial espionage operation. The descent into unlawfulness might have been encouraged by the managerial level's unwillingness to act on the apparent unlawful actions.

6.1.2. APPARENT UNAWARENESS

Apparent unawareness refers to corporate crime committed with an ostensible unawareness of the criminal implications. A lax corporate culture can influence employees to perform illegal actions without the individual being fully aware of the illegal implications. For instance, information can be presented to individuals that they do not and could not have known was illegally obtained.

6.1.3. CONTEXTUAL AMBIGUITY

Contextual ambiguity refers to grey zones in the law which encourage would-be offenders to believe that they are not engaged in illegal activity. Differences in local/national legislation can encourage self-justification of illegalities. Collecting information one has access to without technically doing anything illegal, then leaving it to somebody else to consider the legality in whether to use it or not, is an example of a grey zone.

6.1.4. ETHICS

Business decision-making is often conducted with a focus on utilitarian criteria (Vaughan, 2007, p. 10); that is, the decision is made on the basis of what is for the greater good of a company. However, there is a risk this can lead to an absence of ethical considerations. If the company culture is lax, the result can be a normalisation of deviance leading individuals, groups and in particular the leadership in an organisation to perform illegal acts like industrial espionage.

Legal, competitive intelligence-gathering ends where industrial espionage starts. A business's motivation to venture into the illegal sphere, as I will debate later in this chapter, is influenced by the organisational culture. Also, the sheer size of the potential economic up-side contributes. The core logic for all capitalists is to maximise profit and shareholder value. In this perspective, bigger short-term profit based on better information, even illegally obtained, makes sense. Some managers or operatives will stop where the legal information-gathering takes them, then instigate analysis. Others do not stop where the law instructs. A contributing factor here is that the risk of getting caught is low, and prosecution and punishment are kept at low levels. Michalowski and Kramer (2007) argue that the dominant understanding of crime in the US and UK, as well as other western countries, is restricted to the criminal law area, whereas actions of white-collar crime, herein industrial espionage, is affected by regulatory law. The elite classes

in society, which are the most likely offenders of crimes under regulatory law, remain administratively segregated from the lower classes of ordinary crime (p. 202).

To make the right decisions, in this case to create a company culture and a company set of ethics that does not promote illegal actions in order to maximise profit, leaders must use a mix of all three ethical criteria, involving also a respect and responsibility for the societal context. Lee and Gailey (2007, p. 53) present the 'Amoral Calculator Model' as a means of graphically displaying organisational deviance on whether to engage in illegal acts such as industrial espionage or other types of corporate crime:

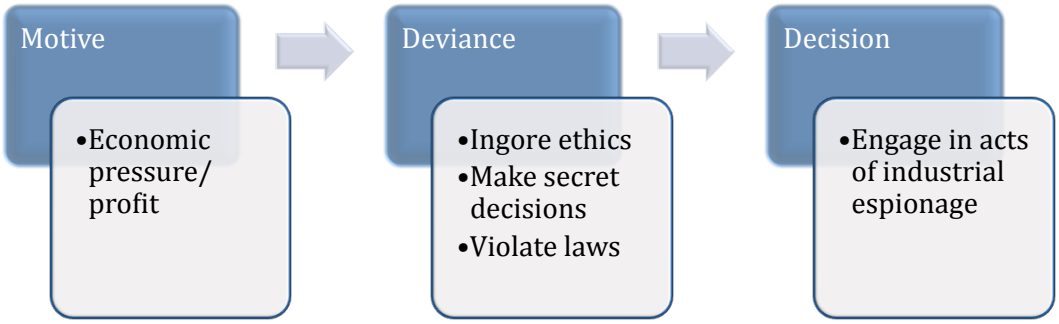

Figure 3: Amoral Calculation Model (Source: Lee and Gailey, 2007)

6.1.5. CASE: SAS-BRAATHENS DATA-THEFT FROM NORWEGIAN AIRLINES, 2004-2005

When the Norwegian airline company Braathens Airlines merged with SAS (Scandinavian Airlines Systems) in 2004, Braathens still had access to Norwegian Airlines' booking information (Gran, 2007) under a former arrangement where the two minor airlines Braathens and Norwegian cooperated to pool planes and flights in order to compete with SAS more effectively. The contract of cooperation was only valid throughout 2002, but Norwegian never technically terminated the access to its booking information. Former Braathens employees who knew about the security glitch at Norwegian continued to access the Norwegian booking-information after the merger via

the system Amadeus, giving SAS-Braathens first hand pricing information on its main competitor.

These actions are an example of what Gobert and Punch describe as 'apparent awareness' (2007, pp. 101-102). Due to the impact on the pricing policies of SAS-Braathens, the information collected illegally from Norwegian required members of the top management to be informed, or acting with disqualifying negligence. After three rounds in the Norwegian court-system, SAS-Braathens was found guilty of industrial espionage and sentenced to pay Norwegian a fine of NOK 4 million (€ 500 000) (Gran, 2007). Applying the Amoral Calculation Model presented by Lee and Gailey, a simple sketch of organisational deviance emerges:

Figure 4: SAS-Braathens Amoral Calculation (Source: Lee and Gailey, 2007)

In this case the organisation's ethics – more precisely the lack thereof - play a central role; at group level one or two persons may have shifted the consensus of all members of an involved group towards allowing for the use of illegal methods. On the organisational system level, none of the organisations had ethical awareness that stopped the illegal activities.

6.2. EMPLOYEE VULNERABILITY

Mendell (2003, pp. 111-112), Rustmann (2002, pp. 31, 158-161), and Lawton *et al* (1988) all point to the fact that the threat of industrial espionage often lies within the organisation itself. Though most companies have a protection of rights effectively covered in any employees contract, corruption in the form of selling information is one of the most common methods of conducting industrial espionage. Unsatisfied or dishonest employees are a risk in any organisation, and especially so in companies which are particular potential targets of industrial espionage. Hence employee satisfaction becomes a key strategic issue for managers. Organisations are as vulnerable as its employees are ethical and trustworthy. Considering this employee vulnerability, the risk of falling victim to industrial espionage thus starts with the hiring process.

6.2.1. THE HIRING PROCESS

The globalised information age has brought us tremendous possibilities for business and communication. It has also provided dishonest people with ample opportunity to acquire false credentials to enhance their candidacy (Rustmann, 2002, p. 160). Hence the checking of references becomes increasingly important. The information provided by an applicant himself or herself must be judged in the light of the fact that few people, if any, pass on unfavourable information about themselves. Consequently human references provided are likely to provide positive information, and it is good practice to seek alternative references that may obtain a more complete picture of the applicant's work history and performance (Winkler, 1997, pp. 304-306).

In technologically advanced economies, like South Korea, Japan, USA and most EU-countries, there is a considerable focus on academic merit and formal qualifications. Furthermore, high tech companies require a higher level of security, for instance companies working with defence or communication systems. Employees in such companies can be required to handle industrial secrets of national or military importance. Consequently a high level of relevant education is an advantage. Jong-a (2007) portrays how, in South Korea, "Diplomas from the best local universities and distinguished

overseas schools, especially in the US, are considered a ticket to success." However, several incidents of false credentials, both among students as well as among top members of society and private enterprises have been disclosed (Jong-a, 2007). In such circumstances an ordinary check with a former employer, accompanied by copies of educational certificates, will not provide enough information. Donkin (2007) portrays how the private business intelligence outfit Kroll in 2007 performed abut 70,000 job-screening assignments in its Europe, US an Middle East offices. Furthermore, most governments allow companies to apply for a more thorough background and security checks, involving criminal and financial records, when their products are fully or partly of strategic interest to the nation. The government or military authority as a purchaser of services or products often requires such checks.

