Journal of Intelligence Studies in Business

Journal of Intelligence Studies in Business

Publication details, including instructions for authors and subscription information: https://ojs.hh.se/index.php/JISIB/index

Economic and industrial espionage at the start of the 21st century – Status quaestionis

Klaus Solberg Søilen[a]

[a]Department of Engineering, Natural Sciences and Economics, Faculty of Marketing, Halmstad University, Halmstad, Sweden; klasol@hh.se

To cite this article: Søilen, K.S. (2016) Economic and industrial espionage at the start of the 21st century – Status quaestionis. *Journal of Intelligence Studies in Business*. 6 (3) 51-64.

Article URL: https://ojs.hh.se/index.php/JISIB/article/view/179

Journal of Intelligence Studies in Business
Vol. 6, No. 3 (2016) pp. 51-64
Open Access: Freely available at: https://ojs.hh.se/

Economic and industrial espionage at the start of the 21st century – Status quaestionis

Klaus Solberg Søilen[a]

[a]*Department of Engineering, Natural Sciences and Economics, Faculty of Marketing, Halmstad University, Halmstad, Sweden*

**Corresponding author: klasol@hh.se*

Received 2 October 2016; accepted 15 December 2016

ABSTRACT This article is a literature review where the aim is to define a *status quaestionis* for the field of economic and industrial espionage. History shows how those who engage in these activities often are the scientifically and industrially weaker party, the party that is learning or trying to catch up. On a global scale economic and industrial espionage can be seen as a form of *involuntarily sharing* that has a series of positive results for economic development. On the scale of the individual businesses attacked, and for tax authorities in those countries, it is a troublesome phenomenon that must be regulated and punished. Governments must prepare society for systematic and frequent cyberattacks. Private companies are wise to move to stricter security controls, which must include encryption. A number of specific research projects are suggested throughout the article. In the literature we have identified the following agent motives: the employee who *needs money, has split loyalties, leaves angry, the occasional thieve and the professional spy.*

KEYWORDS Economic espionage, hacking, industrial espionage, literature review, signal intelligence

1. INTRODUCTION

About ten years ago - in 2005 - I defended a doctoral thesis on industrial espionage in Germany (Solberg Søilen, 2005). Now the question arises: what has changed in this field over the past decade? A quick look shows that the capabilities and practices have seen a degree of change that is nothing short of a revolution. In the late 1990s, when I did most of the literature research, government institutions were lagging far behind in technology. Private companies were dominating the field with customer relation management (CRM), business intelligence (BI) and what was to become data mining (DM). The important technical contributions all came from different private actors, but it was made possible by massive government funding. It is a myth that the internet was created within the military. Espionage companies were suddenly doing what only states had done previously. After the Cold War thousands of spies had been dismissed and were seeking jobs in the private sector, a reason why there is still a concentration of corporate espionage consultancy around Langley, Virginia, USA. This was a period of private intelligence gathering. Many of the ideas about gathering large amounts of data on users grew out of the marketing field and were related to customer loyalty programs, bonus cards and in-depth customer segmentation.

My dissertation was about industrial espionage in trade negotiations. Negotiations are still a primary target for agents but the field has been vastly expanded. Just like then, companies today are still poor at detecting and stopping attacks, preferring to simply fire the alleged culprit hoping to avoid negative

publicity (Schultz, 2001, p. 202). There is always a fear that admission of breach may lead to loss of confidence and lower share price. So the stories seldom become public, if they are not leaked by state intelligence organizations or spread as anecdotes by retired executives at cocktail parties.

Spying on allies for economic gains has been normal practice within Europe for many years, especially ahead of major European summits (Corera, 2016, p. 361). German intelligence can detect increased activities before commercial negotiation with the Chinese. Most of the attacks are traced back to the same cities: Beijing, Shanghai and Guangzhou (Corera, 2016 p. 242). At other times, hacking attempts have come from Hainan, which is the headquarters of signals intelligence for the People's Liberation Army (PLA). Other attacks come from Chinese universities and may be just for practice. Western adversaries are engaged in many of the same practices.

For spies, the use of the computer is far safer and less risky than snooping around in person. When we copy from a personal computer instead of stealing a briefcase we do not leave a trace if we are good, so it's an attractive form of espionage. It's also difficult to separate good from bad guys on the internet, which makes the place a natural environment for deception schemes.

Our computers are faced with possible hacking (mainly fishing) attacks every day. This has become normal. Computers are simply not safe. Even though safe email services exist, like Phil Zimmermann's PrettyGoodPrivacy (PGP), created in 1991, which caused no end of panic in the US government and the US Naval Research Laboratory's TOR, companies are slow to adopt it, maybe because they find it difficult to use or are afraid that the messages cannot be opened by the receiver or will arrive much later (Schultz, 2001, p. 206).

Before we look to the literature and the discussion it's necessary to give some background to the field of economic and industrial espionage to describe current capabilities.

