INDUSTRIAL ESPIONAGE AND CORPORATE SECURITY: THE ERICSSON CASE

INDUSTRIAL ESPIONAGE AND CORPORATE SECURITY: THE ERICSSON CASE

Lauri Holmström

REPORTS OF THE POLICE COLLEGE OF FINLAND 87/2010

The Police College of Finland
Tampere, 2010

Lauri Holmström
INDUSTRIAL ESPIONAGE AND CORPORATE SECURITY: THE ERICSSON CASE
Reports of the Police College of Finland 87/2010

ISBN 978-951-815-187-9
ISBN 978-951-815-188-6 (PDF)
ISSN 1797-5743

Tampereen yliopistopaino - Juvenes Print Oy, Tampere 2010

Table of Contents

Abstract

Keywords: industrial espionage, corporate security, high technology, Finland, Sweden, Ericsson

This dissertation has researched current industrial intelligence efforts towards private sector entities in Finland and Sweden through a historical and theoretical framework where the main findings have been geared around a study on the 2002 Ericsson espionage case. The official documents and reports of the national intelligence agencies in Finland and Sweden figure most prominently in the source base, while the single most important primary source has been the judgment of the Stockholm District Court in the Ericsson case. Supporting sources have been drawn from a pool of articles and literature on the subject. Industrial espionage has both risen and grown more complex in recent years and it is important for both the state and private sector actors to counter this threat by investing in functioning corporate security practices that are supported by the national intelligence agencies. The competition between rival states has been replaced to some degree by the complex picture of shifting loyalties and changing identities with corporations having taken over some of the areas of influence previously possessed only by nations. The importance of a knowledge-based economy and the rise of information technology have been beneficial to the economies of Finland and Sweden. However, the industries that now matter are prone to information security risks. Industrial espionage is also closely connected to the defense doctrine and national security issues in both countries. The relationship between public and private sector actors thus brings an important dimension to the problem of industrial espionage.

Tiivistelmä

Asiasanat: talousvakoilu, yritysturvallisuus, korkea teknologia, Suomi, Ruotsi, Ericsson

Tämä tutkimus on keskittynyt ajankohtaisten tiedustelu-uhkien tutkimiseen yksityisen sektorin kohteita vastaan Suomessa ja Ruotsissa historiallisen viitekehyksen kautta, jossa tärkeimmät tutkimustulokset on nidottu vuoden 2002 Ericssonin vakoilutapauksen ympärille. Keskeisinä lähteinä tutkimuksessa on käytetty Suomen ja Ruotsin kansallisten turvallisuuspalveluiden virallisia dokumentteja. Tärkein yksittäinen alkuperäislähde on ollut Tukholman käräjäoikeuden päätös Ericssonin tapauksessa. Lisäksi työssä on hyödynnetty aihepiiriä käsitteleviä artikkeleita ja kirjallisuutta. Talousvakoilu on ilmiönä sekä kasvanut että muuttunut monimutkaisemmaksi viime vuosien aikana. On tärkeää sekä valtiolle että yksityisen sektorin toimijoille vastata tähän uhkaan investoimalla toimiviin yritysturvallisuusmenetelmiin, jotka saavat tukea kansallisilta turvallisuus- ja tiedustelutoimijoilta. Kansallisvaltioiden välinen kilpailu on korvaantunut tiettyyn pisteeseen asti monimutkaisella vaihtuvien lojaliteettien ja muuttuvien identiteettien ilmiöllä, jossa yritykset ovat vallanneet joitain sellaisia alueita, jotka olivat aiemmin valtioiden yksinomaisuutta. Tietotalouden merkitys sekä informaatioteknologian nousu ovat olleet merkittäviä tekijöitä Suomessa ja Ruotsissa. Kuitenkin ne teollisuudenalat, jotka ovat nyt tärkeitä, ovat alttiita erilaisille tietoturvariskeille. Talousvakoilu liittyy myös läheisesti molempien maiden puolustusdoktriineihin sekä laajempiin kansallisen turvallisuuden kysymyksiin. Yksityisen ja julkisen sektorin toimijoiden välinen suhde tuo siten tärkeän ulottuvuuden kansallisen talousvakoilun ongelmaan.

Abbreviations

DCI	Director of Central Intelligence
EC	European Council
EU	European Union
KRP	The Finnish National Bureau of Investigation (Keskusrikospoliisi)
NATO	North Atlantic Treaty Organization
NBF	Network-based defense (Nätverksbaserat försvar)
PERSEREC	Defense Personnel Security Research Center
Sitra	The Finnish National Fund for Research and Development
Supo	The Finnish Security Police (Suojelupoliisi)
SVR	The Russian Foreign Intelligence Service (Sluzhba Vneshny Razvedky)
Säpo	The Swedish Security Police (Säkerhetspolisen)
Tekes	The Finnish National Technology Agency
VTT	The Technical Research Centre of Finland (Valtion teknillinen tutkimuskeskus)
WMD	Weapon of mass destruction

1 INTRODUCTION

Industrial espionage has experienced a resurgence since the end of the Cold War. Today, more than ever before corporations and nations are being targeted through illegal methods that strive to acquire new technologies, information and innovations in a wide variety of disciplines. High technology, military applications and biotechnology are at the frontlines of these attacks. Corporate security has become a vital component in preventing and fighting industrial espionage. While national intelligence agencies are combating espionage efforts aimed at the important industries of their respective countries, in an age of increasingly rapid globalization the private sector must also rise to the challenge through improved and intensified corporate security.

1.1 The research subject

This study investigates the rise of industrial espionage efforts towards private sector entities in Finland and Sweden during the last two decades against the backdrop of the globalizing economy. Both countries have invested heavily in research and development and are home to a number of important and innovative companies that produce some of the world's most advanced technologies. The phenomenon of industrial intelligence is analyzed through the framework of corporate security, which functions inside nation states. Thus, the emphasis here is twofold. Both private sector security and the role of national security organs with regards to industrial intelligence will be explored. This work represents the part of intelligence and security studies that seeks to understand contemporary processes through practical examples that are supported by theoretical thinking. While it can be argued that all social sciences are historical by nature, the effort has been made to bring the research as up-to-date as possible, while acknowledging the fact that the subject matter is a vibrant and constantly changing object, which makes any final judgments or conclusions from it temporary. What this study has achieved is the mapping of the fundamental problems and questions associated with industrial espionage in Finland and Sweden. Furthermore, these results have been applied to practical and current examples of corporate security that offer ideas and solutions to counter covert and illegal practices. The main research question is: what is the current picture of industrial espionage in Finland and Sweden and how can corporate security counter it? Further questions that are explored are: what are the main trends of industrial espionage in the post-Cold War era and how is industrial espionage affected by globalization and new technological advances?

The main thesis of this study is that industrial espionage has both risen and grown more complex in recent years and it is important for both the state and private sector actors to counter this threat by investing in functioning corporate security practices that are supported by the national intelligence agencies. The cooperation between the state, the universities and the companies has produced significant technological advances of intellectual property in Finland and Sweden. These innovations have then been successfully marketed on a global scale. The emergence of high technology as a key driver of the restructured, knowledge-based economy has been significant. It has been possible because of the existing frameworks of higher education as well as functioning national innovation systems. High technology companies are nationally important to both Finland and Sweden. Both countries count on their technology companies to continue as leading competitors in the global economy. Finland and Sweden have a lot at stake when it comes to high technology, innovations and intellectual property. Although the most prominent actors in the field are private sector companies, the state has a lot to lose if important firms are hurt by industrial espionage. At the same time, the companies themselves stand to lose to their competitors in the fields of research, product development and markets. Corporate security is the most important tool for protecting the intellectual property of companies. The national security agencies also carry a large responsibility for the security of universities, research centers and companies located in their country.

Individual cutting edge technologies have become vital in a number of areas important to society, not least as a stimulating force for continued technological development and economic growth. This technology is desired by both nation states and private companies looking to make fast advances, cut costs or gain an edge in competition. While many rising powers such as China have been accused of illegal commercial practices in public, industrial intelligence is also very much a phenomenon inside trading blocs and between political and military allies. Some products and know-how especially in the field of biotechnology are also a target for international terrorist networks, which seek to turn this knowledge capital into weapons.

1.2 Earlier research and resources

The focus of this study is on both Finland and Sweden because the economies of the two countries are similar and highly integrated. The availability of good sources and practitioner advice has also affected the decision to expand point of view of the research into two countries. The comparability of economies, political systems and perceived threats has made it possible to

deal with Finland and Sweden as one entity in this context. The historical and theoretical background of this study has been built on multiple articles that have appeared in a number of professional and scientific journals. The most important resources from this category have been the writings of Samuel Porteous[1], who has written extensively and insightfully on the different questions and concepts of industrial intelligence. The research by Porteous used here is from the beginning of the 1990s and is then somewhat dated. However, because his perspective is mostly a theoretical one, it has been deemed sufficient to cover the needs of this study. Katherine Herbig and Martin Wiskoff have researched the question of how the loyalty of people to their respective nation states has changed during the globalization of economy.[2] The traditional model of espionage is also connected strongly to the idea of a nation state. Applying this view to the subject of industrial espionage has been constructive for this study. Herbig and Wiskoff have produced their research for the Defense Personnel Security Research Center (PERSEREC) of the United States. As such, it is an official study and its reliability is high. However, even if its findings have not been based on data gathered from Sweden or Finland, the conclusions and ideas it presents regarding espionage and nation states can be easily implemented here. Hugo Cornwall's aptly titled *The Industrial Intelligence Handbook*[3] is very much a product of journalistic writing geared to churn out a compact and slightly entertaining product. Its greatest merit lies in the good definition of the different types of agents and discussion of general information security issues. On the Finnish side, Marinka Lanne has written extensively on corporate security in Finland. Her doctoral thesis[4] as well as the study on the theoretical model for the Finnish security business[5] have been of great value. They are both published by the Technical Research Centre of Finland (VTT, Valtion teknillinen tutkimuskeskus) and have thus the same limitations and assets as Herbig and Wiskoff's text. However, because Lanne has especially studied corporate security in Finland and is one of the leading pioneers of the field, her research can be considered to be high

1 Porteous Samuel (1993) *Economic Espionage*. Canadian Security Intelligence Service, Commentary Number 32; Porteous Samuel (1994) *Economic Espionage (II)*. Canadian Security Intelligence Service, Commentary Number 46.

2 Herbig, Katherine L. & Wiskoff, Martin F. (2002) *Espionage Against the United States by American Citizens 1947-2001*. PERSEREC Technical Report 02-5, July 2002.

3 Cornwall Hugo (1991) *The Industrial Espionage Handbook.* London: Century.

4 Lanne Marinka (2007) *Yhteistyö yritysturvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa.* VTT publications 632. Helsinki: Edita Prima Oy.

5 Lanne Marinka and Kupi Eija (2007) *Miten hahmottaa security alaa? Teoreettinen malli Suomen security-liiketoiminta-alueista.* VTT Tiedotteita - Research Notes 2388. VTT Technical Research Centre of Finland [www] Available from http://www.vtt.fi/publications/index.jsp [Accessed on 4 April 2008]

class and relevant to this study.

The second main category of resources are primary sources. The official documents and reports of the national intelligence agencies in Finland and Sweden, the Finnish Security Police (Suojelupoliisi, Supo)[6] and the Swedish Security Service (Säkerhetspolisen, Säpo)[7] have appeared in electronic formats on the webpages of the respective services. However, they have also been published as printed sources. The decision has been made to refer to them as documents authored by the agency in question and from then on by simply using the title of the source. Other governmental material from both countries has also been utilized in passages dealing with national information security strategy, the larger national context of industrial espionage and corporate security and legislation. Of these, especially the strategy of the representatives for Finnish trade and industry and authorities to prevent corporate crime[8] and the Finnish National Information Security Strategy Proposal[9] have been very useful. As official documents they are the best resources dealing with the role of the state in industrial intelligence. While they sometimes are restrictive in their details or offer only general views on the subject, they nevertheless carry a high degree of reliability and the most current information available in print. The official documents of the Finnish National Bureau of Investigation (Keskusrikospoliisi, KRP) regarding corporate crime have also been utilized. They offer a more professional view from the field that balances the academic research used in this study.

The most important primary source has been the judgment of the Stockholm District Court in the Ericsson espionage case number B 7025-02.[10] It is the only publicly available legal document on the case. The judgment details the espionage operation, the backgrounds of the perpetrators, the investigation that led to the capture of the offenders and the stolen documents as well as information on the significance of the case to Ericsson and Swedish national security. As such, a lot of weight has been placed on it. Because it is a legal document – albeit a sanitized one – the information it supplies us with is valid, if at times a little vague. This vagueness has not been a major problem

---

6 The Finnish Security Police, Suojelupoliisi [www] Available from http:www.poliisi.fi/supo [Accessed 4 April 2008]

7 The Swedish Security Service, Säkerhetspolisen [www] Available from http://www.sapo.se [Accessed 4 April 2008]

8 *Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi.* Sisäinen turvallisuus, Sisäasianministeriön julkaisuja 15/2006.

9 *National Information Security Strategy Proposal*. November 25, 2002, Proposal of the Advisory Committee for Information Security [www] Available from http://www.ficora.fi/englanti/document/infos.pdf [Accessed 4 April 2008]

10 Stockholms Tingsrätt, Rotel 1301, Avd 13, Dom, Mål nr B 7025-02, meddelad i Stockholm, 2003-06-17.

for this study, because the information provided by the court judgment has been informative and analytical enough for a compact case study. Limitations in the source base have been overcome by gearing the focus of this study towards a research goal that has been both reasonable and attainable, without sacrificing the ambition to produce new views and information on the subject.