6.2.2. FOREIGN SPIES

Foreign nations might very well find great interest in the products or know-how within companies working with defence or weapon systems in particular, but also communication systems, medical or nuclear research. A common method of obtaining such information is to recruit spies within the target organisations (Cornwall, 1992, pp. 35-38). This is much more effective than forced entry, theft or computer break-ins, and with a much lower risk of being found out. The recruitment of spies (also described previously in the HUMINT section of Chapter 5) often relies on where a person's loyalty lies (Rustmann, 2002, p.29). Primarily a person's loyalty lies with his or her family. After that we can assume nationality is important (Winkler, 1997, p.60). Many persons also have a great sense of loyalty towards particular organisations, companies, groups of people within companies or religion and political parties. Government spy organisations actively use their own citizens' loyalty when recruiting agents for industrial espionage among respective Diasporas. This is also called 'ethnic targeting'. CIA officials have in fact publicly stated about Israel intelligence services that they "depend heavily on various Jewish communities and organizations abroad for recruiting agents and eliciting informants' (Rustmann, 2002, p. 125). For the same reason the CIA does not send Jewish

agents in assignments in Israel; the risk of double-agent recruitment is considered too high (p. 125).

One final situation to consider here is the planting of foreign spies. If one country, nation A, produces a highly effective gun, nation B might be interested in detailed information about the production process they cannot successfully derive from reverse engineering. Nation B might then resolve to plant an agent within the Private Company X producing the gun. As government spy agency of nation B is involved, they have complete resources at hand to create a false background and technical background for a 'spy engineer' to qualify for work at Private Company X. A relevant example is all the Indian engineers working for Western companies. India experiences unprecedented growth. Consequently India's need for technological progress is massive. To what extent are Western employers doing background checks on individuals or recruiting firms?

Faced with the level of intelligence professionalism imposed by government spy organisations, managers ought to take the matter of recruitment or planting of spies within its own organisation seriously. No private company, perhaps but a few, will have the resources to monitor or detect attempts of recruitment of its employees at this level. Managers can in such cases consider hiring outside professionals from security or business intelligence outfits. Many such companies employ qualified professionals or even former intelligence agents. However, as industrial espionage and the prevention of such is a matter of national importance for any nation, it might be an equally viable option to engage in a closer cooperation with national security agencies. A combination of these two approaches is also common.

6.2.3. IN GOOD TIMES…

During optimistic periods, where businesses experience growth and better margins, the managerial focus tends to be on facilitating growth. For managers such times are fulfilling, with increased sales, better results and better bonuses. But in good times finding qualified personnel can become an obstacle for further growth. A recent example is that of Norway. Its energy-based economy has produced unprecedented times of economic growth and rise in living standards, with an equal decrease in unemployment.

At the time of writing this dissertation, the Norwegian unemployment-rate is 2,5% (SSB, 2008) while the Eurozone average was 6,8% (EPP, 2008). As ethnic Norwegians among the population in Norway grow older, new workers are needed en masse. A considerable work-related immigration is taking place from Asia and the former East-European states. In late 2007 the NSA (National Security Authority) in Norway voiced concern that the capability to perform security checks was limited partly due to under-capacity, but equally important was the lack of public records or accessible information about many of the new workers from countries like India, Vietnam, the Baltic nations, Poland or Romania. For companies working with strategic important projects with deliveries to the Norwegian armed forces, the NSA is left with two options: 1) not granting the desired level of security clearance or 2) lower its standards. The latter will, naturally, increase the risk as screenings become less thorough.

Managers faced with ample opportunity for growth, provided more people are hired to the company, run a higher risk of recruiting spies or unethical individuals. A company with a strict hiring procedure as well as a good corporate culture on risk management might stand a better chance of avoiding hasty and bad decisions.

6.2.4. CASE: A REVERSE EXAMPLE

A manager may find herself or himself contributing to industrial espionage without having done anything actively to arrive in this situation. Some managers might recognise the following; an employee from a competing firm starts working for the company or department one is responsible for. During a difficult part of, say, an engineering or software development process, this employee suddenly comes up with solutions derived from projects he or she has been assigned to at the former workplace. Perhaps downright copied source code or pieces of engineering. At the point in time at which a manager becomes familiar with information of this character, a number of serious dilemmas occur. First and foremost, people cannot *not* know. If you know, you know. This means, under the legislation in most western countries, that a manager is obliged to flag the knowledge of such information. An ethical and strong manager may try to inform the former employer, negotiating the situation into a confidential process – n avoiding bad publicity

– then dealing with the employee's unethical conduct. This could mean sacrificing an employee. There is also the risk of the former employee not honouring confidentiality, in which case the manager will also have to deal with negative PR. Many managers will therefore opt to act differently. Depending on the type of information disclosed, there may be other approaches, for example to use the situation as an example of unacceptable conduct and an organisational case of learning. I have myself arrived at this conclusion in one identical situation, but where the information provided was a third party's bidding price for a contract. We resolved to disregard the information, placing our bid at a higher cost. The employee involved clearly saw the problematic ethical side of her actions. A third and completely unethical option is of course to use the information. Then the manager is in breach of several legal and ethical principles – 1) accepting to use illegally obtained information, 2) avoiding alerting the target organisation, 3) avoiding alerting legal authorities, 4) instigating a corrupt practice in his or her own organisation and 5) becoming an accomplice in industrial espionage.

A relevant case is the Lockheed vs. Boeing 1998 bidding contest for a US Air Force rocket launch system, where a former Lockheed employee, Dean Farmer, at that time working at Boeing, was found to have provided Boeing with sensitive bidding information brought with him from Lockheed. "In an investigation the US Air Force found that Boeing had acquired 25 000 Lockheed documents during the 1998 competition" (Ferdinand, Simm, 2007).

After resolving the situation, incidents like this leave a manager with some degree of uncertainty towards a particular employee. Was it just bad judgement and a once and only incident? What happens to *our* company's secrets and know-how if he or she starts orientating towards yet another job? What are the reasons for an employee bringing sensitive information from one employer to another? A possible explanation can be internal self-promotion, or perhaps even economic motives. If the new employer knows about the information available, it could even be a part of an employment deal.

7. CRISIS MANAGEMENT

A company targeted by industrial espionage may experience the loss of sensitive information to a hostile company. In the case where the business doing the spying is a direct competitor, the costs and strategic implications are huge, in the worst case devastating for the target company. As portrayed hereto, the full scope of the industrial espionage threat can be overwhelming for a leader. How can these threats be met effectively at the managerial level? This chapter aims to provide some practical perspective and guidance on how to meet this threat.

Considering the financial and technological impact associated with industrial espionage, it is, for the victim company, nothing short of a crisis. Leadership techniques used to plan for and manage a crisis should therefore be transferrable for the purpose of handling the threat of industrial espionage, as well as the results of an attack. As Fink puts it (2002, p. 7): "Anytime. All the time. Be vigilant. Be prepared."

A pragmatic definition of a crisis is *a turning point for better or worse*. Fink (2002, p. 15) points to the importance of being able to predict and plan for a crisis. He defines the anatomy of a crisis to include four defined phases; the prodromal crisis stage, the acute crisis stage, the chronic crisis stage and the crisis resolution stage (p. 20). The prodromal stage is the pre-crisis stage, where small signs can bear warning of a crisis in the making. For instance, a security glitch in your IT-system could be a prodrome for a possibility of an industrial espionage attack. The acute crisis stage is when the crisis situation is acknowledged. For our purpose, the acknowledgement of when we have a crisis could originate from at least three situations: 1) discovery of a possible information leak via employees, communications or IT-systems, 2) firm knowledge of an information leak to competitors or 3) firm evidence of industrial espionage for example in the form of the emergence of a copy-product or a perfectly timed counter-attack on market strategies. The chronic crisis stage describes the phase when companies deal with the crisis, cleans up and recovers from it. Finally, the crisis resolution stage "is when the patient is well and whole again" (Fink, 2002, p. 25). This is when the organisation can look forward

again. Figure 6 compares these crisis phases described by Fink with the anatomy of a successful industrial espionage attack.