1.1 Definitions capabilities for economic and industrial espionage

Economic espionage (also *government espionage*) is a government's efforts to collect information, appropriate trade secrets, and steal knowledge (Nasheri, 2005). *Industrial espionage* is the same, but without direct government involvement. *Information warfare* (also *cyberwar*) on the internet, as conducted by the military, is a version of economic espionage where the primary aim is first of all to destroy vital infrastructure in another country, not to steal company secrets or help companies become more competitive.

Private companies gather their data either from the traces we make when we engage on their sites or by active searches on the internet, such as when we look up a name on a site. Governments gather their data by controlling the entry points where the internet is brought into a country, by setting up black boxes inside of telecom companies and by tapping data directly from the databases of private companies like Microsoft or Facebook by forcing them to build side doors (in the US this is controlled by the 2008 Foreign Intelligence Surveillance Act). FISA says the government has the right to collect any data that comes through your software program and that you are obliged to facilitate this gathering. They also get data through a system of information exchange with other countries. Private telecom, internet and software companies cooperate with their national intelligence organizations because they know they have to in the end, or because the government is a major customer or out of some feeling of patriotism. The public at large is unaware of these deals and forms of cooperation.

In the end, the internet is a physical infrastructure consisting of cables and routers. More than 90% of the world's data pass through fiber-optic cables (Corera, p. 306) and the US (most of the rest pass via other UKUSA member states). Foreign powers can now break into anything that is connected to the internet. With the help of traditional agents (carrying malware on a USB stick) they can also break into closed systems. Of concern to private organizations is that this knowledge is just as easily available to their competitors.

An important strategic advantage is related to who can supply the cables and internet infrastructure. Today there are only two companies that are suppliers of complete telecoms networks in the world: Huawei and Ericsson. The US has made a point of not letting Huawei in to the US due to allegations that it's a spying tool for the Chinese government. The only evidence so far is that the NSA has spied on Huawei since at least 2007 (Corera, 2016, p. 373). Huawei may soon

be the only major supplier that can set up and run a telecoms network from scratch if Ericsson is outcompeted, as is indicated by recent sales figures and economic results. We do not know what Huawei will be like in the future, once it has established its role as the dominant supplier.

All this raises a number of questions as to how companies can protect their secret information. The aim of this paper is to try to define a number of these questions for future research based on a literature review of scientific papers and books published during the past ten years (the research gap) followed by a lengthy discussion on some key issues.

2. METHOD

How does one perform research into economic and industrial espionage? Is it even possible? Most sources are based on interviews with employees of western intelligence services and will naturally be skewed in that direction, for example showing how they never engage in economic espionage themselves but try to stop it when it comes from other, unfriendly nations. The us-and-them rhetoric is strong in these sources (mainly books). All services systematically exaggerate the dangers coming from other countries to obtain larger budgets and employ more staff. The assumption here is that one party is predominantly good. Compared with current as well as historical events of aggression between states since the Second World War it's difficult to make this claim stick. Thus, this method can at best be seen as telling one side of the story. The companies themselves do everything in their power not to tell stories about when they are hacked or cheated as it is considered negative publicity.

When authors or researchers do get access to information about industrial espionage inside of companies they have typically had to sign hefty confidentiality agreements. Thus the names of real companies and people are hidden and the stories are one-sided.

One solution to these biases is to set up laboratory experiments where the subjects do not know what is being measured (contrived study setting). Laboratory experiments can be set up as a role play with case studies indicating different roles. The easiest way of running such experiments is with graduate students, but they are not representative of the population we are trying to measure. To strengthen the reliability of the findings such studies can be supported by running the games inside of real companies. A further layer of extending redundancies in method can be done by comparing these results with interviews of executives (Solberg Søilen, 2005). Using the laboratory experiment, a multiple cross-sectional study with constructs measured at multiple points in time and the use of different samples may be imagined. The method is far from perfect when it comes to eliminating biases but relatively good given the nature of the object studied.

When writing on a sensitive issue there is often a considerable delay in the empirical data presented: a story is often first leaked many years after an incident happened. Thus publications today typically reflect a reality that is no longer existent. The more technology that is involved in the problem statement the more prone the answers are to be outdated by the time of publication. In general, however, a number of research strategies are possible: experiments, survey research, observation and case studies.

For this paper a combination of literature review and discussion is chosen to try to define a *status quaestionis* for the field. The aim is to identify a series of new and interesting research problems. As such this paper may be seen as a first step in hypothetic-deductive research. The nature of the subject is more open for exploratory and descriptive research.

Web of Science renders 104 references on the topic of industrial espionage. Forty of these are articles, and, most (8) are written for the study of history. From these the author selected and read little more than two dozen articles based on their relevance for business studies. These and related topics are discussed and future studies defined.

3. LITERATURE REVIEW

Thorleuchter and Poel (2013) confirm that government and industrial espionage has become an increasing problem for governments and corporations. An article in the *Journal of Professional Engineering* (2007) describes how the international Bar Association has warned that businesses are more at risk than ever. This development has been facilitated by users having weak passwords for their systems, a problem identified more than fifteen years ago by Schultz, (2001) and still a major culprit. Thus there are several articles that confirm the existence, the degree and some of the causes of the problem. Other articles focus on solutions.