1.3 Methodological solutions

What can be achieved in a postgraduate level dissertation dealing with an essentially clandestine subject based on open sources? Economic and industrial intelligence have been studied extensively in the academic community. While most research has focused on the role of national intelligence agencies in fighting threats to the industry or economy of a given country, the role of private sector and corporate security has often been secondary. Corporate security has usually been researched by individual companies or national security agencies for their own purposes. These studies are seldom made public. One of the key aims of this study has been to take what has usually been the domain and interest of private sector actors and explore it critically through the academic discipline of intelligence and security studies. This point of view has been shaped by two main considerations. Firstly, to only give an account or a general outline of the world of industrial espionage without any theoretical or historical framework would serve no practical or educational point. Secondly, the realm of espionage and intelligence in the world of international business has restrictions on what an academic researcher can acquire through open sources. The scope and depth of this study is by no means enough to cover the entire field of industrial espionage and corporate security in today's world. Instead, the focus of research has been narrowed to form an overview of the current threat presented by industrial espionage to two closely connected countries and the challenges corporate security faces in countering it. The Ericsson espionage case has been chosen here as a case study because it combines a lot of the elements inherent in current industrial intelligence and the efforts of corporate security as well as the national agencies responsible for preventing such activities. It also reflects the trends and practices of current industrial espionage. Lastly, the Ericsson case fits the profile of a small nation with advanced technology that is integral both to its economy and its military and civilian defense.

Another reason for focusing on a Swedish example of industrial espionage has been the absence of a similar large scale case in Finland. However, this does not mean that there have not been recent incidents of high-profi-

le industrial intelligence cases in Finland. In June 2008 the largest Finnish newspaper *Helsingin Sanomat* reported that both the State of Finland and the Finnish arms industry had been targeted by foreign intelligence operations that had utilized information warfare techniques to reach their goals. The espionage operations were very well planned and specifically aimed at several defense and security related targets. The attacks used e-mails to install viruses on the computers of certain employees, which could then be exploited to acquire secret information from the computer as well as access any databases that the employee in question had used. Traces of the attacks were tracked to Chinese servers, but this fact itself helped little to solve the origin of the operations. The information regarding the case was reported by Supo to the media, but no other details were released to the public.[11] Because of the methodological choices and possibilities regarding resources the case study is from Sweden and much of the corporate security material from Finland. However, for reasons explained above, it has been deemed that this approach and its results have arrived at a product that is both relevant and applicable to the instances of both nations.

This dissertation is structured in the following way: chapter two deals with the concepts and theoretical aspects of industrial intelligence, chapter three discusses corporate security and national intelligence agencies and their relations to industrial espionage and chapter four presents a study on the Ericsson espionage case. Finally, the conclusion will summarize the findings and the main arguments of the study.

[11] Huusko Jukka and Moisio Teppo (2008) Suomen valtio ja aseteollisuus joutuneet verkkovakoilun uhreiksi, *Helsingin Sanomat*, 11 June 2008, p. B 1.

2 INTELLIGENCE, TECHNOLOGY AND SECURITY

Since the end of the Cold War industrial intelligence has become a core area of interest to governments as well as non-state actors engaged in the global competition over new innovations and technologies. Especially in Europe, where production can no longer compete with rising powers such as China, the main thrust in the economic sector has been towards research and development. It can thus be argued that the rise of information technology in both civilian and military use has accelerated the resources allocated to discovering new trends and inventions by clandestine means while protecting intellectual capital and sensitive information has become instrumental for the corporate security of private sector actors and a priority for national intelligence agencies.

2.1 Industrial intelligence in the post-Cold War era

During the last two decades the global economy has developed at an ever-increasing speed. The economy affects political and military relations and many other aspects of life. Globalization has created new conditions for international economy that demand a modern understanding of the definition of loyalty to nation states. This trend together with the dual use of technologies, meaning both civilian and military use, guarantees that industrial intelligence will continue to gain importance while the differences in defense and industrial applications become more unclear.[12] The phenomenon of globalization coupled with the explosion of information technology has had a huge impact on the way societies and nations function. The post-Cold War period has also brought new secret information demands to the fore. Technological advances with enormous economic and military potential generate intensive competition on patents, markets and technological superiority. Interests related to security, technology and the economy are often connected. When assessing the intelligence threat on the economic and technological areas, traditional considerations such as military-strategic importance and geopolitical situation are less relevant. Other aspects, such as a country's international status in

[12] Herbig and Wiskoff (2002) pp. 70, xiv; Samli A. Coskun and Jacobs Laurence (2003) Counteracting Global Industrial Espionage: A Damage Control Strategy. *Business and Society Review,* 108:1, 95-113, pp. 100-101.

research, industry and export become more important.[13] David Boren views economic and social strengths as the future primary factors of world influence. He sees the national security of nations being threatened by the failure to adapt our thinking with the ongoing changes in the world around us.[14]

During the 20th century, the intelligence community led the development of information technology. Modern telephone networks and computers have both originated in this way. Today, the intelligence community is no longer at the cutting edge of development and research in the information world. Bruce Berkowitz has identified the largest problem to be the failure to keep up with changes in how modern societies use information and how information technology shapes the world.[15] Economic information has been a target of espionage especially for nations with less developed industrial capabilities. The different kinds of information that are important to nations is constantly expanding to economies and other areas where it is difficult to guard information. Economy is the backbone of functioning societies as well as international relations. Political entities need networked, active and dependable economic systems. Samuel Porteous sees economic espionage having the same importance for a country's economic interests as more familiar types of espionage have for traditional political and security interests.[16]

Katherine Herbig and Martin Wiskoff view the traditional concept of espionage as a contest between opposing states, which is rooted in the concept of the nation state that is built on the idea of one sovereign power controlling a certain territory. This model assumes that any information about the nation state in question is the property of that state. The citizens of a nation who spy against the interests of their own state endanger its sovereignty and exhibit disloyalty against their government. Where the nation state is responsible for giving its citizens protection against violence and a stable and structured society, the people being governed by the state are implicitly expected to be loyal to their governments. In today's world identities are shaped increasingly by religion, ethnicity and other personal attributes that have rendered the

[13] Clough, Chris (2004) Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation. *International Journal of Intelligence and CounterIntelligence*, 17:4, pp. 607-608; May, Ernest R. (1992) Intelligence: Backing into the future. *Foreign Affairs*, Summer 1992, Volume 71, Issue 3, p. 64; Säkerhetspolisen (2003) *Verksamhetsåret 2002*, p. 14.

[14] Boren David L. (1992) *The intelligence community: how crucial?* Foreign Affairs, Summer 1992, Volume 71, Issue 3, 52-62, p. 52.

[15] Berkowitz, Bruce D. (1996) *Information age intelligence*, Foreign Policy, Summer 1996, Issue 103.

[16] Herbig and Wiskoff (2002) p. 71; Porteous Samuel (1994); According to the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage American companies lose 300 billion dollars a year to economic espionage. Isaacs Richard (2003) Dirty Little Secrets, *Security*, December 2003, 40, 11, 39, p. 39; Luong Minh (2003) Espionage: A real threat. *Optimize*, October 2003, 61-72, p. 61.

nation state model obsolete to some extent. In addition, this trend has pushed corporations into fields of influence formerly occupied by states alone. In a world of increasing globalization these notions about espionage among the system of nation states can be said to no longer hold the same weight as before. It has therefore been argued that power is less vested in territorial hegemony backed up by military strength and more in how successfully the citizens of a given state participate in the global economy. This brings into question the loyalty of the individuals who take part in the global economy through multinational companies, banks and independent agencies.[17]

Today's intelligence activity is formed by the powerfully growing multitude of information in the world and at the same time by the increased access to information via the internet and other computer networks. The possibilities of acquiring both open source and secret information through signals surveillance, internet monitoring and data tresspasses have grown. Parallel to these methods, also traditional covert practices such as coded messages, agent recruitment and pressure against individuals are used to a large extent. Technological development has activated new non-state intelligence actors. It can be hard to assess to what extent espionage is supported by any given state, and there have been cases where suspicions have arisen that information collection has not always been initiated by the country that carries out the activity, but that it is in fact acting on behalf of a third party. Regardless of the actors involved the consequences for those hurt by information loss can be great.[18] Herbig and Wiskoff further state that the global economy has changed the way actors identify friends and enemies who would spy on them. The bipolar system of the Cold War kept espionage among allied nations in check. In today's world there is an abundance of possible customers for information. One scenario of the future anticipates that those who succeed in the global economic competition will share information and work together to grow both their individual and economic powers. While these kinds of groups are still in the process of forming, it is already clear that they will gravitate towards the most advantageous positions available thus potentially ignoring historical alliances or values.[19]

James Adams has given an example of how Soviet industrial intelligence affected the larger Cold War conflict. By stealing plans for the Harrier jet, the BI-B bomber, the American Airborne Warning and Control aircraft and the MK-48 torpedo as well as several air and ground radars the Soviets saved millions of dollars in research and development. As Soviet military techno-

[17] Herbig and Wiskoff (2002) p. 70.

[18] *Verksamhetsåret 2002*, p. 14; Säkerhetspolisen (2006) *Spionärenden 2005 - en sammanställning från öppna källor*, p. 14.

[19] Herbig and Wiskoff (2002) p. 71.

logy advanced, The North Atlantic Treaty Organization (NATO) was forced to undertake new research projects in order to keep its qualitative advantage over the East. This escalated the arms race and thus contributed to the overall elevation of the Cold War.[20] While claims such as these are difficult to evaluate, they indicate a perception that some intelligence services and their respective governments seek actively to benefit from industrial espionage. Recently China has been the country most often associated with industrial espionage. The main reason for this is the rapid industrial development in Asia. As the Asian market grows, more companies are placing their production there and at the same time Asian companies and researchers are working abroad. The fixed costs connected with research and development can be reduced through successful economic espionage. For example, if the production technology of a foreign company is acquired through clandestine means, domestic firms will benefit from lower costs and also achieve a strategic benefit in the global markets.[21]

2.2 Concepts and methods of industrial intelligence

After the Cold War the need for military intelligence staff diminished and industrial intelligence started to employ a larger part of the professional intelligence officers. When the economic depression of the early 1990s was over, trade and industry regained their strength as industrial espionage grew into an even more central and critical factor.[22] The constantly increasing value of trade secrets and the quick expansion of technology have created a large increase in the motives, possibilities and activities of industrial espionage. These efforts are not only aimed at finished products and marketable ideas, but also towards the processes themselves that generate them. Samuel Porteous has drawn attention to the lack of a coherent terminology in dealing with issues related to economic and industrial intelligence. He has defined economic intelligence as "the policy or commercially relevant economic information, including technological data, financial, proprietary commercial and government information, the acquisition of which by foreign interests could, either directly or indirectly, assist the relative productivity or competitive position

[20] Adams James (1995) *The New Spies: Exploring the Frontiers of Espionage*. London: Pimlico, p. 128.

[21] Porteous Samuel (1993); Säkerhetspolisen (2004) *Företagsspionage Rapport 2/2004*, p. 4; Whitey Merril E. and Gaisford James D. (1996) Economic Espionage as Strategic Trade Policy. *The Canadian Journal of Economics / Revue canadienne d'Economique*, Volume 29, Special Issue: Part 2, April 1996, 627-632, p. 627.

[22] Kajava Jorma (2003) *Henkilöturvallisuus osana organisaation tietoturvaa.* Oulun yliopisto, tietojenkäsittelytieteen laitos. Sovellukset ja hallinto, Sarja D 12, Oulu: Oulu University Press, p. 6.

of the economy of the collecting organization's country". Most economic intelligence gathered by governments and companies is collected legally from open sources using overt methods. The use and collection of information in this manner, be it through visiting students, scientists or businesses, is a favorable feature of an open society and crucial to technological and economic development. Economic intelligence can however slide to the realm of economic espionage, when obtrusive and covert methods are used.[23]

According to Porteous, economic espionage is "the use of, or facilitation of, illegal, clandestine, coercive or deceptive means by a foreign government or its surrogates to acquire economic intelligence. The acquisition of an actual piece of technology, such as physical examples of technological information or documents, is assumed to be included in this definition". He further defines industrial espionage as "the use of, or facilitation of, illegal, clandestine, coercive or deceptive means by a private sector entity or its surrogates to acquire economic intelligence". When competitive intelligence is taken too far, it becomes corporate espionage. Where business intelligence deals with legally available information in an analytical manner, industrial espionage is essentially about stealing corporate secrets.[24] In this study, the terms industrial espionage and industrial intelligence are used interchangeably, and are understood to encompass the same essential characteristics of illegal intelligence activity.

Many intelligence services support their nations' trade and industry, which can raise the vulnerability for different types of intelligence gathering. Technical development and advanced equipment lead to new ways of acquiring sensitive information. Despite a growing information leakage through technical equipment and surveillance, intelligence still very much happens through human sources. Espionage and gathering are made possible through foreign persons who are officially stationed in the country, are employees with a company or through an official who sells information to a foreign power. A great deal of industrial intelligence gathering has been undertaken by former employees. It is not unusual that espionage is carried out by storing or sharing secret information on portable computers, memory sticks and mobile phones. This places great demands on modern information security, which

[23] Samli and Jacobs (2002) p. 96; Nodoushani Omid and Nodoushani Patricia A. (2002) Industrial Espionage: The Dark Side of the "Digital Age". *Competitiveness Review*, Volume 12, Number 2, 96-101, p. 96; Porteous (1994); McCourt Mark (2008) Keeping Up with New Threats. *Security*, March 2008, 45, 3, 16-18, p. 16.

[24] Porteous (1994). For discussion of concepts see also Wright Phillip C. and Roy Géraldine (1999) Industrial espionage and competitive intelligence: one you do; one you do not. *Journal of Workplace Learning*, Volume 11, Number 2, 53–59, pp. 53-55; Rothke Ben (2001) Corporate Espionage and What Can Be Done to Prevent It. *Information Systems Security*, November/December, p. 2, Samli and Jacobs (2003) p. 97.

has become one of the main elements in successful corporate security.[25]

The responsibility of the individual has become more important during current times when the security of companies, officials and organizations depends on the security thinking of the employed. It has been estimated that approximately half of all information technology related crimes that happen could have been prevented if the existing security systems had been used properly. The largest challenge is to adapt the previous security consciousness to the technical, mobile and international context of today. A number of intelligence services spend resources on improving their technical information gathering capacity, resulting in more discrete and efficient intelligence activities. The transmission of more and more information via mobile means of communication, together with the increased integration of data and telephone communications, makes communication systems more vulnerable and increases the risk of computer intrusion, tapping and signals intelligence activities. Improved protection measures for sensitive or particularly vulnerable communication systems are necessary to counter such risks. The growth of industrial espionage has been helped by the advances in the technical equipment applicable to covert information gathering.[26]

As for the perpetrators of industrial intelligence, Hugo Cornwall has divided the human sources into two categories. A covertly corrupted agent supplies information for compensation and sees nothing wrong in his actions. An example of this might be someone who gets close to secret information in their job and discusses it with an outsider, while considering his actions to be for example a form of consultancy. A volunteer agent is someone who sells information for a price and knows he is engaged in illegal activity. His actions are usually planned and systematic. The volunteer agent is more likely to get caught than the covertly corrupted agent. There is also the danger that a potential customer can betray the agent to the authorities.[27] For example, most of the crimes involving trade secrets in Silicon Valley have been committed by employees and other persons working for the company. In short, it has been shown that the staff of a company is behind most information crimes and cases of industrial espionage.[28] The highest risk groups for corporate trade secrets include former employees, temporary staff, current employees,

---

25 *Spionärenden 2005*, p. 12.