Stage	Characteristics	Approach
Prodromal Stage	Continuous threat of being targeted in industrial espionage	Continuous organisational alertness on the threat of industrial espionage, contingency planning
Acute Crisis Stage	Your organisation is in fact targeted, theft of strategic/sensitive information is a fact	Assemble crisis team, identify key crisis – namely what information is stolen by whom, isolate the crisis – avoid spreading or escalation, manage the crisis, gather all available information, start assessing damage scenarios, try legal avenues if applicable
Chronic Crisis Stage	A competitor has started producing "almost-copies" of your product at a quarter of the cost, the financial and strategic strain on your company is severe	Assess why and how, re-organise if necessary, management replacements, use learning's for further and better threat-management
Crisis Resolution Stage	Your company comes out of the crisis, business continues	Handling technological and strategic damage caused by the attack, looking forward with a higher alertness

Figure 5: Crisis stages (Source: Fink, 2002)

As Figure 5 shows, the phases in a crisis, and the subsequent techniques described by Fink to manage a crisis, correlates with the anatomy of an industrial espionage attack. In an everyday management perspective, managers will have to focus on the prodromal phase, where the continuous threat of being targeted lingers. A related perspective presented by Nasheri (2002, p. 50) describes how the very nature of the global economy, where companies are "increasingly forced to share critical proprietary information with customers, contractors, consultants, and strategic partners during early stages of product development." Again, the expression 'business is war' seems apt. In a context where the

current global business climate presents a continuous prodromal crisis, the old military strategies of Sun Tsu strengthens the argument of a heightened awareness (Cantrell, 2006, p.32): “You can be sure of succeeding in your attacks if you only attack places which are undefended.”

Leaders must plan for the inevitable, and should instigate a scope of counter-measures relevant to the perceived threat to the organisation. But as the context in which a business operates is continuously changing, it leaves leaders with an ever-changing risk scenario. Changing cultural, economical or business specific factors contribute to the need for a contingency-based leadership to effectively face the risk of industrial espionage. The Fiedler contingency model, referred by Robbins (2003, pp. 320-322), describes an approach where one is “matching leaders and situations”. Furthermore, the performance of a task group, here the crisis group, is influenced by how the leader’s style matches the situation at hand and the context created by this situation. Different contextual situations call for different leadership skills.

The process of protecting an organisation from industrial espionage attacks is continuously changing. In particular the cyber-crime approaches change rapidly, troubleshooting new threats is an ongoing process. People who lead under such circumstances will benefit from a high capacity of logic thinking, quick assessment and the ability to perform well under stress. Managers responsible for counter-measuring the threat of industrial espionage should select a situational leadership style in order to create a high level of readiness among the team. Leaders with high tolerance for ambiguity will be better equipped to interpret threat situations, and to use the collected data from the different threats to adapt effectively to these situations.

7.1. FINANCIAL IMPACT

For a business that falls victim to successfully targeted industrial espionage by a competitor, the resulting financial losses can be of disastrous proportions. Depending on the significance of the information stolen, a competing business could make stellar technological progress in a field it does not have the sufficient expertise to exploit successfully. It is much cheaper to steal a product-idea than to fully develop it. For the

spying company the gains can be astronomical. In a report to the U.S. Congress in 2001 the National Counterintelligence Executive claimed economic espionage against U.S. businesses could be costing up to $ 250 billion a year (Fink, 2003, p. 7, Nasheri, 2002, p. 59).

Depending on the complexity of a product or concept, competitors with the wrong intentions could produce a product or prepare for a service parallel to the inventing company's efforts and development. If the espionage efforts successfully allows the spying company to obtain sensitive information illegally and undetected, the victim company's market could be completely undermined with lower-priced products from the spying company, but at a better revenue than the inventing company, which has had to bear the cost of product development. The more complex a product development phase is, the more a company stands to lose if it is targeted by industrial spies. Fink's Crisis Barometer, a graphic presentation of the impact of a crisis, is relevant here.

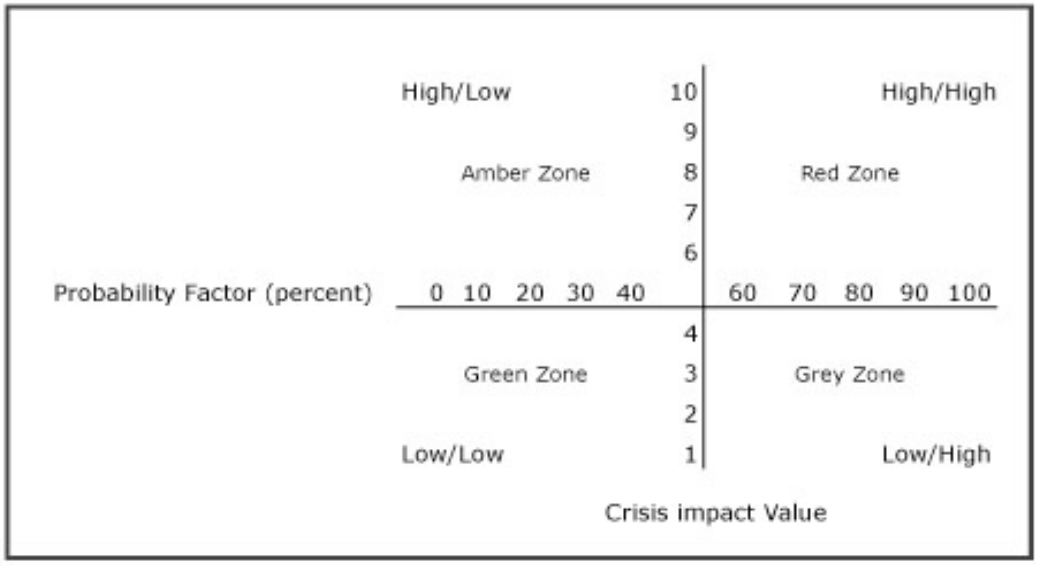

Figure 6: Crisis Barometer (Source: Fink, 2002, p.45)

Given that a company develops new technology competitors can benefit from, the probability of industrial spies targeting this particular new technology is high. The impact of a successful espionage attack on a newly developed product will be equally high, as

argued above in this segment. The probability/impact factor places the attack in the High/High area. This is a major crisis with major financial impact. An opposite example; a product in a late, declining market-phase is less likely to attract spies because the financial gains will be low for the spying corporation. The financial impact will be low for the target company. The probability/impact factor places this scenario in the Low/Low area.

Another perspective is shareholder value. If industrial spies target a public company, and if the information about this company falling victim to industrial espionage finds its way to the financial press (it often does), the financial markets and investment communities will act negatively. In other words, industrial espionage influences the overall value of the target company. Referring again to Figure 7, a high probability of information leaks, as well as a high financial impact provides another High/High scenario.

Spying on competitors to gather sensitive information about market strategies also represents a considerable threat, with a likely big negative financial impact, for the victim company. Launching products into new markets require costly and time-consuming market analysis, including demographic and cultural analysis, researching and planning of marketing campaigns, negotiating local distribution deals, acquiring licenses from the local authorities etc. The initial investment made by a company is considerable. If a competitor offering equal or similar products acquires such information illegally, economic gains are equal to the invested sum at the victim company. The company involved in this type of industrial espionage can surf into the same market, acting on the same strategic material and analysis their competitor has, but at a much lesser cost. Again the target company can be out-priced, still at better margins for the spying company. Market shares are reduced and revenue is lost for the target company.

Financial information can also be of great value for competitors, and therefore is a likely target for industrial espionage activity. In a situation where several businesses are bidding for the same contract, sensitive information disclosing bad liquidity and financial stress at one of the businesses can be used by others to doctor their bid to place the victim company in financial trouble.

In a different perspective, when planning a take-over of another company, corporate intelligence plays an important role in the gathering of strategic information about the target company. In the case of a hostile take-over, the buying company might depend heavily on corporate intelligence, possibly also utilising industrial espionage to obtain the desired information.

7.2. FORMULATING STRATEGY

The threat of industrial espionage is part of the context for the strategy formulation process. Hence, the process of strategic assessment needs to address the risk of industrial espionage.

Herring (1992b) emphasises three major inputs for a good strategy formulation against the threat of industrial espionage; 1) your own company's resources and capabilities, 2) the company's external environment, the business context in which it operates and, importantly, 3) the collection and analysis of information on the competition and its external environment and any factors that affect their competitiveness. The latter is important because it provides an understanding of a competitor's likely needs and wants. This input then becomes valuable in the strategic formulation process when assessing threat-levels; which among the competing organisations represent the highest risk of spying on you? Which have the most to gain from getting access to your strategic information? Ironically, a consequence of this is the fact that good business intelligence lays the groundwork for good, preventive informational input into that part of the strategy formulation process that is aimed at fighting off industrial espionage.

Winkler (1997, p. 12) argues that risk is the core of espionage. Referring again to the Risk Equation Model (Figure 1.), a company's vulnerability, and any weaknesses in a company's countermeasures, are what spies exploit. Logically, avoiding industrial espionage is the sensible strategic intent for any organisation running a risk of being spied on. A strategic assessment considering the value, risk and vulnerabilities will help in defining a preventive, strategic approach.

An example: a European company considers introducing a fresh food product in an Asian country. Two options for regional production are available: 1) in-country, where local government requires a joint-venture operation with a national producer, and the country is well known for its industrial espionage activities, and 2) farther away in a country with a more transparent economic culture, but also 40% more expensive. Where does the company locate its production, involving technologically sensitive activities? The increased cost must be juxtaposed with the level of risk of being targeted, and the potential economic loss of losing the recipe to government-backed competitors.

Assessing, discovering and selecting the right counter-measures should be considered an intrinsic part of the process of formulating the strategic choices of a company. With this in mind, at what levels in the organisation should technology-based companies implement concerns for industrial espionage? As discussed in the previous chapters, many levels of an organisation will be affected by the threat of industrial espionage. Marketing and PR in relation to what can and cannot be communicated, the IT-department with regard to computer and Internet security, the H&R department with regard to recruitment and hiring processes, research and development as well as production departments with regard to restricting access, and communication procedures with regard to restricting distribution of sensitive information and the means of communication.

7.2.1. PUBLIC STRATEGY

Information and PR strategies are worth a particular scrutiny because they are very difficult to control during a crisis situation after or during an industrial espionage attack. Naturally, companies with a thorough crisis communications strategy will be much better prepared to deal with the immediate consequences. Fink (2003) describes a hands-on, cut-to-the-bone communications strategy. First – the key message points need to be established, making the communicator able to present the story quickly and with a logic rationale that the media easily can convey to its audience (p.136). Second – an internal Q&A sheet circulated throughout management level in order to collect all relevant knowledge within the organisation (p. 137). Third – employees, the financial community

and key customers and suppliers must be notified before the story breaks in the media. Though a victimised company clearly has not done anything wrong, public knowledge of the fact might still hurt the company, and subsequently shareholder's value.

Does the communication strategy presented by Fink represent a feasible and sound approach for a company targeted by industrial spies? In essence the strategy describes know what to say, how to say it and make certain the key players in your economic and industrial sphere hear it from you first. A clear and logical message will convey that you are in control of communication, but it will also communicate that you are in fact managing the crisis.

Fink argues it is a relevant question whether a company should go public at all, or just keep quiet and sit it out – a "sadder but wiser" option (2003, p. 116). From my own experience working in the news media, my assessment is that a complete control of a negative message is unrealistic. Good PR strategies handled by PR professionals are helpful, but provide no guarantee for which direction a story will play out in the media. What other stories are out there about your company that might influence this story? An example; Company A in the UK is a victim to industrial espionage. The evidence is there: let us assume a small time Brazilian Company B has successfully copied a product and beat the Company A to market. But, three months ago a story about inadequate leadership in the UK Company A ran in the financial press. This story will inevitably be linked to the new industrial espionage story, presenting a hostile press with a drama of an alleged inept management. So, instead of sympathy we get a triple crisis; 1) the original industrial espionage crisis, 2) a PR crisis and 3) a financial crisis due to both loss of revenue because of the industrial espionage and a loss in shareholder value because of bad press.

Lawton *et al* (1988) reveal responses from a questionnaire circulated among business professionals in the UK in 1988 that portrays a culture where serious cases, perhaps involving high-profile staff, were simply not aired in public. Furthermore, according to the same sources, a victimised company will seek to keep such information out of reach of their clients and competitors. Indeed much has happened over the last 20 years, not least on the information scene. However, the patterns described by Lawton *et al* are consistent with what Fink questions based on the current 21st-century media situation. But, how risky is it to keep quiet? In the current information-driven, global

economy, information travels incredibly fast. Information that is not intended for the public travels faster than anything. The risk associated with keeping quiet is therefore linked to the organisation's ability to contain information effectively – without leaks. If management opt for secrecy, but the information still leaks, the damage is that much greater because the initial secrecy will look suspicious. The end result is both an offspring crisis, and a boost to the original crisis.

A targeted company will, in order to get the case investigated, have to involve the respective national police authority's economic crime unit. However Fink (2003, p. 115) presents an important point here; the economic crime unit can have a different agenda than that of the victim company. Consequently the company loses control of the process: the implications here are severe.

A closer look at the alternatives for a targeted company reveals at least three options; 1) go to the proper police or intelligence authority, 2) litigation against the alleged thieving company or 3) do nothing. Fink argues alternative 2 and 3 gives some sort of control to the targeted company, but when organisations like the FBI or other nations' equivalents go to work, they can take control of the process (2003, p. 116), and make their own priorities – not necessarily in your company's best interest. Again, when assessing which strategy to choose after the attack, it is paramount to evaluate if other circumstances regarding your company might play negatively into a public investigation. What, for instance, will the public investigators say about your company? Will they perhaps send out a message portraying bad internal security? How will competitors react? How will the stock exchange and stockholders react?

7.2.2. INNOVATION / R&D

For innovative, technological start-ups a difference in interest exists between the innovators' need to show their invention in order to mate with investors, and the need to keep secrets to prevent persons from stealing their commercial ideas. The paradox of wanting to sell their idea of a product, but not disclose any information, is difficult. An illustrative example is presented by Penenberg and Barry (2000, introductory chapter), where a group of venture capitalists were gathered for a pitch on a new high-tech idea in

Silicon Valley. A seasoned industrial spy attended the pitch on behalf of a client, and immediately noted that everyone in the room except the entrepreneur were corporate spies. Innovative processes often involve establishing new companies. Entrepreneurs are, to say the least, very vulnerable to industrial espionage.