26 *Verksamhetsåret 2002*, p. 26; Säkerhetspolisen (2004) *Annual Report 2003*, p. 27; Säkerhetspolisen (2004) *Företagsspionage Rapport 1/2004*, p. 4.

27 Cornwall (1991) pp. 35-37; Samli and Jacobs (2003) p. 101.

28 DeWitt Maggie (2006) Corporate Criminals. *Business Forms, Labels & Systems*, June 20, 44, 6, 46-49, p. 48; *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva syksy 2007.* Keskusrikospoliisi / rikostietopalvelu 1.10.2007, p. 16; *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva 17.10.2006*, p. 15; Hazelhurst Jeremy and Higgins Joanna (2004) Clear and present danger. *Director*, October 2004, 58, 3, 78-83, p. 83.

vendors or suppliers and consultants.[29] In the Ericsson espionage case, the offenders were all volunteer agents inside the company.

Lisa Kramer and Richards Heuer have summarized the often complex motivations of individuals as an interaction between situational factors and personal characteristics. Most people with access to classified information do not commit acts of spying. However, it has been suggested that certain people can be influenced by circumstances in their personal or professional lives to undertake illegal actions. Moreover, people can be pushed to spy on their employers by emotional ties to foreign entities, personal discontent towards the employer or financial troubles. When for example a person experiences that he or she is not treated well by the employer it can be easier to rationalize the choice of engaging in espionage.[30] This self-rationalization was strongly present in the Ericsson case.

A common method among intelligence services is to frequent fairs and conferences. To be able to talk with one or several researchers or representatives for firms in that situation under a visibly legitimate context, can give a lot of valuable information. Even stolen briefcases, computers and other equipment are utilized. Another method of espionage among companies is the "lending" of an employee by one firm to another. The person in question then proceeds to learn the competitor's business secrets and later returns to his original employer. Espionage can also be carried out by disloyal employers, who feel that they have been mistreated or feel unhappy in some way. Tommy Svensson, a security expert at the Confederation of Swedish Enterprise says that redundancies and other turbulence at the workplace raise the risk of employees becoming disloyal. In essence, honorable people can be tempted into illegal activities. At a time when people are being laid off, some employers have gone to a competitor or started up their own business, taking with them critical information. This is an even bigger threat against business. The advent of a large, movable work force has contributed to the reduction in loyalty to a particular company. With the rise of industrial espionage the security measures of companies have toughened. Together this with the intensified monitoring of employees brings distrust in the workplace. The so-called mosaic method, where information fragments from different open and secret sources are pieced together can very well lead to the exposure of an entity that gives away information that would have otherwise remained secret. Some intelligence services have systematized this approach through a network of visiting students and researchers from their country. Intelligence

[29] Denning Dorothy E. (1999) *Information Warfare and Security*, Addison-Wesley, ACM Press Books, New York, p. 53.

[30] Kramer, Lisa A. and Heuer Jr., Richards J. (2007) America's Increased Vulnerability to Insider Espionage. *International Journal of Intelligence and CounterIntelligence*, pp. 53-55.

officers often seek to get close to personnel in defense, company directors, product developers, researchers and other bearers of attractive information. Other nations' research institutes, companies, delegation visits and dissident circles are examples of traditional areas where an intelligence actor under cover or false identity can work through illegal or legal channels.[31]

Industrial espionage is a security intelligence subject targeted by counterespionage. The largest element of risk in industrial intelligence has always been the human factor. Recent cases clearly show that companies risk the most damaging information losses via their staff. Moreover, the fact that the storage and systematization of information nowadays takes place using technical aids has also facilitated individuals' access to large amounts of information. This means that intelligence organizations aspire to recruit human sources. The recruitment of an agent is no coincidence, for it is preceded by careful studies where factors such as motivation, access and reliability are thoroughly assessed. Recruitment is always approved by the head office of the intelligence service.[32]

Kramer and Heuer think that rapid advances in information technology have made it more difficult to restrict access to secret information. While information technology has increased the productivity of employees it has also given them new tools for espionage. The storing of information in large databases that can be easily searched has made it easier to locate specific information. Another significant feature is the possibility of storing huge amounts of data on small portable devices. The globalization of trade and research has facilitated the opportunities for industrial espionage by increasing cooperation between people from all over the world. This provides opportunities for recruitment as well as sharing and selling classified information. Furthermore, counterintelligence is now faced with the difficult challenge of separating normal working relationships from those that could potentially turn into a security risk.[33] For example, scientific research is built on collaboration that in

[31] Säkerhetspolisen (2004) *Att skydda svensk bioteknik. En broschyr om att skydda forskning, kunskap och produkter mot spionage och framställning av biologiska vapen*, p. 8; Kivinen Osmo and Varelius Jukka (2003) The Emerging Field of Biotechnology: The Case of Finland. *Science, Technology, & Human Values*, Volume 28, Number 1, 141-161, p. 149; Säkerhetspolisen (2005) *En vägledning till Säkerhetsanalys*, p. 6; Repo Walter (2004) Spionen från Rotebro, *Shortcut Magasin*, #2 April 2004, 36-45, p. 39; Isaacs (2003), p. 39; Säkerhetspolisen (2005) *Företagsspionage Juni 2005*. Rapportserie 2005:3, p. 3; Jones, Andrew (2008) Industrial espionage in a hi-tech world. *Computer fraud & security*, January 2008, 7-13, p. 12; Chan Marjorie (2003) Corporate Espionage and Workplace Trust/Distrust. *Journal of Business Ethics*, 42, 45-58, p. 46; *Verksamhetsåret 2002*, pp. 27-29.

[32] Herman Michael (1996) *Intelligence power in peace and war*. The Royal Institute of International Affairs. Fifth Edition. Cambridge: Cambridge University Press, pp. 53-56; Säkerhetspolisen (2004) *Verksamhetsåret 2003*, p. 27.

[33] Kramer and Heuer (2007) pp. 51-52.

today's world is increasingly international in its nature. It can be very difficult to decide which information of a given project should be protected.

If the economic power of a nation is understood to be as integral to national security as military power, how should the covert collection and use of industrial intelligence be handled? Further questions rise if the government of a given nation decides to give economic intelligence to its national companies. How do multinational corporations fit into this configuration? Ultimately, we are facing a question of conflicting national loyalties. In the United States, former Director of Central Intelligence (DCI) Stansfield Turner has suggested that making information public could diminish the edge a foreign company might have over a domestic one. This leads to the idea that the worlds of intelligence and business must strengthen their ties with the rise of economic importance. Turner has arrived at the conclusion that global economic competition requires nations to spy on each other's economic secrets. This should be done in his view by technical collection rather than traditional human intelligence means.[34]

2.3 Innovation and high technology

Osmo Kivinen and Jukka Varelius have pointed out that the term innovation has been used mainly in the past to signify original scientific discoveries but in the current technology policy discourse it has expanded to include inventions that have possible marketable applications. An innovation system is organized action that strives to create, develop and exploit innovations. In the context of the nation state the innovation system is called a national innovation system. Technology and knowledge have become key factors in the economy and are considered as important as economic growth, capital and work. Within the framework of the national innovation system and technology policy, the private and public sectors and universities are expected to work together transcending institutional boundaries. Knowledge is now considered intellectual property as well as a potential product that can be exploited in the market. This reconceptualization can be seen as the industrialization of the production of scientific knowledge. The universities are no longer the sole places producing new knowledge. The private sector will be more instrumental in creating technological advances than public sector actors while research and development will shift from the academic domain to companies. Research results are achieved in the process of knowledge production itself and in the movement of actors from one context of knowledge use to another.

[34] Turner Stansfield (1991) Intelligence for a New World Order. *Foreign Affairs*, Fall 1991, Volume 70, Issue 4, pp. 152-154.

This interdisciplinary research creates its own type of theoretical knowledge, practices and methods of inquiry. The quality of research is also increasingly measured in competition on the market and in terms of cost-effectiveness.[35]

Innovative companies are the main drivers of economic growth in a knowledge-based economy in Finland and Sweden. Technology is the most important industry in Finland. It constitutes 60 % of Finnish exports and 75 % of research and development investments are directed towards the technology industry.[36] With the rapidly changing processes of technology diffusion and innovation, the national innovation and production systems are becoming more interdependent. The state is often the lead actor in promoting innovation through funding research and development as well as investing in technological applications. For example, innovation has been integral in the restructuring of the Finnish economy. During the past 20 years, research and development intensity of Finland has grown to the second-highest levels within the European Union (EU) and the Finnish share of high-technology products to total exports among the highest in the industrialized world.[37] The geo-economic competition between nation states has in Robin Ramcharan's view become more important with deepening trade relations. Today, the struggle for trade secrets is a part of the national security of nations. However, this development has a contradictory effect where each nation strives to hold on to its comparative advantage or protect specific industries. The role of intellectual property becomes not only important as a resource but also as a part of the national competitive advantage. This is especially vital for nations which invest in high technology development.[38]

One example of the Finnish national innovation system has been the implementation of an alliance between companies, universities and the government called the triple helix model, which has helped to establish technology centers in cooperation with universities. The idea behind these centers is that the development of new technologies and the differentiation of customer-specific markets are understood to be the main reasons that drive com-

[35] Räikkönen Timo and Rouhiainen Veikko (2003) *Riskienhallinnan muutosvoimat. Kirjallisuuskatsaus.* VTT Tiedotteita - Research Notes 2208, VTT Technical Research Centre of Finland, Espoo: Otamedia Oy, pp. 31-32; Kivinen and Varelius (2003) p. 143. McCourt (2008) p. 16.

[36] Teknologiateollisuus ry [www] Available from http://www.techind.fi/ [Accessed 4 April 2008]

[37] Leinbach Thomas R. and Brunn Stanley D. (2002) National Innovation Systems, Firm Strategy, and Enabling Mobile Communications: The Case of Nokia. *Tijdschrift voor Economische en Sociale Geografie*, Volume 93, Number 5, 489-508, pp. 491-493; Daveri Francesco and Silva Olmo (2004) Not only Nokia: what Finland tells us about new economy growth. *Economic Policy*, April 2004, 117-163, p. 129, Kivinen and Varelius (2003) p. 144.

[38] Ramcharan Robin (2005) Intellectual Property and Security: A Preliminary Exploration. *Contemporary Security Policy*, 26, 1, 126-159, pp. 128, 141.

panies to specialize further and create new kinds of knowledge and technologies. For example in the 1990s, biotechnology centers were founded in six different locations around the country. The centers were established mainly through public funding by the Ministry of Education, The Finnish National Fund for Research and Development (Sitra) and the National Technology Agency (Tekes) that operates under the Ministry of Trade and Industry.[39]

In Finland, a significant increase in economic growth since 1995 has been driven by the productivity enhancing aspects of information technology. The sectors that did experience marked productivity gains were involved in both the production and the use of information technology goods and services led by Nokia,[40] the most important Finnish company and the leading global innovator in telecommunication technologies. International comparisons of business and technology environments have repeatedly ranked Finland at the top. Already in 1998, Finland featured the largest per-capita surplus in the foreign trade of communication equipment in the world, followed by Sweden and Ireland. Nokia has been called the archetype of a metanational firm. The essence of this notion is the ability to sense new pockets of knowledge and to mobilize them globally. Exploiting the knowledge-based economy by finding new ideas in diffuse locations and transforming them into global products is the key. Firms in the Nokia cluster may benefit from technological spillovers from Nokia because the company may share the results of its research and development spending with them or because some skilled employees, formerly trained at Nokia, may move to a firm in the Nokia cluster, bringing the knowledge accumulated at Nokia with them.[41] This raises problems related to security intelligence, which have been described earlier.

The international competitiveness of both Finland and Sweden is linked to the rise of high technology companies and the emergence of a knowledge-based economy. A modern technology policy that has been a priority in both countries is responsible for advancing economic growth through technological development. Industrial espionage corrodes the national investment and innovation frameworks supported by the state and causes financial and intellectual losses to companies and research centers. Industrial espionage can also act as a deterrent to innovation and may in the long run even cause losses to consumers around the world.[42]

---

[39] Kivinen and Varelius (2003) p. 142. For more on Finnish innovation see HighTech Finland [www] Available from http://www.hightechfinland.fi/ [Accessed 4 April 2008]

[40] In 2007, Nokia invested approximately 32% of its total workforce in research and development. Nokia [www] Available from http://www.nokia.com/ [Accessed on 4 April 2008]

[41] Daveri and Silva (2004) pp. 119-125, 146; Leinbach and Brunn (2002) p. 495.

[42] Whitey and Gaisford (1996) p. 632.

2.4 Industrial intelligence targets in Finland and Sweden

Changes in the post-Cold War global economy have shifted intelligence priorities in Finland and Sweden towards the high technology industry and research institutes.[43] The level of foreign intelligence in Finland has stayed at the same level during the last few years in both its quantity and quality. During 2006, the number of foreign intelligence officers grew a little but did not affect the number of aggressive recruitment cases. The greatest intelligence threat in Finland is directed against the key areas of high technology and the political machinery. The international energy questions, which carry a growing political dimension, have also been of interest to foreign intelligence. In this area, both civilian and military intelligence have converging aims. Scientific and technological intelligence has been dominated by a very broad open source gathering, where targets range from research centers to private companies. Foreign intelligence has also been interested in small firms, which are in possession of or have access to interesting technologies. General facts about the intelligence target in question are usually obtained at public fairs and seminars. Contacts and recruitment attempts of company personnel have been relatively rare, because both the desired technology and the key persons connected to it are selected extremely carefully. Sectors that have a dual use importance are a clear priority. Especially in telecommunications and information technology Finland has certain special areas that are of interest to foreign intelligence. The foreign intelligence services operating in Finland showed great interest in confidential conversations, situational estimates nearing completion and plans that were still worked on. The access to potential people that could be approached for secret information and their possibilities to influence the course of action is also charted carefully. The constant level of foreign intelligence in Finland shows that gathering secret and confidential information through human sources in a modern information society has not lost its meaning. Attacks against information systems pose a new and growing international threat. Recently the Finnish defense industry has been a target for these kinds of concentrated attacks. Scientific and technical intelligence efforts are especially focused on biotechnology, medical science and pharmacy, new materials, nanotechnology, telecommunications and positioning technology. In addition to basic knowledge, foreign intelligence has also been interested in the cooperation between research and business that aims to produce practical applications. In 2007 about 10 % of the Finnish companies interviewed by Supo said that they had been a target of illegal intelligence

[43] *Att skydda svensk bioteknik*, foreword; Anderson Julie (2007) The HUMINT Offensive from Putin's Chekist State. *International Journal of Intelligence and Counterintelligence*, Volume 20, Number 2, 2007, 258-316, p. 269.

gathering during the last two years.[44]

In Sweden, foreign financial and technological intelligence activities often go hand in hand and it is not unusual that technological gathering for military purposes is used to create a financial advantage. Defense-related intelligence gathering thus blends into the financial and technological gathering, whereas purely military intelligence is no longer a priority. Research in areas such as biotechnology, the science of engineering and building materials, optoelectronics, data fusion and other high technology are important gathering areas. Information advantages, competence of strategic importance to a country's development, cutting edge technology and competitiveness are the overriding aims for most of the intelligence activities carried out in Sweden with the purpose of optimizing the interests of a foreign country.[45] A considerable number of intelligence organizations are engaged in activities and at least 15 states have persons with intelligence missions posted in Sweden. Among intelligence actors present in Sweden there are officially reported persons posted to embassies and other official missions as well as unreported staff, which may for instance be working under cover. Additionally, a number of states send their intelligence personnel on regular missions to Sweden. Intelligence services use cover companies and perform in different roles in businesses to be able to get close to key persons and gather information in a natural way. Even representatives from known companies or organizations can work for or give information to foreign intelligence services on the side of their official business. The extent of the presence of foreign intelligence services is considered remarkably large in relation to Sweden's size and power. This can largely be explained by the priority given to financial and technological intelligence gathering, which are areas where Sweden is at the forefront of development. Telecommunications, biotechnology, new materials and innovative defense technology rank high on the intelligence priority lists of many states. As long as there are economic, political or knowledge-related advantages to be gained through intelligence gathering, the risk of espionage will be present and several countries will be seen as a significant threat.[46]

Sweden is at the cutting edge in many technological areas concerning dual use products that may be used in the production of weapons of mass

---

[44] Suojelupoliisi (2007) *Suojelupoliisin vuosikertomus 2006*; *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva syksy 2007*, p. 11; Suojelupoliisi (2008) *Suojelupoliisin vuosikertomus 2007*, p. 6.

[45] Säkerhetspolisen (2003) *Annual Report 2002*, p. 29; *Annual Report 2003*, p. 26.

[46] *Verksamhetsåret 2003*, p. 26; *Annual Report 2003*, pp. 26-28; *Att skydda svensk bioteknik*, p. 5; *Annual Report 2002*, p. 29; Säkerhetspolisen (2007) *Spionärenden 2006 - en sammanställning från öppna källor*, p. 12.

destruction (WMD) but which were originally produced for other purposes. Following 9/11 a number of states and non-governmental actors with ambitions to develop WMDs have tried to acquire such products in Sweden. Furthermore, Säpo has seen an increase in purchases of products that only just meet the criteria for exemption from export restrictions. This indicates that countries with WMD ambitions are becoming increasingly skilled in upgrading products for their WMD programs. The search for information on, and the purchase of products that can be used in the production of WMDs increasingly take place via the internet and through extended cooperation between states with WMD programs. The open climate in Swedish research and know-how in areas such as virus and DNA research make it an attractive country for the gathering of information and capability for biological weapons and protection programs. There is a large international interest for Swedish biotechnology and the branch is at risk to be exploited by espionage both by competing firms and foreign intelligence services. In 2006, Säpo arrested a visiting Russian scholar on grounds of industrial espionage against a Swedish university. The case was related to the field of biotechnology. Säpo considers it likely that Sweden can be used for the acquisition of material to be used in the production of WMDs. There is also a risk that Sweden may be used as a transit country for the transportation of such products.[47]

The targets for industrial espionage in Finland and Sweden are very similar. The development of advanced technologies that have dual use applications are the common feature behind most intelligence efforts involving private sector companies. The economies of both countries lean heavily on research and development that can be further refined into marketable products. Industrial espionage also carries a dimension of national security, when intelligence is directed at research, companies and products that are a part of the defense structure of the given country. All these characteristics were also present in the Ericsson espionage case.

[47] *Annual Report 2003*, pp. 30-33; *Annual Report 2002*, p. 33; *Verksamhetsåret 2002*, p. 32; *Att skydda svensk bioteknik*, pp. 2-3; Säkerhetspolisen (2005) *Företagsspionage.* Rapportserie 2005:1, p. 4; Säkerhetspolisen (2006) *Swedish Security Service 2005*, p. 18; Säkerhetspolisen (2007) *Swedish Security Service 2006*, p. 31.

3 CORPORATE SECURITY

The risks and threats faced by private companies are countered by corporate security. Corporate security encompasses both the management and administration of good security practices as well as the actual execution of protective measures designed to drive a company's security policy. The role of national intelligence agencies in fighting industrial espionage through corporate security is important, yet not always easy to define. While there is a high degree of consensus regarding what constitutes good corporate security inside most companies, the larger framework of nation states and their function in the internationalized context of global business add a dimension to the problem of industrial espionage that is very much in constant motion.

3.1 Managing corporate security

Corporate security is the comprehensive realization and implementation of all security-related affairs of a company. Security is a central prerequisite of a competitive company and an important part of high-quality business.[48] The better the risks regarding people, the environment, property, knowledge and reputation are in control, the higher the level of corporate security. Corporate security is managed by methods of risk control and security management and is dependent on the nature and function of a given organization. The process of managing the security of a company is in constant motion from policy and aims to planning, execution, surveillance and assessment back to development and improvement towards a constantly better form. Security management is integrated into the normal administration of an organization. In practice, the activity for securing the integrity of an organization can be divided into different sectors such as environmental security and information security. The entity formed by these different sectors makes up corporate security. The organization of corporate security is also influenced by the role of security as the protector of the continuation of the business of an organization.[49] The management of a company's security is the responsibility of the corporate leadership. The personnel of a company are the key component of all security-related matters. Continuous monitoring and evaluation are an integral part of a functioning corporate security.[50]

---

[48] The Confederation of Finnish Industries, Elinkeinoelämän Valtuuskunta, EK [www] Available from http://www.ek.fi/ytnk/tiedotteet/yritysturvallisuuden_perusteet.php [Accessed 4 April 2008]

[49] Lanne (2007) pp. 6, 11-13, 22.

[50] Yrittäjän turvallisuuopas 2005 [www] Available from http://www.v-syrittajat.fi/turvallisuusopas.pdf, [Accessed 4 April 2008] pp. 6, 11.

The last years have seen an increase in industrial espionage and corporate crime.[51] Every company has corporate secrets regardless of its size or expertise.[52] The improvement of corporate security has been an important issue during the last years in Europe. The European Council (EC) and the EU have acknowledged the needs to improve the partnership between private and public sector actors. Crimes against companies hamper fair competition and increase the costs of business. Corporate security is an important national competition advantage in Finland and Sweden. A company can base their decision to stay or settle in a country by the level of security that is available there.[53] Expensive technical and organizational security measures have little value if security regulations are not followed by the personnel. A prerequisite for a good level of security is an educated and motivated personnel. There must also be a shared responsibility to follow adopted security routines.[54]

Internet and network crimes constitute a special threat to the intellectual capital of companies, because these crimes are both easier and cheaper to commit in a virtual environment than in real life. The risk of getting caught is also significantly smaller than for example in industrial espionage that utilizes human sources. The attacks against information systems can be categorized into random attacks such as spam e-mails and viruses and targeted attacks that seek to copy or steal the intellectual capital of a company. Companies who have intellectual capital that is of interest to professional criminals are most often attacked by targeted information attacks. Because there is very little talk in public about the way these kinds of attacks are carried out, companies do not necessarily pay attention to this kind of internet traffic or protect themselves from it.[55]

Professional information network crimes are often a latent form of crime. A motivated industrial spy can go unnoticed by the victim. At the moment, the problem is the fragmented nature of information. The police have knowledge of the motives and ways of the crimes committed, but not of the intelligence or targeted attack traffic that is actually present in the internet. Through the cooperation of companies and authorities it would be possible to get valuable information on corporate security work and crime intelligence and better the general protection against targeted internet crimes. The

---

[51] Lanne and Kupi (2007) p. 11.

[52] *Yritysten rikosturvallisuus 2005*: Riskit ja niiden hallinta. Keskuskauppakamari ja Helsingin seudun kauppakamari, p. 17.

[53] *Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi*, pp. 8-11.

[54] *Att skydda svensk bioteknik*, p. 7.

[55] Lanne and Kupi (2007), p. 12; *Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi*, pp. 10-11, 23; *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva syksy 2007*, p. 10.

information possessed by the authorities is not enough alone to form an all-encompassing big picture about the crime situation and its future evolution. Also information from companies is needed. This is especially important in recognizing the threats to companies and countering the crimes against them. The cooperation between officials and different actors in trade and industry must be developed so that companies have better abilities to function in a changing security environment.[56]

The interdependency between the national security machinery and private corporations is at the core of a successful security strategy against industrial espionage. However, this interdependence is not without tensions. Fitting legislation and accountability together must be done without restricting privacy or hampering business. According to Dorothy Denning, these goals can only be reached with extensive collaboration between the private and public sectors.[57] The responsibilities and functions of corporate security and national intelligence agencies sometimes overlap and it is not always easy to identify where the role of one actor ends and another takes over. The legal perspective on industrial espionage and corporate security perhaps best illustrates this problem. The main question in this respect is: how should the legislation on these matters be formed so that the law would be as effective as possible against covert industrial intelligence while still retaining the freedom of information? In the ideal world, the end product of this process would be a situation where the internal security of private companies is maximized and the free flow and access to information is protected. However, because this configuration is in many ways unattainable and because any legislation is a creation of its time, an ongoing dialogue on the matter is needed to stay as up-to-date as possible and to produce a flexible response to new and rising threats to corporate security. In the end, we must ask ourselves what kind of and whose interests are we trying to protect? Which threats are we preparing ourselves against? In all this, it must be remembered that protecting a company's interests might sometimes go against the rights and interests of the individuals who make up that company. This problem leads us once again to the idea of conflicting loyalties within and between the citizens of nation states.

3.2 Information security and corporate responsibility

The development and competitiveness of the information society depends

[56] *Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi*, pp. 8-12, 23-24.

[57] Denning Dorothy E. (2003) *Information Technology and Security*, in Brown Michael (ed.) *Grave New World: Global Dangers in the 21 Century*, Georgetown University Press, p. 20.

largely on the ability to protect the nation's knowledge capital. The importance of information security has increased now that knowledge, whether possessed by individuals or organizations, has become an essential economic resource. Rapid technological development and widespread use of networked information technology has generated risks that are difficult to foresee. Information security is understood to refer to protecting information, services, systems and communications in whatever form with appropriate measures to manage the risks that are threatening them. Information security is a concept wider than the technical security of information and communications technologies. Information security is considered to have been implemented correctly when the confidentiality, the integrity and the availability of information is ensured. Information security is a component of all functions of a society. It also covers information and services that may comprise material protected by intellectual property rights. The conversion of knowledge into capital reinforces the economic importance of information security. At the same time innovative solutions and the identification and development of commercial and widely usable applications must be supported. Information security risks are becoming increasingly diverse with completely new risks and threats continuing to emerge. Identifying and managing risks in advance is a requirement for national security. When risks are reliably identified, their adverse effects can be minimized by developing information security. This will focus on anticipation, not reaction. Risk management also requires sufficient and regular monitoring of the national situation.[58]

Information security aims to secure the protection of an organization's activity by protecting its information systems, reducing the risk of mistakes, misuses, disturbances and physical damage to company information. The basic goal of information security is the reliability, integrity and accessibility of information. Crimes against information security seriously threaten the intellectual capital, efficiency and competitiveness of companies. At the core, a realistic and current picture of existing and future threats and a wholesome preparation for risk situations is needed. The vulnerability of the information society is a growing threat. Companies are more and more dependent on information networks and information systems.[59] In some cases, information security has become important only after the crime has been committed. This is why it is vital for companies to anticipate and not just react to breaches of information security. One of the largest challenges for corporate security is to prevent departing employees copying sensitive information for their own uses. In essence, this is what happened in the Ericsson case. In

[58] *National Information Security Strategy Proposal*, pp. 6-9.

[59] *Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi*, pp. 10, 17.

2005, nearly every fifth company in Finland noticed information copying. Discussions about confidential information and disseminating documents from former employers was also estimated to be quite common.[60] When an organization's intellectual property is transferred and stored in a network, its protection becomes much harder. Ben Rothke's idea behind information management is that when the value of information goes up, so does its value for an organization's competitiveness.[61] Denning has stated that it is impossible to ever have completely secure systems. There will always be vulnerabilities in any technology and what is more, people will make mistakes. Insider espionage is also inevitable. It is therefore important to be able to rapidly detect and respond to any security breaches that may happen.[62]

In Finland, a national intellectual capital project was started as part of the national information security strategy in 2003. Part of the project was a report that interviewed actors from both private and public sector. They represented areas such as teleoperators, universities and research, health care, energy production, forest industry, the civil aviation authority, the national emergency supply agency and banking and finance. The project defined intellectual capital to be non-physical capital which is made of data, information, immaterial rights and the organization itself. Intellectual capital is formed of systematically created conceptual information, which is essential for the efficient functioning and basic tasks of an organization. Examples of this are inventions, technical descriptions and drawings, methodologies, programs, applications, documents and other information objects. In the private sector vital intellectual capital is also comprised of corporate secrets, client information and product development information. In 2007 in Sweden, The Swedish Security Service's security audits identified several flaws in the information security of private companies. Some of the problems were linked to questions of national security and protection against terrorism.[63]

An interesting view about the national dimension of intellectual capital came to the fore in the Finnish report. Especially in the forest industry sector and the telecommunications sector it was noted that national boundaries were blurred in the ownership of intellectual capital. Intellectual capital is the property of an organization and it is not always relevant for a certain area or country. If the intellectual capital leaks out of the organization and finds

---

60 *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva syksy 2007*, pp. 2, 11; *Yritysten rikosturvallisuus 2005*, pp. 17, 47.