Patents provide some protection, and should ideally be in place before external persons are allowed to see sensitive material, drawings, sketches or CAD-models. However, this is often difficult as investors and financers will need to see solid evidence of a product-idea before they decide to invest, and the entrepreneur needs the money to develop further and file a good patent that will protect the product's market position. NDAs (Non Disclosure Agreements) can also provide some judicial protection prior to a patent being in place, but is judicially more difficult to enforce than a patent as, for instance, a venture capitalist could easily say he or she was given the same pitch by somebody else, but he or she cannot provide evidence to this fact as that would mean a breach of another NDA.

Is keeping it completely secret the safest approach? Forming alliances with companies or people with complementary knowledge is a common approach for innovators when seeking to solve a technological problem. In order to do so, entrepreneurs need to disclose information. With an NDA-based approach, the dilemma of disclosing information in exchange for better technological knowledge should be considered from situation to situation, paying attention as much to the possible gains from sharing information, as the need for keeping secrets. One may justifiably think that many entrepreneurs block their own ideas' full potential through exaggerated secrecy.

Entrepreneurs go through a series of typical phases. Based on my own experience as an entrepreneur in several companies, but also on the overall perspective of the literature reviewed for this dissertation, I present Figure 8 on the following page, which portrays the risks of industrial espionage associated with the typical entrepreneurial phases.

Phase	Risk of espionage/theft	Comment
Idea-creation	Very high	Anyone you show the idea to could steal it
Filing patent demands	Medium	Filing patents allows the larger professional organisations, which search for newly filed patents regularly, to read your demands. Complete secrecy is an alternative.
Search for technological partners	Very high	Potential partners will need to see your idea to evaluate it, and are likely to know more about what is technologically and commercially viable than you
Search for start-up investors	Very high	Entrepreneurial presentations attract industrial spies, where they can get valuable information about you from a competitor's perspective
Teaming up with technological partner	High	Trust and information sharing are important
Teaming up with financers	Low	The entrepreneur and the investor will have common interests in commercial success
Developing / designing your prototype product	High	During this process the patent is usually not completely in place, as the development will reveal technological points for a revised filing of patents
Presenting the product to the market	Medium	Again, patents fully covering the competition

Figure 7: Entrepreneurial risks

Comparing the above scenarios with the risk-equation model (Figure 1, page 45), we see the potential loss in value – here the revenues lost due to an act of industrial espionage –correlates with the value and risk variables described in the risk-equation model. The Very High phases Idea-creation, Search for technological partners and Start-up investors also places themselves in the High/High area on Finks Crisis Barometer (Figure 6, page 61); the probability is high – so is the financial impact for the entrepreneur.

8. INFORMATION SECURITY

IT systems are the backbones of a vast majority of businesses. Strategic and financial information is stored in the IT-system, as is intellectual property. The threat of being subject to industrial espionage is entangled with a company's information security. For technologically advanced companies, IT systems are instrumental in carrying out any activity within production, research & development or administration.

According to Fink, "The Internet is the fastest growing technique for foreign firms to obtain sensitive business information," (2003, p.119). Industrial or economic espionage via the Internet, 'netspionage', (pp. 120-121) involves professional spies who break into competitors' networks and steal information. However, to counter this threat, Calder and Watkins (2006) point to how an information security management system (ISMS) represents in itself an organisational, systematic approach to meet the threats to the availability, integrity and the confidentiality of an organisation's information (p. 9). Incorporating ISMS into an organisation's culture and strategic thinking is a first and key step to meet the continuously increasing information security threats.

8.1.1. CYBER THREATS

The Internet is a dynamic, public space, and there is no built-in endpoint security. Anyone can log on. Communication between computers logged on is done via different protocols. Because the access point is the Internet connection, practically any attempt getting access to company servers can be categorised as a cyber threat. Given the fact that practically all information is stored digitally somewhere in an organisation, an inevitable consequence is an increased risk of information leakage by an industrial espionage attack via the Internet. New challenges require new strategies and new assessments of risks. As Nasheri (2005, p. 13) points out, "The Internet is making it easy." Because the information age has created a whole spectre of new crimes, ranging from malware and

illegal copying to intercepting techniques and computer break-ins via Internet connections, a corresponding risk of being subject to industrial espionage occurs. Calder and Watkins (2006, pp. 16-19) put further weight to an increasing risk-scenario by pointing to trends that are likely to worsen the information threats: the increased use of distributed and mobile computing, as well as wireless communications, combined with the increase in business communication over Internet, create new and more severe information threats as criminals and hackers become more sophisticated, and to a greater extent cooperate.

File sharing protocols like BitTorrent present yet another sophisticated threat as this type of software uses all logged-on computers' resources to process and share data. Similar techniques can be used effectively for espionage purposes via Bot armies; sleeper software that stays undetected for months or even years before it is called to action via the Internet (Altucher, 2007). The successful installer of such malware, designed, for instance, to seek out particular types of information, can acquire information at a later time and sell it to the highest bidder.

The risk of being targeted by industrial spies, and the perceived threat associated with the risk, are then closely linked both to a company's level of IT security and to its communication procedures over the Internet.

8.2. CASE: TROJAN ESPIONAGE

Cyber-related threats can be difficult to grasp as they appear only in the virtual cyber universe. Hence, it requires discipline to maintain a reasonable approach. In a concrete example, reported by the BBC Radio 4, *Bugging the Boardroom* (BBC, 2000), Israeli police discovered that a computer expert living in London, Michael Haephrati, and his wife Ruth Brier-Haephrati, were running a highly sophisticated industrial espionage scheme targeting Israeli businesses (Wallis, 2005). The expert and his wife had designed a Trojan capable of escaping the scrutiny of virus software. Once installed, the Trojan software provided access to sensitive information, without firewalls or other IT-security measures discovering the activity. The Trojan was allegedly spying on the RaniRahav PR agency as well as Champion Motors, importer of Audi and Volkswagen cars. The

information provided was sold to private investigators working for other Israeli companies, spying on their competitors.

The Trojan was distributed and activated via email attachments or CD-roms. The technique used was that Ruth Brier-Haephrati would call up executives with an effective telephone pitch on a hoax business deal, followed up by emails and a CD mailed to an executive in the company because the contents were said to be commercially extremely sensitive. Once the CD was installed on the executive's PC, the Trojan was let loose – undetected. For our purpose in this dissertation, the installation of the CD-rom is the failing point in IT security. And it becomes increasingly interesting to learn how easily the spies gained access to presumably high-security IT systems (Fink, 2006, pp. 129-132).

This case portrays clearly the difficulties involved in maintaining a secure IT infrastructure. Spies, or hackers working on their behalf, are often savvy computer professionals operating one step ahead in the IT-security business. Managers and IT-security officers need to be aware of this threat, and not trust traditional firewalls and anti-malware for its entire IT security. The CD scam in this case is also a prime example of how endpoint security glitches can allow industrial spies to cause severe damage to a company.

8.2.1. ORGANISING INFORMATION SECURITY

Again, a risk assessment is the sensible start for an effective evaluation of the information threat against a company. Calder and Watkins (2006, pp. 46-47) rightly state that in order to achieve a level of information security that effectively meets the threat, security goals should be identified and clearly formulated. When objectives and plans are established, they should be communicated throughout the organisation. A manager responsible for this should be appointed. These steps make up the skeleton of the ISMS as described by Calder and Watkins.

But as the dynamics of the Internet age continuously alter the threat scenario, how can an organisation routinely and effectively review its ISMS? A cross-functional management team is a likely good approach, as it provides input from respective

departments as well as different professional perspectives. Also, outside input from relevant authorities such as national security organisations and outside specialist environments would provide valuable knowledge when reviewing the ISMS.