61 Rothke (2001) p. 4.

62 Denning (2003) p. 13.

63 Bäckström Jan and Tupala Vesa (2004) *Raportti. **Liikenne- ja viestintäministeriö - Kansallisen tietopääoman suoja –hanke***, 9.12.2004, PriceWaterhouseCoopers, Helsinki, pp. 3-4; Säkerhetspolisen (2008) *Swedish Security Service 2007*, p. 44.

its way to the hands of a competitor, it is considered more damaging than if it is acquired by a foreign nation. In addition, the flow of information inside an organization is more important than protecting information. Despite these views, the report argues that in the end the intellectual capital handled by certain organizations is important to the national competitiveness of Finland because they are based and function in Finland. Many of the organizations mentioned a growing dependency on information technology and the outsourcing of activities. Both things create problems and risks that were not always fully understood.[64] Outsourcing and contracting creates more information security risks and raises the threat of industrial espionage. Exposure to the risk of espionage occurs with outsourcing, both on and offshore. When a company entrusts its proprietary information to a third party, there is a heightened chance that its production methods may be copied and shared.[65]

One of the main techniques employed in industrial espionage that is closely connected to information security is social engineering. The main component in social engineering is the ignorance of the persons who are targeted. When an outsider is familiar with the structure of an organization, it is relatively easy to exploit this knowledge to locate a suitable target within the organization in question. Social engineering can also be applied to persons who lack proficiency in information technologies and security practices. Both of these perspectives inherent to social engineering were present in the Ericsson case where the foreign agent handler exploited the position of an employee inside Ericsson, who in turn used social engineering to widen his collection efforts through two sub-agents. Social engineering has been on the rise in Europe for some time and is thought to be significantly more common than is generally acknowledged.[66]

The rational control of information risks demands the clear acknowledgment of threats. The largest threat is made of the vulnerabilities that make the attacks against corporate security possible.[67] Threats to company networks come from both inside and outside of a company. Special emphasis on information security should be placed against illegal intelligence gathering that focuses on scientific and technical areas.[68] The reality of current threats to

---

64 Bäckström and Tupala (2004) pp. 6-8.

65 *Yrityksiin kohdistuva rikollisuus – teematilannekuva 12.3.2007*. Ulkoistamiseen ja alihankintaan liittyvä rikollisuus. Keskusrikospoliisi: pääosasto ja rikostietopalvelu, Viite: RTP 479/213/2007, pp. 2-3; Tarrant Deborah (2007) A breach of trust. *Intheblack*, October 2007, Vol. 77, Issue 9, 32-35, p. 33.

66 Kajava (2003) p. 7; *Yritysten rikosturvallisuus 2005*, p. 17; *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva syksy 2007*, p. 11.

67 *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva 17.10.2006*, p. 12.

68 *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva syksy 2007*, p. 13; *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva 17.10.2006*, p. 12.

sensitive corporate information places intellectual capital at a level probably never witnessed before. Protective measures are sometimes neglected because of the perceived difficulties or costs associated or simply because the problem of corporate security has not been understood properly.[69]

If a company wants to protect itself against industrial espionage, certain parameters have to be established in order to keep security measures from going overboard. The company must also be able to weigh the value of general espionage protection against investments in research and development. While the defense of intellectual capital is an integral task for any company, increased research efforts aimed at creating new and better intellectual capital should not suffer for the sake of security. Evidence in corporate crimes falls into two main categories: physical and digital evidence. Physical evidence means concrete items whereas digital evidence can be for example data on a computer or a company document.[70] In the Ericsson case, digital evidence revealed the identities of the three perpetrators and physical evidence found in the possession of the main suspect confirmed the source of the information leak.

Industrial espionage can devastate or even bring down a company. Any business whose livelihood depends on information stands to lose it to industrial espionage. While corporate security is the responsibility of the leadership and security unit of a company, it can not be effectively addressed by any individual entity within an organization. Corporate security is ultimately the responsibility of every employee of a company. It has been estimated that the real cost of economic espionage is higher than previously thought. All businesses that have intellectual property of significant value are likely targets for industrial espionage. However, companies are usually reluctant to disclose any perceived vulnerabilities because of the damage it would do to both their reputation and competitiveness.[71]

Hugo Cornwall has identified two broad approaches to handling organizational secrets: information denial and permission granting. In a system where everything is judged to be a secret, individuals are informed only on a "need to know" basis. Cornwall calls this a closed system. In an open system, everyone has access to everything except to the information that is specifically labeled as secret. The closed system becomes problematic when employees need information that is essential to their job, but are denied access to

---

69 Jones (2008) p. 13.

70 Samli and Jacobs (2003) p. 110; Rust James William (2006) *Corporate Management of Computer Forensics Evidence.* Information security curriculum development. Proceedings of the 3rd annual conference on Information security curriculum development. Kennesaw, Georgia, 175-178, p. 176.

71 Tarrant (2007) pp. 32-33; Luong (2003) pp. 62, 72.

it. An open system faces problems in identifying what to protect and how to ensure that all employees operate sensitive information in confidence. Most organizations operate an uneasy hybrid of the two systems.[72] The large electronic database at Ericsson that was at the center of the espionage case is a good example of this. While housing sensitive and confidential information, in the end it was possible for someone who no longer worked at Ericsson to access the information without anyone noticing it.

3.3 The role of national intelligence agencies

Where do national intelligence agencies fit in the world of industrial espionage and corporate security? Samuel Porteous has identified the key question in this regard to be the part a foreign government plays in the perceived case of industrial espionage. By this he means that national intelligence agencies must have a clear mandate on what they are defending the private sector actors against. If a foreign government is either directly involved or supports industrial espionage, the intelligence service of the country in question could act by justifying that another nation state is threatening its national interests. The second choice would be to respond to any industrial intelligence efforts whether initiated by private or public sector actors.[73]

The strongest argument for requiring foreign government involvement as a precondition for an intelligence service to take action is that a foreign intelligence service has considerable resources at its disposal because it is linked to a nation state. The damage a foreign government can do to natural business competition is significant and thus national intelligence agencies should respond to the threat. Industrial intelligence between companies is in this view considered to be a part of normal competition in the private sector, and intelligence services should not get entangled in it. However, it is often difficult in practice to determine if a case of industrial espionage is in fact organized or enabled by a foreign government. The focus on only government-directed efforts at industrial espionage is not always assessing the situation correctly. In many cases, large multinational corporations can employ their own intelligence resources with far better results than an under-resourced nation state trying to steal economic secrets. Porteous estimates that the influence and global reach of the most powerful companies make them as dangerous as the strongest nation states in the field of industrial espionage. If we compare the actors behind terrorism and industrial espionage, we can see that national intelligence agencies respond to the former even when there is no

[72] Cornwall (1991) p. 104.
[73] Porteous (1993).

proven link to any nation state behind it. In the same vein industrial intelligence is a threat to society as a whole, regardless of what entities lay behind it. Every government must decide whether possible economic and intellectual losses are enough of a concern to warrant the use of national intelligence agencies against industrial intelligence.[74]

The role of national intelligence agencies is further complicated by the fact that industrial intelligence is sometimes practiced between allies that share the same political or military commitments. Intelligence services can therefore find themselves competing and cooperating between each other where their countries' economic interests diverge from political and military interests. Samuel Porteous lists this potential conflict between the economic interests and the military and political interests of a nation state as one of the main reasons national intelligence agencies have reservations about their role in preventing industrial intelligence from happening. An additional thing to consider is the possible damage to traditional intelligence-sharing networks that can ensue from the overlapping of private and public sector interests. One future possibility is the emergence of intelligence-sharing networks in economic and industrial intelligence modelled after political and military matters. These networks would most probably be conceived as regional agreements. In Europe, the EU would be the natural framework for this. However, over time economic intelligence-sharing networks built on regional trade groups may seem too inflexible. Nation states and maybe even some unattached economic zones within these states can develop short-term, goal-oriented fluid economic intelligence alliances instead.[75] This perspective also brings into play the earlier question of the loyalty of people to nation states. The emergence of new international networks and alliances would most likely be a sign and also contribute to the erosion of existing loyalties inside the given nation states participating in any future activities of this kind.

New and strengthened alliances based on economic interests will test the longevity of existing military and political coalitions. For example, separate economic intelligence-sharing networks based on rival trade groups inside a larger political union would surely weaken that alliance. Porteous sees the question of industrial intelligence and economic security to be in this way an integral part of the debate on the nature of international economic relationships. In his words, the most important question a nation state needs to ask itself with regard to industrial espionage is: are economic competitors enemies?[76]

---

[74] Ibid. (1993).
[75] Ibid. (1993).
[76] Ibid. (1993).

4 THE ERICSSON ESPIONAGE CASE

Ericsson is a Swedish company that is one of the leading suppliers of telecommunications services and equipment to mobile and fixed network operators around the globe. Ericsson also shares a joint venture in mobile phones with Sony in the Sony Ericsson Mobile Communications company. Ericsson's headquarters are located in Stockholm, Sweden.[77] In 2002 Ericsson was a target of industrial espionage.[78] The Swedish authorities were quick to respond and intervened before any substantial losses were sustained. The Ericsson espionage case has been called the largest case of industrial espionage in Sweden to date.[79]

4.1 The outline of the case

The Swedish Security Service Säpo began to take an active interest in two persons working at the Russian Embassy in Stockholm, identified in the text as number 1 and number 2. These individuals were later judged to be intelligence officers working under diplomatic cover. Consequent investigations revealed number 1 to have been in charge of an operation that included running agents that number 2 later took over. A breakthrough in the investigation occurred on 5 August 2002, when it was established that number 2 met a man at a train station in Norrvik, north of Stockholm. They were shadowed and the man in the company of number 2 was identified as Afshin Bavand.[80]

Afshin Bavand was born and raised in Iran. He was educated as an engineer in the Philippines and came to Sweden as a political refugee in 1983. Bavand started working at Ericsson in 1995-1996. He was made redundant in the summer of 2001 because of a shortage of work. However, Bavand remained connected to Ericsson until August 2002 through "Framtidsforum" (the Future Forum), a program designed to help him find a new job. It was during this year that Bavand became engaged in industrial espionage against his former employer. Despite the fact that he had been let go, Bavand still had access to the internal GASK network at Ericsson that stores all data from previous and ongoing projects, to his work computer that was connected to Ericsson's intranet and the internet as well as to his phone number and e-mail address with Ericsson until August 2002. During one of his last days at

---

[77] Ericsson [www] Available from http://www.ericsson.com/ericsson/corpinfo/index.shtml [Accessed on 4 April 2008]

[78] *Verksamhetsåret 2002*, p. 31.

[79] Repo (2004) p. 37.

[80] Stockholms Tingsrätt, Rotel 1301, Avd 13, Dom, Mål nr B 7025-02, meddelad i Stockholm, 2003-06-17, p. 9.

Ericsson, Bavand had wheeled out documents and noticed that no one had paid any attention to his activities. He planned to support himself by finding new business contacts in telecommunications. Bavand visited Ukraine, Dubai and Poland and also had intentions in Iran regarding the metal industry. A company was registered under his name that was supposed to deal in all kinds of export and import activities. Bavand also rented an office for this purpose outside of Stockholm in September 2002.[81]

Afshin Bavand did not act alone. After intensive investigations that included intercepting phone calls, it was established that Bavand had contacts with both Mansour Rokkgireh and Alireza Rafiei Bejarkenari, who at the time were employed as test and development engineers at Ericsson. Rokkgireh came to Sweden in 1979 and studied at the Stockholm Technical Institute. He worked at Ericsson for 15 years. Rokkgireh met Bavand by chance and the two of them became very close. They originally hailed from the same part of Iran and a childhood friend of Rokkgireh's was married to Bavand's sister. Rafiei received an e-mail from Bavand in May 2002 and they met for lunch in June. They discussed Rafiei's work at Ericsson. Earlier they too had met randomly. Bavand also knew Rafiei's brother who went to The Royal Institute of Technology in Stockholm.[82] Bavand first requested information from Rokkgireh probably through a fax message sent in April 2002. He received the information on 30 to 40 computer disks. Rokkgireh never questioned the legality of his actions. He did not ask if Bavand was still employed at Ericsson. On 15 October Bavand called Rokkgireh with a list detailing his interests. Rokkgireh visited Bavand's office a few times and Bavand also came to Rokkgireh's workplace at Ericsson during the summer to show him how to get documents from the GASK network. It was estimated that of the total documents found in Bavand's possession, about 30 to 35 % had come from Rokkgireh. He also planned to join Bavand's business, but nothing concrete was decided.[83]

Rokkgireh thought that employees had the right to take documents from GASK without any restrictions. He was not familiar with the security classifications at Ericsson and had not signed an agreement related to these matters. From April until August Rokkgireh gave documents to Bavand on approximately five occasions. Rokkgireh thought that Bavand held a managerial position and that the documents would be used for his work at Ericsson. Bavand did not compensate Rokkgireh in any way for his work. From the spring until the fall of 2002 Rokkgireh worked for three different chiefs. He was not clear on how internal documents should be handled and his English was poor even though it was the company's official language. Furthermore, Rokkgireh was

[81] Ibid., pp. 18-19; Repo (2004) p. 37.
[82] Stockholms Tingsrätt, Rotel 1301, Avd 13, Dom, Mål nr B 7025-02, pp. 9, 20-22.
[83] Ibid., pp. 19-20.

confused what Bavand meant in their phone conversations by "a person" or "friends" who were involved in the gathering of information. Rokkgireh was also unsure what Bavand implied when he spoke of creating trust and that the information he was looking for needed to come from the inside of the company and "must not be found about" for "otherwise they do not want it".[84]

According to Rafiei, he met Bavand five or six times. Rafiei promised to tell Bavand if he found out that Ericsson was selling the kind of measuring instruments Bavand was interested in. Rafiei thought that Bavand was interested in his work because he was applying for a job with his department. Rafiei did not give any documents directly over to Bavand, but instead worked on them at home, where he erased the reference numbers to lessen the risk that they should be traced back to Ericsson if they ended up in the wrong hands. During questioning, he could not explain how certain documents that he had worked on ended up on discs and a hard drive found with a computer in Bavand's office.[85]

Six months after he lost his job, Bavand was contacted by a Russian engineer who phoned him. The Russian, who called himself "Boris" (and who Säpo later identified as number 1), met Bavand two or three times. They talked about their common interests such as importing gas from Russia to Finland and further on to Sweden and Germany. Boris planned to start a company that could cooperate with Bavand's future business. When Boris traveled back to Russia, he left his phone number and a pager for Bavand. No contacts took place between the two men in the subsequent months and Bavand began to get nervous. During this time it is possible that Bavand was being approved as a contact with the Russian intelligence service.[86] He talked with an Iranian friend living in Russia, named Sulyeman, who told him that he would be contacted. In the beginning of July Bavand received a call and was told that another man would visit him. This man was known as number 2 in the investigation of the case.[87] Number 2 was not as proficient in technical matters as Boris had been. The third time Bavand and number 2 met, Bavand appeared serious as he talked about a company called Simontech he would establish. During the fourth meeting they talked about patents and Bavand gave some documents to the Russian to show in which areas he could work. For this, he was given no payment. While Boris used to meet him at his home, number 2 met Bavand in different locations usually when one of them was running errands. They met five to six times.[88]

---

84 Ibid., pp. 20-22.
85 Ibid., pp. 22-23.
86 *Annual Report 2003*, p. 27.
87 Stockholms Tingsrätt, Rotel 1301, Avd 13, Dom, Mål nr B 7025-02, pp. 23-24.
88 Ibid., p. 24.

4.2 Information security and the stolen documents

Testimonials were carried out to further investigate claims of industrial espionage and spying on the request of the prosecutor. Some of the witnesses were given code names while the rest were identified in the judgment. Witness RPS 1579 was part of the team that examined the cd disc, computer discs and two hard drives that were confiscated from Bavand. The material was copied to avoid any damage to the original files. The so-called forensic mirror copies were then analyzed and identified. The cd disc found on Bavand when he was arrested contained a lot of the material found on the hard drive of his computer. The hard drive was divided into an upper and a lower drive, where the upped drive had 7,080 files and the lower contained 4,791 files assigned to the catalogue named "Projekt". In total, there were a great number of files, around 20,000 to 100,000 documents. Bavand had searched for documents at Ericsson that were classified as "limited internal" or higher.[89]

Witness RPS 1429 inspected the two hard drives and discs that were connected to Rokkgireh. While the hard drive contained nothing of interest, the discs on the other hand included a large number of secret documents. The witness examined 164 discs, of which around half contained Ericsson's documents. Some of them were classified as "confidential". Witness RPS 1488 worked with the material that was judged to have come through Rafiei. Two discs found at Bavand's office were inspected and two files from the first disc were located on Bavand's hard drive under the folder "8 Document 11-new deliver on 22 aguast" while six files were found in the folder "AAL DOCUMENT DELIVERED\Aguast-document Delivered 2002-0805\this document belong to Number 2 person". Moreover, 11 files from the second disc were found on the same hard drive under the folder "AAL DOCUMENT DELIVERED\8-Document11-new deliver on 22 aguast". Ericsson identified eight of these documents to be classified as "limited internal". Rafiei's username "rsarafi" that he used at his workplace at Ericsson was also connected to the copying of the files.[90]

Carl Siegfelt was Rokkgireh's superior from January until July 2002. He testified that Rokkgireh worked as a member of a 7 to 8 person strong team that was tasked with integrating hardware with software and carrying out tests. Siegfelt went through the cd disc that contained the documents found on the discs. He specified that the discs that contained information Rokkgireh could have possibly needed for his work. Siegfelt considered the persons working in his unit to be well aware that they were dealing with secret material. Tommy Pollack worked as the director of a development unit at Ericsson.

[89] Ibid., pp. 27-28.
[90] Ibid., pp. 28-30.

From July to September 2002 Rokkgireh worked for him as a test engineer for certain programs. Rokkgireh did not have time to familiarize himself with the work before he was transferred to other tasks. Pollack went through two cd discs and identified the documents that included information Rokkgireh needed for his work. It is possible that Pollack encouraged Rokkgireh to use GASK to get started in his new work. Pollack did not speak to Rokkgireh about approved security rules. Hosoon Ku worked as a technical director at Ericsson where he was Rokkgireh's superior from September to November 2002. He looked at two cd discs with the police and gave his evaluation on the documents in question. Ku spoke English with Rokkgireh, who had difficulties with the language and especially with technical expressions. Like Pollack, Ku did not go over the security rules with Rokkgireh.[91]

Jan Uddenfeld, who at the time was a technical director at Ericsson, testified that products under development are documented in databases so that the people who work on the project can get the information they need. The work is guarded by rigorous security measures and access to the information itself is protected by different layers of security and built on agreements with the employees. If a person has bypassed the layers of security, it is because they have needed the information in their work. Uddenfelt emphasized the fact that Ericsson's future was built on research and development and that it is important for Ericsson to bring new products to the market before their competitors. In 2001, 40 billion Swedish kronor (c. 3,8 billion euros) were allocated to research and development, with the majority of funds going to mobile systems. In 2002, the sum was 30 billion kronor. Ericsson's turnover was around 150 billion kronor in 2001. Carl Olov Blomqvist was at the time the chief lawyer at Ericsson. He told the authorities that all documents at Ericsson are classified by whoever produces the document. The documents that are not open are divided into four different classes which are Ericsson wide internal, limited internal, confidential and strictly confidential. If a document is not classified, it is considered to be "limited internal". Blomqvist understood the level of security awareness at Ericsson to be good.[92]

4.3 Significance of the case to Swedish national security

The arrest that concluded the surveillance phase of the case was preceded by a focused counter-espionage operation that detected and established the

[91] Ibid., pp. 30-31.
[92] Ibid., pp. 31-33.

industrial espionage against Ericsson. Through operative fieldwork in conjunction with intelligence analysis Bavand's identity was revealed.[93] The arrest also meant that a number of other people were detained and thoroughly questioned. Moreover, the intervention resulted in two Russian diplomats being declared persona non grata.[94] The police were inclined that Bavand was going to turn over secret material and were going to stop it. However, the location of the next meeting between him and his handler was not clear. On 5 November 2002, a Säpo officer sighted number 2 at Sollentuna train station, where he walked through the building towards the town center. After about 50 meters he turned abruptly and walked out of the building. Number 2 then entered a Chinese restaurant and drank a beer. Afterwards, he made his way back towards the train station and stood on the platform where the train for Stockholm would stop. Directly before the train going to the opposite direction arrived, number 2 quickly changed platform sides and took the train north. He exited the train at Norrvik station and walked into a parking lot by the station building. When Bavand was seen approaching the station he checked the time and looked around. Bavand was carrying a cd disc in a transparent cover. Number 2 seemed happy and was soon met by Bavand. They got into Bavand's red Mazda and drove away in the same direction that Bavand had come from. A conversation ensued with number 2 gesturing a lot and carrying the conversation. The car disappeared for a while and was then spotted in a parking lot in Edsberg where number 2 and Bavand were taking a walk and talking.[95]

The surveillance team following them called backup, which arrived at the scene shortly. One of the officers recognized Bavand. At approximately 17.30 in the darkening evening plain clothed Säpo officers with their guns drawn interrupted the meeting and arrested the two men. Bavand was restrained with handcuffs. A cd disc, a pager and a paper with a phone number and some other papers were found in his pockets. A portfolio with documents was also detained from his car. Bavand claimed the Russian to be a business acquaintance with connections to Poland and that they had known each other for a long time. Bavand was surprised about the arrest but did not seem shocked or distressed.[96] The Russian seemed astonished. A reference list from Ericsson with four markings was found on him as well as a notepad and a paper with a sort of list for a curriculum vitae that could work as a foundation for the recruitment of agents through Bavand. The Russian also had an envelope with 40 uncirculated 100-dollar bills. With the discovery of the Ericsson

[93] *Verksamhetsåret 2003*, p. 25.
[94] *Annual Report 2003*, p. 25.
[95] Stockholms Tingsrätt, Rotel 1301, Avd 13, Dom, Mål nr B 7025-02, pp. 33-35.
[96] Ibid., pp. 33-34.

documents, he identified himself as a Russian diplomat. This was confirmed by phone from the Swedish Ministry of Foreign Affairs. The diplomat was offered a lift, but he declined. Rokkgireh and Rafiei were also arrested on the same day.[97] The largest case of industrial espionage in Sweden had come to a dramatic close in a parking lot outside of Stockholm.

When Bavand and number 2 were captured, Bavand claimed he did not know why the Russian diplomat had 4,000 American dollars with him and said he had no intention of giving any of the documents he was carrying to the Russian. He further disputed that the expression "have deliver" found in the folders on his computer meant that the documents in question had been delivered to another person but that the information had been transferred from discs to the hard drive for Bavand's personal use. The documents were supposedly organized in different formats as a security measure so that Bavand could take them home and read them there. The fact that there were deposits on Bavand's bank account right after certain meetings with number 2 was also something Bavand denied having a connection with delivering information to another person. On 22 August he met number 2 in Häggvik, and it is possible that he had carried a cd disc with him. However, Bavand denied giving the disc over to number 2 and claimed it contained music, not secret information. The next day Bavand received a payment in his account with the online stockbroker Avanza. He also received money after the meetings on 9 July and 5 August. On these occasions Bavand's bank account was credited.[98]

As to the communications with his handlers, Bavand told that it was Boris who gave him the pager and instructed him on its use. He thought it was a strange way to communicate. When Bavand placed a call to Boris or number 2, it was always from a phone booth. He had been told not to use a mobile phone. However, the meetings were never scheduled with the pager. Bavand told that he also had the list of qualities that possible recruits should have that number 2 was carrying when they were captured. The list was meant to show the possible areas that Bavand could work on and it was probably him who made the notes on the list. Bavand had received help and advice on technical questions related to the topics on the list from a South American person who had been previously employed at Ericsson. The South American had returned home and was not involved in the dealings with the Russians. Both number 2 and Bavand had identical papers with a curriculum vitae, which was supposed to be used in guiding the recruitment process of new agents. Cooperation was at the top of the list of desirable qualities. Number 2 had three names on

[97] Ibid., pp. 10, 34.
[98] Ibid., pp. 24-25.

his list that had been selected due to their backgrounds and skills and were thought to be interested in his project. Bavand also had a letter with him that started with the words "Hello dear friends" directed to the Russians he hoped to cooperate with. In the letter he named Rokkgireh and Rafiei among the persons he thought could be considered for the project. Bavand told that his emphasis on getting internal information through Rokkgireh was based on his curiosity. When asked about the comment he had made to Rokkgireh "otherwise they do not want it, you can find them yourself", Bavand replied he was referring to the potential customers of his company in Iran and elsewhere. Bavand explained that if he would do business in Iran with Ericsson's products, it would also benefit Ericsson.[99]

One of the primary tasks of the Säpo's Counter-Espionage Section is to interrupt any clandestine contacts between intelligence actors and information carriers before they lead to espionage or other crime. An important part of the Section's preventive efforts consists in increasing the awareness of other authorities and Swedish companies in Total Defense, especially in the risks of intelligence activities in order to make them better prepared to counter such activities.[100] Changes in the Swedish law have incorporated industrial espionage under the crime of spying. What was earlier a crime against "the defense of the state" has now been replaced with the term "total defense". Spying can now be seen as an offence against either national security or Total Defense. The offence must be something severe to be classified as espionage. In the judgment of the Ericsson espionage case, such things are considered to be Swedish industrial secrets and other research findings that can become important in the future manufacturing of new Swedish military equipment. The threat assessment and the direction of military defense in Sweden have changed considerably since the spy section of the law was altered in 1981. In the Swedish armed forces much weight is placed on terms such as "information advantage" and "management advantage" and how they can be achieved by using modern technology. One way for a state that is interested in this is to thwart the progress of other states in acquiring an advantage by building more advanced systems or finding points of attack in the others states' systems. For Sweden, plans of a network-based defense (nätverksbaserat försvar, NBF) have begun to take shape. Military defense has changed its direction from an anti-invasion force to cooperation with military units and civil authorities. Technical development has importance for management and connection systems as well as the construction of NBF mainly in civil high technology companies. Ericsson is one of these companies and one of the world leaders

[99] Ibid., pp. 25-27.
[100] *Annual Report 2002*, p.31.

in the development of mobile technology. Representatives of Swedish military security and Säpo have stated that technical development is the factor that has affected intelligence activities the most in recent years. The assessment of the intelligence threat to the country's international status in research and development in the field of high technology has considerably risen in importance when compared with other things that tend to be of interest to foreign intelligence activity.[101]

A great number of documents belonging to Ericsson were found on a cd disc that Bavand had in a plastic bag when he was captured. Moreover, around 2,700 documents from Ericsson were found on the hard drives in Bavand's computers. Of the documents a considerable amount were classified as "confidential" or "limited internal". It means that certain persons inside Ericsson have had access to the information and the material in question has not been allowed to be disseminated outside of Ericsson without the company's permission. According to a witness testimonial by technical expert Gösta Lemne from Ericsson, the material concerns technical solutions with a connection to mobile phones as well as landline telephones and concerns both existing systems and future systems. Lemne testified that Ericsson would have suffered great economic losses if the material had found its way to the hands of competitors. It seems that the material in question was directed at finding out more about the different parts of systems than about technical information that could have been put to use directly. According to Lemne this can be interpreted to mean that the persons were trying to manipulate the system rather than seeking to build a corresponding system themselves. The copying of the system would have required more information and skills. In a secret enclosure to the judgment it has been shown that the information in question had both importance to the Swedish military and the civilian defense.[102]