Calder and Watkins (2006, p. 119) suggest further a system that classifies and labels information. This is a parallel approach to the intelligence services' Unclassified, Confidential, Secret, Top Secret and the NATO clearance Cosmic Top Secret. With regard to preventive actions against industrial espionage, a labelling system will provide management with a simple ISMS tool:

Information which...

SEC 1 ... the organisation wish to keep private
SEC2 ... could cause significant harm to the organisation's interests
SEC 3 ... could cause serious damage if disclosed to competitors

Organisations with a graded labelling system like the one described here should emphasise that their IT system stores, regulates access to and handles information in consistence with this policy. But, how preventive is such an approach with regard to industrial espionage attacks? Nasheri's (2005, p.73) categorisation of sensitive business information into 1) intellectual property; patents, manuscripts, inventions, formulas etc., and 2) operational information; production details, strategic details, financial and marketing details and so forth, must under this scheme be treated as SEC 2 or SEC 3 information. The restriction of information spread within an organisation will, quantitatively, lower the risk of leaks. However, if professional netspionage operators manage to hack into a system, there will be a chance that they are savvy enough to hack their way to the inner core of a system – to SEC 3. In this perspective, the internal grading of information becomes useful as a means of restricting possible leaks via employees, but as long as a computer is connected to the Internet, its contents are never really safe.

Yet another challenge is social engineering, meaning manipulating someone into divulging information he or she would not do without the effort of a trustworthy 'social

engineer' (Fink, 2003, pp. 129-130). In other words a HUMINT method, like what Cornwall (1992, p. 35) describes as unaware agents. No matter how good your ISMS approach is: if passwords, strategic information or intellectual property can be socially engineered out of your employees, the new state-of-the-art firewall is not useful. Ironically, the attacks carried out by the Haephratis were aimed at the management, and therefore bear clear evidence of how important it is that all levels of an organisation are included in awareness programs.

Virtual societies like Facebook provide an arena for digital social engineering. Here, other conventions apply for how people interact than in real life. For managers, the risk of social engineers attacking your employees, present an ambiguous challenge; a focus on awareness can be helpful, but there are limits as to how deep into the personal sphere of its employers management can be – or is – allowed to reach.

8.2.1. INFORMATION HANDLING

Classifying information has two preventive effects: it restricts access to authorised individuals, and it raises awareness of the strategic importance of the information, helping create a cautious culture. Under classified information schemes the need arises for an evaluation of what individuals need to have access to what information in order to do their job. Such restrictions should not influence production flow or a sensible flow of information. If it does, the result will be loss of efficiency. But the process of evaluation of individual's suitability to handle restricted information, and verification of an individual's need to access sensitive information, builds organisational awareness.

Information handling when dealing with subsidiaries, subcontractors, clients and associated companies is particularly sensitive. A routine for verifying identities of individuals, their respective role in projects as well as the purpose for why they might need information, is an effective approach to externally restrict unwanted spreading of sensitive information. As an example, the engineering company where I work experienced a quite fresh approach from a Scottish subsea operator; the Scots were in negotiations for an ROV-operator contract with one of our clients, and during the process resolved to place a call to our project engineer for specific technical details regarding the

ROV-tool we were commissioned to build for the same client. When checking the Scot's credentials and authorisation to have access to this information we were told specifically not to convey it. Firstly negotiations were not concluded, and secondly this particular information would provide the Scottish subsea operator with knowledge it could use actively in its negotiation strategy.

8.2.2. THE IT SYSTEM

An overall ISMS-based approach, as described by Calder and Watkins (2006, pp. 147-155), involves a structured view on the whole IT-system, where the physical security is emphasised. Examples of physical factors are choice, maintenance and placement of equipment, the quality and physical placement of cables and routines for taking laptops off-site (pp. 160-165). However, the level of security accomplished is restricted to the physical perimeters of your own IT-system. If employees for instance bring computers off site, there is a whole new situation. Such information security issues that occur where the company security system ends, for example smart-phones, home computers, company laptops taken off-site, USB sticks, MP3 players etc., is described as endpoint security (Calder and Watkins, 2007, p. 184). Importantly this is an entry point for malware, and where industrial spies might find the opportunity to snatch information or plant spyware. Again, the Israeli case is a n excellent example because the attack was comprised of at least two elements: one social engineering part, and one endpoint security failure.

Other basic pre-emptive steps described bye Calder and Watkins are continuous, updated and cross-organisational installation of antivirus software, a hierarchal storage of data with access limitations according to individual needs, and the use of passwords in logons.

A next level of security is to ensure quality and security during remote logons, and to restrict these logons to a minimum. Temps, individuals from subcontractors or clients should only be given basic, time limited access when absolutely necessary. Wireless networks are practical, but much easier to hack than cable networks (Calder and Watkins, 2006, p. 17).

Back-up of information is crucial. This should be a routine procedure shifting data from the company's server discs to a remote, secure location. As soon as this process is in place, a new risk-analysis should be carried out in connection with the external data transfer routine. In effect the risk of industrial spies targeting your information has now doubled, as information is stored in two locations. However, the risk of losing all information in a computer crash outweighs the risk of industrial espionage.

8.2.3. SPYWARE

Malware consists of viruses, worms or Trojans designed for malicious purpose ranging from the rather innocent jokes that pop up on a screen to complete computer breakdown, and spyware. A virus depends on a host file and is capable of replicating itself. A worm does not depend on a host file, and is autonomous. It spreads via transmission mediums such as emails, IRC, network transmissions. Polymorphic worms are capable of changing in the wild, making them difficult to detect. A Trojan conceals hostile code within what seems to be bona fide code. It is designed to be launched inadvertently, often with the aim of seizing control of the target PC or computer system. Spyware is specifically designed to gather information.

The threat of all malware can be met effectively with anti-malware software. However, great care should be taken in choosing software that is effective and has a high rate of updates. The speed at which hackers produce new malware is astonishing; in order to be effective, updates of malware definitions must be done several times each day.

8.2.4. HARDWARE

The ISMS should describe how to dispose of media like hard drives, portable USB discs or portable discs. Ideally, all media drives should be neutralised (reformatted, de-magnetised) before disposal. Disposal of hardware represents an endpoint information security challenge. Old laptops, hard drives, USB drives and other digital media should be degaussed or their hard drives completely destroyed in order to avoid unwanted

information leaks. One relevant example of how important this is was revealed in a BBC one broadcast on August 14th, 2006, in the programme *Real Story* (BBC, 2006). Here the BBC portrayed how the bank account details of many Britons were lifted from used computers sold to Nigerian operators. Even though the computers' former owner may erase such information, a computer specialist can easily retrieve passwords, personal information, financial or other business information unless the hard drive has been re-formatted, or even better, completely destroyed. No wonder, then, with all the Nigerian scams…

8.2.5. CRYPTOGRAPHY

One of the biggest risks of information theft occurs when exchanging information via email. As described in Chapter 5, the methods and resources available to industrial spies for accessing emails are advanced and far-reaching. The ISMS should describe routines for what information is allowed to send via email.

Cryptography is an effective and relatively cheap way to reduce the information threat, especially when bringing laptops off-site. Hard drives that carry sensitive information and are brought off-site should be encrypted. This will provide a technological obstacle for industrial spies, and hence reduce the risk of theft of sensitive information. Yet as with all IT-related issues, there is no guarantee.