Bavand was no longer employed by Ericsson from August 2001 on, as he himself also admitted. He could not have needed the documents in question in his work at Ericsson and he did not have access to the GASK database, which housed the information. At the time of his capture, Bavand had an envelope, which showed his contacts with Rafiei and Rokkgireh. The finding also strengthens the argument that Bavand was involved in information gathering for number 2 and that the intention was to engage other people in the activity. It can therefore be argued that Rokkgireh and Rafiei were acting as Bavand's sub-agents. In the light of RPS 1625's testimony about the ways the Russian intelligence services operate and run agents, these conclusions appear to support the argument. Through the information RPS 1625 gave and

[101] Stockholms Tingsrätt, Rotel 1301, Avd 13, Dom, Mål nr B 7025-02, pp. 36-37.
[102] Ibid., p. 38.

what else was found out about the Russian diplomats' travels, meetings and their actions in these relations, the District Court considered further proven that both number 1 and number 2 were Russian intelligence officers with a cover position in the Russian Embassy in Stockholm.[103]

Bavand's contacts with number 1 corresponded with notes in his calendar for 2000-2002. Telecommunications data retention from Bavand's mobile phone also revealed him to have been in the places that were located near the meeting places. In connection with the meetings money deposits were made in Bavand's bank account and depot with Avanza. The investigations concluded that already in 2001 Bavand was in contact with number 1 and the meetings between the Russian intelligence officers and Bavand amounted to a substantial economic benefit for Bavand. Certain names in the folders in Bavand's computer with the words "document" and "deliver" as well as the dates or months had a clear correlation in terms of time with the meetings and the deposits during the summer and fall of 2002. This, together with the testimonial of witness RPS 1875, made it possible that Bavand had passed on documents in these meetings. The pager that was found on Bavand was connected to a number of calls made from payphones in Stockholm and the number of the pager was found in the notes on Bavand. The pager was also called from the places and times when Bavand had been near a base station according to his mobile phone. Evidence also indicated that communication between Bavand and the Russians was handled by two pagers equipped with a code for meetings and the calls were always made from a public phone so that they could not be traced to a certain person. Witness testimonials from RPS 1625 further backed the claim that this procedure is compatible with intelligence operations.[104]

Was Bavand knowingly involved with a foreign power? In questioning, Bavand stated that he thought Boris and number 2 were representatives for some Russian company. He had no evidence of this during his time with the Russians. The meeting places were chosen because they were protected from visual observation, listening and the use of anti-observation measures. Furthermore, the existence of coded messages was a clear indication of a foreign intelligence activity. Of special interest were the pager and the codes as well as the letter found on Bavand with the introduction "Hello dear friends". Witness RPS 1625 has asserted that the use of codes and the existence of such a letter would not have been possible until the agent had been approved to be reliable and loyal to his runners. The real name of number 1 and the note "Russian Embassad" are further evidence of this. The judgment of the court decided that Bavand had a direct involvement with a foreign intelligence ser-

[103] Ibid., pp. 38-39.
[104] Ibid., p. 40.

vice and that he illegally gathered and provided them secret documents.[105]

4.4 Assessing the case

Tomas Lindstrand, the chief prosecutor on the Ericsson case, said it was the first real industrial espionage case in the country and the first industrial espionage case that has led to a judgment for serious espionage.[106] The documents found in the possession of Bavand that were classified as "confidential", "limited internal", "internal limited" or "restricted intern" came for the most part through Rokkgireh. This was established by phone calls between Rokkgireh and Bavand as well as logging in to the GASK system using Rokkgireh's username. The fax messages that were found from Bavand and Rokkgireh showed that the cooperation for getting information from Ericsson had been underway since at least 17 April 2002. The information supplied by both Bavand and Rokkgireh made it clear that sometime during the summer of 2002 Rokkgireh let Bavand take out documents himself from GASK by using Rokkgireh's computer at his workplace. The court judged Bavand to have been guilty of espionage. The crime concerned a great deal of high technology information, which in the hands of a foreign power could cause significant injury to Total Defense in the event of a crisis or a war. It is because of this that the circumstances were of great importance and the sentence was therefore given on serious espionage.[107]

Rokkgireh was employed as a technician for many years at Ericsson and was therefore aware of the importance of not letting sensitive company information get into the wrong hands. If Bavand had needed information for his own work at Ericsson, he should have been able to get it himself from GASK. Rokkgireh never asked why Bavand himself could not retrieve the information and must have been aware that Bavand was unable to do that. Rokkgireh must also have been aware of Bavand renting office space in Sollentuna and that Bavand committed himself to diverse business ventures without a connection to Ericsson. An aggravating fact for Rokkgireh is that he knew from Bavand that the information he was supplying to him was going to be handed over to other persons and that the information was to be such that could not be gathered from the outside. Rokkgireh was sentenced on accessory to industrial espionage that was considered serious. Rafiei stated that he thought Bavand was still working for Ericsson and was allowed to get secret information. The eight documents that came from Rafiei were from a technical area that he worked on. The do-

[105] Ibid., p. 41.

[106] Repo (2004) p. 43. See also *Verksamhetsåret 2002*, p. 31; *Annual Report 2002*, p. 32; *Företagsspionage Rapport 1/2004*, pp. 8-9.

[107] Stockholms Tingsrätt, Rotel 1301, Avd 13, Dom, Mål nr B 7025-02, pp. 43-44.

cuments were found on his work computer in their original form whereas the documents found on Bavand were altered so that it was not possible to directly see that they came from Ericsson. Rafiei must have been aware that the documents contained sensitive information to the company. Rafiei had signed an agreement that made it clear he was aware of rules and industrial secrets at Ericsson. The information in Rafiei's documents had a significant importance and this must have been clear to him, because it involved his area of work. Rafiei was also sentenced on serious industrial espionage.[108] If the crime had not been discovered by Säpo as early as it was, the case would have become much more serious than it did, for Bavand was set to increase the number of informants. No military threat towards Sweden was perceived during the time that the crime happened. The judgment stated that it is also possible that fast developments in technology can overcome some of the weaknesses exposed by Bavand's espionage in the not too distant future. Bavand was sentenced to 8 years in prison. Rokkgireh was sentenced to 3 years and Rafiei to 1 year.[109]

The three Iranians guilty of industrial espionage had all been employed by Ericsson for some time. They were also all connected on a personal level through ethnic and family ties. While the guilty parties claimed not to have been aware of the security measures at Ericsson, it is also clear that corporate security at Ericsson failed to protect its secret information from insider espionage. The poor security practices at Ericsson have a large responsibility for what happened. Both Rokkgireh and Rafiei must have known that they were engaged in illegal activities. When Rafiei erased the reference numbers from the documents he had copied, it is very doubtful that he was not aware of what was going on. In Bavand's case, it is most obvious that he made a conscious decision to spy. He supplied the Russian diplomat with secret information from Ericsson out of his free will seeking classified documents in a systematic matter. Later, he was also rewarded money for his services. The two lists present in the evidence also confirm that the operation was well planned and professional. It is reasonable to assume that Bavand was recruited and worked for the Russian Foreign Intelligence Service (SVR, Sluzhba Vneshny Razvedky), which is in charge of Russian industrial espionage in foreign countries. The areas of interest and the guidelines for recruiting more agents speak volumes on this matter. Bavand also knew his handler to be connected to the Russian government and the Russian embassy in Stockholm. Lastly, the communication between Bavand and the Russians is a classic example of a covert intelligence operation. Codes, pagers, payphones and secretive meeting places all confess to the world of illegal intelligence gathering.

[108] Ibid., pp. 44-45.
[109] Ibid., pp. 46-47.

5 CONCLUSION

This study has mapped out the current trends and problems in industrial espionage and corporate security in Finland and Sweden. By incorporating previous research with a case study that both encompasses and expands on these points of departure, the research object has been dealt with in a way that makes it now possible to answer the research questions of this dissertation and address the additional issues that have accompanied it.

5.1 Industrial espionage in Finland and Sweden

Industrial espionage has been on the rise after the end of the Cold War and it has become a core concern for companies as well as the national security agencies in Finland and Sweden. The importance of a knowledge-based economy and the rise of information technology have been beneficial to the economies of these two nations. However, they have also made the national economies more vulnerable because the industries that now matter are prone to information security risks. Industrial espionage often utilizes new technologies efficiently, while still employing classic methods and sources such as human agents. The phenomenon of industrial espionage is in constant motion. While the basic elements have gone relatively unchanged the aims, methods, uses and intentions behind industrial espionage are expanding into new territories. The damage done by industrial espionage is not only restricted to the company that falls victim to illegal or covert intelligence practices. Industrial espionage also hurts the state, which in the case of both Finland and Sweden has invested in higher education and research that produces the people working for the company. The state is further responsible for providing a secure and beneficial environment for the companies housed inside its borders. Industrial espionage can also influence the course of economic policy and global competition. Lastly, industrial espionage efforts are closely connected to the defense doctrine and national security questions in Finland and Sweden. The companies that produce some of the most exciting new technologies and innovations today contribute their knowledge and dual use products towards national defense. In the Ericsson case this was one of the main reasons the stolen information had such a significant meaning for the Swedish state as well as for Ericsson.

The emergence of trading blocs and the deepening economic integration in Europe has added further questions to the realm of industrial espionage in Finland and Sweden. During the Cold War, illegal collection and outright theft of economic information was kept mostly in check inside the Western

bloc. Now, in the age of fluid alliances and multinational corporations, industrial espionage happens between political and military allies as well as inside individual countries. While there is yet no direct evidence of this between Finland and Sweden (due also to the high level of integration between the two economies), it is worth remembering that for example Nokia and Ericsson are very much rival companies and hugely important to their respective countries. The increased economic competition also brings into question the difference between normal, open source information gathering used in competitive intelligence and illegal intelligence methods. While covert methods are evolving, the dividing line between what is acceptable and legal and what is not has not changed much over time. This area of industrial espionage is connected especially to questions of information security.

The role of corporate security is the most prominent element in preventing industrial espionage. In most espionage cases, security breaches have been contributed to problems with the company personnel. It is possible that not all employees are always clear on what is permissible and what is not, but this margin of misunderstanding is overshadowed by the fact that not even the best physical security measures can function efficiently if they are targeted by dedicated and skilled agents from inside. As the Ericsson case shows, there is no panacea against human sources operating against their current or former employer. What corporate security can do is to invest resources into recruiting, security awareness and discreet monitoring in the workplace that do not cross the boundary of trust between employees and their employer. This is the practical point of view on industrial espionage as it is seen in the private sector. On a more theoretical level, corporate security is connected to the larger question of loyalty towards nation states and companies. If we look at industrial espionage from the position of the national security agencies, the question of loyalty to both companies and nation states is at the intersection of the problem. Globalization has changed many of the traditional notions of intelligence. With regards to industrial espionage, the competition between rival states has been replaced to some degree by the complex picture of shifting loyalties and changing identities in a world where corporations have taken over some of the areas of influence previously possessed by only states. While economic power is still crucial to the national security of a state, the responsibilities and the power of the companies that make up the national economy stretches beyond national boundaries. The relationship between public and private sector entities thus brings an important dimension to the problem of industrial espionage.

As the world economy and the national economies of states become more important in the international discourse, the domains of business and

intelligence must strengthen their relations. In Finland and Sweden, the ties between private and public sector actors have traditionally been close. However, what is needed is more interaction and communication in areas of corporate security. The national intelligence agencies or other authorities cannot respond adequately to corporate crime and industrial espionage if the companies in question do not voluntarily cooperate. On the other hand the corporate security units of companies need continued assistance and up-to-date intelligence and information from the state in order to not just anticipate, but to efficiently react to different threats of industrial espionage. The tension in the interdependency between the national security machinery and private corporations is best encapsulated by the legal perspective on illegal industrial intelligence. While freedom of information and civil liberties must be a continued priority of an open society, the current and future threats to for example a company's intellectual property demand strong, flexible and modern responses.

5.2 Researching intelligence and security

Researching the current and relevant elements of industrial espionage in a coherent and compact way has been challenging. This study on industrial espionage has been based on publicly available open sources. As such, it has had limitations from the start as to what degree it has been possible to provide new information in this context. It would have been interesting to use the internal studies on industrial espionage prepared by both Supo and Säpo, but these are classified documents. The case study on Ericsson has confirmed many of the existing ideas on corporate security and industrial intelligence. The broader significance of the findings presented here is the application of current scholarship on industrial espionage to the context of the knowledge-based economies of Finland and Sweden. The limitations of this study are visible both in its scope, which has been curbed by the available sources and its depth, which has been dependent on what new information can produced in a postgraduate level dissertation dealing with a fragmented and mostly clandestine subject. Future research would do well to utilize quantitative methods such as statistics and structured interviews to further clarify the picture of industrial espionage in Finland and Sweden. The use of legal documents and the possibility of employing secret documents would also undoubtedly bring more weight and credibility to the research.

The threat posed by industrial espionage comes from both nation states and multinational corporations. The economic competition between trading blocs, nations and private sector entities is an important part of international

politics and commerce and it will continue to gain significance in the future. Industrial espionage encompasses subjects as diverse as possible links to terrorism and questions of national security. Both corporate and national security actors in Finland and Sweden face a long-term challenge in better understanding and countering industrial espionage.

References

For a detailed explanation of the Finnish and Swedish sources used in the text, please see pages 2-4.

Primary sources

Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi. Sisäinen turvallisuus, Sisäasianministeriön julkaisuja 15/2006.

Judgment of the Ericsson espionage case. Stockholms Tingsrätt, Rotel 1301, Avd 13, Dom, Mål nr B 7025-02, meddelad i Stockholm, 2003-06-17.

National Information Security Strategy Proposal. November 25, 2002, Proposal of the Advisory Committee for Information Security [www] Available from http://www.ficora.fi/englanti/document/infos.pdf [Accessed 4 April 2008]

Suojelupoliisi (2007) *Suojelupoliisin vuosikertomus 2006.*

Suojelupoliisi (2008) *Suojelupoliisin vuosikertomus 2007.*

Säkerhetspolisen (2003) *Verksamhetsåret 2002*.

Säkerhetspolisen (2003) *Annual Report 2002*.

Säkerhetspolisen (2004) *Att skydda svensk bioteknik. En broschyr om att skydda forskning, kunskap och produkter mot spionage och framställning av biologiska vapen.*

Säkerhetspolisen (2004) *Verksamhetsåret 2003*.

Säkerhetspolisen (2004) *Annual Report 2003*.

Säkerhetspolisen (2004) *Företagsspionage Rapport 1/2004.*

Säkerhetspolisen (2004) *Företagsspionage Rapport 2/2004.*

Säkerhetspolisen (2005) *En vägledning till Säkerhetsanalys.*

Säkerhetspolisen (2005) *Företagsspionage.* Rapportserie 2005:1.

Säkerhetspolisen (2005) *Företagsspionage Juni 2005.* Rapportserie 2005:3.

Säkerhetspolisen (2007) *Spionärenden 2006 - en sammanställning från öppna källor*.

Säkerhetspolisen (2006) *Spionärenden 2005 - en sammanställning från öppna källor*.

Säkerhetspolisen (2008) *Swedish Security Service 2007*.

Säkerhetspolisen (2007) *Swedish Security Service 2006*.

Säkerhetspolisen (2006) *Swedish Security Service 2005*.

Yritysten rikosturvallisuus 2005: Riskit ja niiden hallinta. Keskuskauppakamari ja Helsingin seudun kauppakamari.

Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva 17.10.2006. Keskusrikospoliisi / rikostietopalvelu / tiedustelu 1 / tutkimus. Arkistoviite KRP/RTP 7936/213/06. 12.10.2006.

Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva syksy 2007. Keskusrikospoliisi / rikostietopalvelu 1.10.2007. Arkistoviite KRP/RTP 479/213/07.

Yrityksiin kohdistuva rikollisuus – teematilannekuva 12.3.2007. Ulkoistamiseen ja alihankintaan liittyvä rikollisuus. Keskusrikospoliisi: pääosasto ja rikostietopalvelu. Viite: RTP 479/213/2007.

Yrittäjän turvallisuuopas 2005. [www] Available from http://www.v-syrittajat.fi/turvallisuusopas.pdf [Accessed on 4 April 2008]

Literature

Adams James (1995) *The New Spies: Exploring the Frontiers of Espionage*. London: Pimlico.

Anderson Julie (2007) The HUMINT Offensive from Putin's Chekist State. *International Journal of Intelligence and Counterintelligence*, Volume 20, Number 2, 2007, 258-316.

Berkowitz, Bruce D. (1996) *Information age intelligence*, Foreign Policy, Summer 1996, Issue 103.

Boren David L. (1992) *The intelligence community: how crucial?* Foreign Affairs, Summer 1992, Volume 71, Issue 3, 52-62.

Chan Marjorie (2003) Corporate Espionage and Workplace Trust/Distrust. *Journal of Business Ethics*, 42, 45-58.

Clough, Chris (2004) Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation. *International Journal of Intelligence and CounterIntelligence*, 17:4.

Cornwall Hugo (1991) *The Industrial Espionage Handbook.* London: Century.

Bäckström Jan and Tupala Vesa (2004) *Raportti. Liikenne- ja viestintäministeriö - Kansallisen tietopääoman suoja –hanke*, 9.12.2004, Helsinki: PriceWaterhouseCoopers.

Daveri Francesco and Silva Olmo (2004) Not only Nokia: what Finland tells us about new economy growth. *Economic Policy*, April 2004, 117-163.

Denning Dorothy E. (2003) *Information Technology and Security*, in Brown Michael (ed.) *Grave New World: Global Dangers in the 21 Century*, Georgetown University Press.

Denning Dorothy E. (1999) *Information Warfare and Security*, Addison-Wesley, ACM Press Books, New York.

DeWitt Maggie (2006) Corporate Criminals. *Business Forms, Labels & Systems*, June 20, 44, 6, 46-49.

Hazelhurst Jeremy and Higgins Joanna (2004) Clear and present danger. *Director*, October 2004, 58, 3, 78-83.

Herbig, Katherine L. & Wiskoff, Martin F. (2002) *Espionage Against the United States by American Citizens 1947-2001*. PERSEREC Technical Report 02-5, July 2002.

Herman Michael (1996) *Intelligence power in peace and war*. The Royal Institute of International Affairs. Fifth Edition. Cambridge: Cambridge University Press.

Huusko Jukka and Moisio Teppo (2008) Suomen valtio ja aseteollisuus joutuneet verkkovakoilun uhreiksi, *Helsingin Sanomat*, 11 June 2008, p. B 1.

Isaacs Richard (2003) Dirty Little Secrets, *Security*, December 2003, 40, 11, 39.

Jones Andrew (2008) Industrial espionage in a hi-tech world. *Computer fraud & security*, January 2008, 7-13.

Kajava Jorma (2003) *Henkilöturvallisuus osana organisaation tietoturvaa.* Oulun yliopisto, tietojenkäsittelytieteen laitos. Sovellukset ja hallinto, Sarja D 12, Oulu: Oulu University Press.

Kivinen Osmo and Varelius Jukka (2003) The Emerging Field of Biotechnology: The Case of Finland. *Science, Technology, & Human Values*, Volume 28, Number 1, 141-161.

Kramer Lisa A. & Heuer Jr., Richards J. (2007) America's Increased Vulnerability to Insider Espionage. *International Journal of Intelligence and CounterIntelligence*, 20:1.

Lanne Marinka and Kupi Eija (2007) *Miten hahmottaa security alaa? Teoreettinen malli Suomen security-liiketoiminta-alueista.* VTT Tiedotteita - Research Notes 2388. VTT Technical Research Centre of Finland. [www] Available from http://www.vtt.fi/publications/index.jsp [Accessed on 4 April 2008]

Lanne Marinka (2007) *Yhteistyö yritysturvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa.* VTT publications 632. Helsinki: Edita Prima Oy.

Leinbach Thomas R. and Brunn Stanley D. (2002) National Innovation Systems, Firm Strategy, and Enabling Mobile Communications: The Case of Nokia. *Tijdschrift voor Economische en Sociale Geografie*, Volume 93, Number 5, 489-508.

Luong Minh (2003) Espionage: A real threat. *Optimize*, October 2003, 61-72.

May Ernest R. (1992) Intelligence: Backing into the future. *Foreign Affairs*, Summer 1992, Volume 71, Issue 3.

McCourt Mark (2008) Keeping Up with New Threats. *Security*, March 2008, 45, 3, 16-18.

Nodoushani Omid and Nodoushani Patricia A. (2002) Industrial Espionage: The Dark Side of the "Digital Age". *Competitiveness Review*, Volume 12, Number 2, 2002, 96-101.

Porteous Samuel (1993) *Economic Espionage*. Canadian Security Intelligence Service, Commentary Number 32.

Porteous Samuel (1994) *Economic Espionage (II)*. Canadian Security Intelligence Service, Commentary Number 46.

Ramcharan Robin (2005) Intellectual Property and Security: A Preliminary Exploration. *Contemporary Security Policy*, 26, 1, 126-159.

Repo Walter (2004) Spionen från Rotebro, *Shortcut Magasin*, #2 April 2004, 36-45.

Rothke Ben (2001) Corporate Espionage and What Can Be Done to Prevent It. *Information Systems Security*, November/December.

Rust James William (2006) *Corporate Management of Computer Forensics Evidence.* Information security curriculum development. Proceedings of the 3rd annual conference on Information security curriculum development. Kennesaw, Georgia, 175-178.

Räikkönen Timo and Rouhiainen Veikko (2003) *Riskienhallinnan muutosvoimat. Kirjallisuuskatsaus.* VTT Tiedotteita - Research Notes 2208, VTT Technical Research Centre of Finland, Espoo: Otamedia Oy.

Samli A. Coskun and Jacobs Laurence (2003) Counteracting Global Industrial Espionage: A Damage Control Strategy. *Business and Society Review,* 108:1, 95-113.

Tarrant Deborah (2007) A breach of trust. *Intheblack*, October 2007, Volume 77, Issue 9, 32-35.

Turner Stansfield (1991) Intelligence for a New World Order. *Foreign Affairs*, Fall 1991, Volume 70, Issue 4.

Whitey Merril E. and Gaisford James D. (1996) Economic Espionage as Strategic Trade Policy. *The Canadian Journal of Economics / Revue canadienne d'Economique*, Volume 29, Special Issue: Part 2. April. 1996, 627-632.

Wright Phillip C. and Roy Géraldine (1999) Industrial espionage and competitive intelligence: one you do; one you do not. *Journal of Workplace Learning*, Volume 11, Number 2, 1999, 53–59.

Internet

The Confederation of Finnish Industries, Elinkeinoelämän Valtuuskunta, EK [www] Available from http://www.ek.fi/ytnk/tiedotteet/yritysturvallisuuden_perusteet.php [Accessed 4 April 2008]

Ericsson [www] Available from http://www.ericsson.com/ericsson/corpinfo/index.shtml [Accessed on 4 April 2008]

The Finnish Security Police, Suojelupoliisi [www] Available from http:www.poliisi.fi/supo [Accessed 4 April 2008]

HighTech Finland [www] Available from http://www.hightechfinland.fi/ [Accessed 4 April 2008]

Nokia [www] Available from http://www.nokia.com [Accessed on 4 April 2008]

The Swedish Security Service, Säkerhetspolisen [www] Available from http://www.sapo.se [Accessed 4 April 2008]

Teknologiateollisuus ry [www] Available from http://www.techind.fi/ [Accessed 4 April 2008]

Poliisiammattikorkeakoulun tutkimuksia ISSN 1455-8262

Matti Vuorensyrjä: Tulos- ja kehityskeskustelujen arviointi ja kehittäminen poliisihallinnossa. 37/2009. 17,00 €.

Petri Rainiala: Tiedottajan käyttö poliisin tiedonhankintamenetelmänä. 36/2009. 20,00 €.

Erkki Hämäläinen: Eurooppalaistuva lainvalvonta. Euroopan unionin järjestäytyneen rikollisuuden torjuntapolitiikan toteutuminen Suomessa. 35/2009. 23,00 €

Anna-Liisa Heusala, Anja Lohiniva ja Antti Malmi Ha odnoi storone - po obe storoni granitsi. Sotrutnitsestvo organov vlasti Finljandii i Rossii s tselju ulutshenija pogranitsnoi bezopasnosti. 34/2009. 43,00 €.

Terhi Hakamo, Kirsi Jauhiainen, Anne Alvesalo ja Erja Virta: Talousrikokset rikosprosessissa. 33/2009. 33,00 €

Outi Roivainen ja Elina Ruuskanen: Laki ja järjestys? Poliisien ja kaupunkilaisten näkemyksiä järjestyslaista sekä yleisen järjestyksen ja turvallisuuden valvonnasta. 32/2008. 38,00 €

Anna Vanhala: Piiri pieni pyörii**.** Poliisipäälliköiden ammatti-identiteetti ja työelämäkerrat. 31/2007. 29,00 €

Anna-Liisa Heusala, Anja Lohiniva ja Antti Malmi: Samalla puolella - eri puolilla rajaa. Rajaturvallisuuden edistäminen Suomen ja Venäjän viranomaisyhteistyönä. 30/2008. 43,00 €

Kari Saari: Poliisi ja joukkojenhallintatoiminta Suomessa. Joukkotilanteet ja niihin liittyvä poliisitoiminta suomalaisten poliisien näkökulmasta tarkasteltuna. 29/2007. 32,00 €

Marko Viitanen: Poliisin rikokset. Tutkimus suomalaisen poliisirikoksen kuvasta. 28/2007. 65,00 €

Poliisiammattikorkeakoulun oppikirjat ISSN 1455-8270

Kimmo K. Kiiski: Poliisin rooli kuolemansyyntutkinnassa. 2. uudistettu painos. 18/2009. 20,00€

Johan Boucht ja Dan Frände: Suomen rikosoikeus. Rikosoikeuden yleisten oppien perusteet. Suomentanut Markus Wahlberg. 17/2008. 20,00 €

Reima Kukkonen: Keinotekoisista varallisuusjärjestelyistä ulosotossa ja velallisen rikoksissa 16/2007. 27,00€

Risto Honkonen & Nora Senvall: Poliisin johtamista kehittämässä. 15/2007. 39,00 €

Arto Hankilanoja: Työturvallisuus ja vastuun kohdentuminen poliisihallinnossa. 10/2003. 2., Uudistettu painos 2007. 16,00 €

Janne Häyrynen ja Tero Kurenmaa: Arvopaperimarkkinarikokset. 14/2006. 25,00 €

Anne Alvesalo & Ari-Matti Nuutila: Rangaistava työn turvattomuus. 13/2006. 21,00 €

Anne Jokinen: Rikos jää tekijän mieleen. Muistijälkitesti rikostutkintamenetelmänä. 12/2005. 20,00 €

Nina Pelkonen: Kriisin ABC. Käsikirja poliisin käyttöön. 11/2005. 10,80 €

Poliisiammattikorkeakoulun raportteja ISSN 1797-5743,

Laura Peutere: Poliisin tietoon tullut viharikollisuus Suomessa 2008. 85/2009. 19,00 €.

Jenni Juslén ja Vesa Muttilainen: Korruption ydinalueet 2000-luvun Suomessa. 84/2009. 18,00 €.

Johanna Peurala: The European Union's Anti-money Laundering Crusade. 83/2009. 10,00 €.

Sanna-Mari Humppi: Lapsen seksuaalinen hyväksikäyttö rikosilmoituksissa. 82/2009. 12,00 €.

Anja Lohiniva ja Vesa Muttilainen: Vakuutusala petosten kohteena. 81/2009. 8,00 €

Tuula Kekki: Taparikollisuus, huumeet ja rikoskierre. 80/2009. 12,00 €

Jussi Leppälä: Tulliselvitysrikos. Lainsäädäntöehdotuksen arviointia. 79/2009. 12,00 €.

Kari Laitinen ja Milla Lumio: Terroristin synty ja terrorismin torjunta - Näkökulmia väkivaltaiseen radikalisoitumiseen. 78/2009. 16,00 €.

Vesa Huotari: Seksuaalinen häirintä poliisin perustutkintokoulutuksen aikana. 77/2009. Verkkojulkaisu.

Tuula Kekki: Huumeet ja rikostorjunta - Poliisien käsitykset huumerikollisuuden ja poliisitoiminnan muutoksista. 76/2009. 11,00 €.

Verkkojulkaisut ovat luettavissa osoitteessa www.polamk.fi