8.2.6. PERSONAL NEGLECT AND METADATA

Metadata is hidden information about a document, explained in detail by Mendell (2007, pp. 3-21). With respect to economic espionage, this is an especially important risk because it allows for deleted information not intended for circulation or outside reading to be disclosed. How? Hidden in layers underneath the visible text and layout in, for example, a Microsoft Office document, a history of revisions, tracked changes, identity of contributors, identity of readers, references to other documents, comments, dates of filings, deleted material – and more – is stored as metadata. Failure to use the Microsoft

'Remove Hidden Data' option will provide any reader with the possibility of discovering business secrets. Savvy computer operators will have little trouble finding the full document history. A single employee's neglect can jeopardise a whole organisation's strategy by providing competitors with free information. Naturally, for collectors of business intelligence, documents with a complete metadata history are very valuable; not only do they provide sensitive information but do so at the fraction of the cost of pursuing other, covert sources.

Ward (2003) explains how metadata can be used by the media. In one incident during the Washington sniper case, the Washington Post was allowed to publicise a letter. The letter contained names and telephone numbers not meant for publication. The newspaper tried to hide the sensitive information with black boxes. Online readers easily removed these boxes.

To give a further perspective, Ward cites how computer researcher Simon Beyers gathered about 100,000 Word documents: "In a research paper about the work Mr Byers wrote that about half the documents gathered had up to 50 hidden words, a third up to 500 words hidden and 10% had more than 500 words concealed within them." In other words, the prevalence of hidden, sensitive metadata is considerable, and should be taken seriously with respect to information security.

8.2.7. GOOGLE HACKING

Google makes up a substantial part of most people's lives. Search engines have quite sophisticated search options built into their search algorithms. A sleuth fluent in the syntax of Google search terms and operators can perform very precise searches, penetrating deep into sensitive areas of a server or document, provided the unit or document is facing the Internet without proper information security. Mendell (2007, pp. 30-36) points out that the Google search syntax is very effective when narrowing a search. It can, for instance, be used to look for passwords on Microsoft servers, or specific unpublished documents facing the web.

As an example I have performed advanced searches on Google Norway to see what information I could find about competitors in the subsea/engineering market. The search

‘confidential “petrobras” filetype:pdf’ for the last six months returned about 90 documents, among which were confidential presentations held for stockholders or competitor analyses performed by a financial organisation.

9. CONCLUSION

9.1. CONSTANT THREAT FROM PROFESSIONAL SPIES

First and foremost managers must acknowledge the threat of industrial espionage is a constant factor in contemporary business life. There are no indicator of a decrease in activity; it is here to stay. An inevitable consequence is that all activities relating to prevent industrial spies from targeting an organisation must be continuous.

Secondly, managers must realise their adversaries are not simple backyard detectives, but highly skilled professional spies using the same espionage methods whether they work for a government intelligence agency or a business intelligence outfit. They are technologically advanced, whether they use HUMINT, SIGINT or cyber attack techniques.

9.2. INFORMATION SECURITY IS THE FRONTLINE

The information age presents leaders with new and unprecedented challenges in keeping industrial and business secrets. In the globalised world, information in the form of technological and commercial secrets travels fast. Hence, the most imminent threat of industrial espionage is via cybercrime attacks. An effective ISMS emphasising IT security, with particular focus on endpoint security, is therefore very important. The ISMS should also regulate restrictions in access to information, with a grading system for clear categorisation of information.

Any piece of information stored digitally is physically stored somewhere. Managers must act accordingly in response to this threat. Avoidance to do so borders on the naïve.

9.3. COMPANY CULTURE

The company culture is important both in the context of how effective a company is in meeting the threat of industrial espionage, but also with regard to whether a company or its employees will resolve to use methods of industrial espionage for their own gains.

Awareness programs will help managers in establishing a sensible level of knowledge and routine among employees. Managers should clearly communicate the risks involved, emphasise company values, ethics and accepted practices for information gathering.

9.4. BUSINESS INTELLIGENCE

Information is key in the competitiveness of the information age. Companies should therefore take their own business intelligence seriously. Open-source collections of business intelligence from public registers, websites, press releases, stock exchange information, financial records etc. provide strategic information on competitors. Business intelligence provides strategic input when formulating strategies, not least when formulating strategies to avoid being victimised by industrial spies.

Vice versa, a company should take other companies' business intelligence efforts into account when publishing their own information.

9.5. RISK ANALYSIS

A risk analysis is an effective tool to describe concretely the risk of being targeted by industrial spies. Such an analysis should provide a realistic sense of what values a company possess, a ditto scenario of possible threats, and finally a guide towards a responsible program of counter-measures.

A counter-measure program should include an effective ISMS, emphasising information handling routines, company culture and compliance of information handling towards marketing and PR departments.

9.6. THE VULNERABILITY OF HAVING EMPLOYEES

The ultimate risk of hiring a new employee is that one could hire a spy. The company culture influences the workforce's sense of belonging and perception of doing something meaningful. Dissatisfied employees are more likely to find arguments for disloyal conduct towards one's business. A good working environment helps prevent disloyalty.

Effective hiring processes should of course include proper background and reference checks.

9.7. INCREASED OPENNESS INCREASES RISK

The globalisation of markets, and the increased openness and transparency of societies, also brings about a higher risk of being targeted in industrial espionage. Theft of intellectual property, illegal copying of the works of creative businesses or illegal reproduction of products all require some level of industrial espionage activity. The ISMS should address these issues, with instructions in particular on what information to publicise and what not.

9.8. CONSIDERABLE FINANCIAL IMPACT

Protecting critical knowledge is key to defending a technologically advanced company's competitive edge, and as a consequence, its finances. The financial damages to a company subject to industrial espionage can be severe, at worst fatal. The economic gains harvested by the spying company can be tremendous because the knowledge acquired illegally both creates strategic advantages versus competitors, but at a fraction of the cost because the victim company has funded research and development. This enables the spying company to produce and sell the same products or services at a lower

price, but with higher margins. Under critical circumstances this could simply put the victim company out of business.

9.9. RELEVANT LEADERSHIP TECHNIQUES

The process of protecting an organisation from industrial espionage attacks is continuously changing. As, especially, cybercrime approaches change rapidly, troubleshooting new threats must be an ongoing process; hence leaders with a high capacity for logical thinking, quick assessment and the ability to perform well under stress are best equipped. A dynamic leadership focusing on contingency plans, similar to what is used in crisis management, is useful both as a preventive approach as well as a technique to handle the consequences of an attack.

9.10.PERSONAL EXPERIENCE

The process of writing this dissertation has provided me with a theoretical overview of the strategic and managerial challenges associated with industrial espionage. However, to further analyse the challenges, a quantitative method involving questionnaires and free interviews with operatives as well as victims would provide additional perspectives. Given the secretive nature of the subject, substantial resources would be needed for the required research to collect information about a reasonable amount of actual industrial espionage cases. This has not been available to me during the research for this dissertation, but I allow myself to point in that direction others who find the subject interesting and with access to better resources.

10. BIBLIOGRAPHY

Books

Calder, A. and Watkins, S. (2006), *International IT Governance*, Kogan Page, London.

Clavell, J. (1981), *The Art of War*, *Sun Tzu*, Hodder and Stoughton, London.

Cornwall, H. (1992), *The Industrial Espionage Handbook*, Ebury Press, London.

Clinard, M.B. and Yeager, P.C. (2006) (1980), *Corporate Crime*, Transaction Publishers, New Jersey.

Fink, S. (1986/2002), *Crisis Management: Planning for the Inevitable*, iUniverse, Lincoln, Nebraska.

Fink, S. (2002/2003), *Sticky Fingers: Managing the Global Risk of Economic Espionage*, iUniverse, Lincoln, Nebraska.

Mendell, R.L. (2003), *The Quiet Threat: Fighting Industrial Espionage in America*, Charles C. Thomas, Springfield, IL.

Mendell, R.L. (2007), *Document Security: Protecting Physical and Electronic Content*, Charles C. Thomas, Springfield, IL.

Nasheri, H. (2005), *Economic Espionage and Industrial Spying*, CUP, Cambridge.

Penenberg, A.L. and Barry, M. (2000), *Spooked, Espionage in Corporate America*, Perseus Publishing, Cambridge, MA.

Perman, S. (2005), *Spies Inc.*, Prentice Hall, New Jersey.

Robbins, S. P. (2003) *Organizational Behavior*, Prentice-Hall, New Jersey, USA.

Rustmann, F.W. Jr. (2002), *CIA Inc: Espionage and the Craft of Business Intelligence*, Brassey's Inc, Virginia.

Winkler, I. (1997), *Corporate Espionage: What It Is, Why It Is Happening In Your Company and What You Must Do About It*, Prima Publishing, USA.

Printed articles

Bremmer, I., Charap, S., Washington, USA (2006) The Siloviki in Putin's Russia: who they are and what they want, *The Washington Quarterly,* Winter 2006-2007.

Economist (2008), Whodunnit, *The Economist*, February 21st, 2008.

Ferdinand, J. and Simm, D. (2007) Re-theorizing external learning: insights from economic and industrial espionage, *Management Learning*, 38 (3).

Gobert, J. and Punch, M. (2007), 'Because they can' in: Pontell, H.N. and Geis, G. (eds) (2007), *International Handbook of White-Collar and Corporate Crime*, Springer Science and Business Media, New York.

Gran, B. (2007), Convicted of Espionage, *DagensNæringsliv* (Oslo, Norway), December 22, p. 19.

Herring, J. (1992a), Business Intelligence in Japan and Sweden: Lessons for the US, *The Journal of Business Strategy*, 13 (March-April issue)

Herring, J. (1992b), The Role of Intelligence in Formulating Strategy, *The Journal of Business Strategy,* 13 (5, May issue).

Lawton, T., Rennie, J. and Eisenschitz, T. (1988), Business information from industrial espionage – a state-of-the-art review, *Business Information Review*, 5, (2), pp.

Lee, M., Gailey, J. A. (2007), "Attributing Responsibility for Organizational Wrongdiong" in: Pontell, H.N. and Geis, G. (2007), *International Handbook of White-Collar and Corporate Crime*, Springer Science and Business Media, New York.

Vaughan, D. (2007), "Beyond Macro- and Micro-Levels of Analysis, Organizations, and the Cultural Fix" in: Pontell, H.N. and Geis, G. (2007), *International Handbook of White-Collar and Corporate Crime*, Springer Science and Business Media, New York.

Reports

Bussman, K.D. (2007) (PricewaterhouseCoopers), *Economic Crime: People, Culture and Controls*, Martin-Luther-University Germany, Fourth Biennial Global Economic Crime Survey.

Gerhard Schmid (2001), The European Parliament Report A5-0264/2001, Brussels, Belgium, *Report on the existence of a global system for the interception of private and commercial communications (Echelon interception system)* (2001/2098 (INI))

Internet Sources

All web addresses cited in this dissertation were last accessed in July or August 2008.

Altucher, J. (2007), 'Bot armies' unravel web security net, *Financial Times* http://www.ft.com/cms/s/2/4d7402ee-3ee5-11dc-bfcf-0000779fd2ac.html

Arkady, O. (2003), Putin oversees rise of security apparatus, *Financial Times*, http://search.ft.com/search?queryText=putin+security+apparatus&x=12&y=5&aje=true&dse=&dsz=

Barker, A. (2007), Corporate security: from guard dogs and fences to business intelligence, *Financial Times*, http://search.ft.com/ftArticle?queryText=kroll+business+intelligence&y=2&aje=true&x=17&id=070627000895&ct=0

BBC (2000), http://news.bbc.co.uk/2/hi/technology/5313772.stm

BBC (2006), http://news.bbc.co.uk/2/hi/programmes/real_story/4791167.stm

BBC (2008), http://news.bbc.co.uk/2/hi/science/nature/1357513.stm

BCR (2008), http://www.control-risks.com

Cambridge Dictionary (2008), http://dictionary.cambridge.org

CSIS (2008), Canadian Security Intelligence Service, http://www.csis-scrs.gc.ca/en/priorities/espionage.asp

Donkin, R. (2007), FT report – corporate security: would-be employers grapple with dodgy CVs, *Financial Times,* http://search.ft.com/ftArticle?queryText=background+check+on+employees&y=0&aje=true&x=0&id=070627000835&ct=0

EPP (2008), http://epp.eurostat.ec.europa.eu/pls/portal/docs/PAGE/PGP_PRD_CAT_PREREL/PGE_CAT_PREREL_YEAR_2008/PGE_CAT_PREREL_YEAR_2008_MONTH_01/3-31012008-EN-AP.PDF [it has unfortunately been necessary to reproduce this very long URL in order to make the exact web page accessible]

GPW (2008), http://www.gpwltd.com

GSMBugs (2008), http://www.spyequipmentuk.co.uk/index.php?main_page=product_info&products_id=174&zenid=63473eb94e4396e4d3324812fc4012ef

GSMSpy (2008), http://www.gsmspy.com

Investor Words (2008), http://www.investorwords.com

Jonassen, A., Aale, P. K. (2007), Spying in Norway reaches 'all-time high', *Aftenposten* (Oslo, Norway), http://www.aftenposten.no/english/local/article2244756.ece

Jong-a, S. (2007), S. Koreans unsettled by fake credentials scandals, *Financial Times*, http://www.ft.com/cms/s/0/6f321390-6aa4-11dc-9410-0000779fd2ac.html

Hakluyt (2008), http://hakluyt.co.uk

Kroll (2008), http://www.kroll.com

LANL (2008), http://www.lanl.gov

McQueen, M. P. (2008), Targets of spying get smart, *The Wall Street Journal*, http://online.wsj.com/article/SB121314159777262545.html

Meredith, R. (1997), VW Agrees to pay G. M. $100 Million in Espionage Suit, *The New York Times* http://query.nytimes.com/gst/fullpage.html?res=9C02E0D61638F933A25752C0A961958260&sec=&spon=&pagewanted=print

MI6 (2008), http://www.mi6.gov.uk/output/Page7.html

OPSEC (2008), http://www.opsecsociety.org

Ostrovsky, A. (2003), Putin oversees big rise in influence of security apparatus, *Financial Times* http://search.ft.com/ftArticle?queryText=putin+security+apparatus&y=9&aje=true&x=13&id=031031007274&ct=0

Pesola, M. (2005), UK warning over large scale attack on computer networks, *Financial Times*, http://www.ft.com/cms/s/2/0ebfd236-ddc5-11d9-a42f-00000e2511c8.html

Risk (2008), http://www.riskadvisory.net

Spycatcher (2008), http://www.spycatcheronline.co.uk/spy-phones-c-52.html

SSB (2008), http://www.ssb.no/english/subjects/06/arbeid_en

Star Wars (2005), http://waxy.org/archive/2005/05/19/star_war.shtml

Wallis, W. (2005), Israel probes alleged spyware network , *Financial Times* http://search.ft.com/ftArticle?queryText=israel+industrial+espionage&y=9&aje=false&x=7&id=050530004639&ct=0&nclick_check=1

Ward, M. (2003), The hidden dangers of documents, *BBC* http://news.bbc.co.uk/2/hi/technology/3154479.stm

Wikipedia (2008a), http://wikipedia.org

Wikipedia (2008b), http://en.wikipedia.org/wiki/Larry_Wu-Tai_Chin