Lee (2015) attempts to show how criminal profiling can be used to prevent industrial

espionage. An empirical analysis from South Korea published by the National Intelligence Service (NIS) shows that leaks from big companies come from current employees and from ex-employees in 47.8% of the cases each. For small and medium sized companies the numbers are 5.1% and 71.8% respectively (p. 1693). This means that for small and medium sized companies the problem is basically ex-employees, but that in big companies there problem is evenly spread. It means that for small and medium sized companies the problem of leakages is so small that it may not require our attention. If this data is reliable and applicable to other countries the findings are of great interest.

Meyersson and Glitz (2016) are interviewed in HBR about a large empirical analysis done with data from the DDR during the period 1969-1989, which found that East Germany enjoyed significant economic returns from its government espionage. More interesting, the authors suggest that the DDR was so successful with industrial espionage that it may have crowded out standard forms of R&D (p. 30). For example the DDR was able to reverse engineer the IBM 360 in 1970 so that a company from Dresden was able to make 100 computers per year three years later (p. 31). The authors suggest that this strategy may lead to less R&D by a group's own efforts and therefore an industrial decline in the long run for nations faced with free competition. This raises a strategic question as to which countries, and maybe more interesting for business studies, which industries and companies, are to gain the most by espionage.

Economic and industrial espionage finds interest among a variety of schools of economics, and solutions are suggested using different scientific methods and approaches. For example Barrachina et al. (2014) make an elaborative attempt of a game theoretical approach to economic espionage that show in which case espionage can make the market more competitive.

Another highly analytical paper is presented by Ferdinand and Simm (2007). They analyze industrial and economic espionage as a form of learning. For example Chinese students come to the West to learn as much as possible. The work of Ferdinand and Simm (2007) builds on Greve (1998), Kraatz (1998), and Baum et al. (2000), who describe how organizations learn from their competitors. Following the work of Bapuji and Crossan (2004) Ferdinand and Simm (2007) analyze espionage as a form of external learning (EL) without collaboration, what they also call larcenous learning (LL). This may be a fruitful approach as it gives insights into the motives of much industrial espionage. It is also a constructive conceptual way to avoid the complicated moral discussions which tend to go nowhere (not that they are not important).

As argued by Polanyi (1967), stealing knowledge may in itself be insufficient if we do not have the ability to apply it. Attempts of theft are therefore often followed by attempts to hire key personnel and make other prearrangements. Sometimes in history this has even come to include kidnapping (DeCamp, 1974, Cipolla, 1993). From a strategic perspective this means that espionage should not be seen as an isolated phenomenon, but as a plan for R&D that includes other elements in conjuncture. The question is what elements do you need in addition to the secret information? According to Cotte (2005) technological eve is a precondition for innovation and therefore also for efficient espionage, the importance of which the author considers to be exaggerated, almost a quasi-mythical phenomenon.

According to a study by Sivanesan (2011) agents are normally recruited from science and technology academia. Today preparations for identifying and locating potential agents are normally done on the internet. As an example, LinkedIn is frequently used for this purpose. An initial contact and follow ups are often made on this and similar sites. In the old days recruiting agents used to be a risky and time consuming exercise (instructions though classified ads in a newspaper, etc.). Intelligence services are patient and can spend months cultivating a relationship before they find a way to persuade the agent to hand over valuable information, but this is also a more costly process. Often agents contacted in this way do not know that they have been recruited as spies, but think they are part of a normal market research or consultancy job outsourced to some entity. Again the internet shows itself as an arena for deception. Universities are an especially attractive target, as they, by definition, contain a concentration of knowledge workers with access to cutting edge research. A question that arises is which countries are pointed out as economic spies in the literature? Sivanesan (2011) claims they come from Russia, China, and more generally from the Middle East, Asia and North Africa. Another approach is to define who has the capabilities to perform economic and industrial

espionage and assume that these are being or will be used sometimes in future, for example under another head of state.

New political leadership can lead to increased economic and industrial espionage. But the internet can also help a new group of politicians get elected. A reoccurring topic today is whether false information and disinformation threatens the political model of democracy. Companies operating on the internet pay little attention to if information is true for false. Instead they tend to put all focus on internet traffic; that is how many users they have. False stories are spread just as quickly as and sometimes even quicker than true stories. For example Facebook has been criticized for facilitating spreading false information as news during the last political election in the US between Hillary Clinton and Donald Trump. Agents of false news use Twitter and other networks to create fake accounts that spread untruths or inject fraudulent chatter into the conversation. Dictatorships have been known to create fake videos and images and upload them to YouTube and other websites in the hope that news organizations and the public will find them and mistake them for real (Silverman, 2012). The companies themselves refer back to the freedom of press and argue that censorship is not something they can or will engage in.

At the same time never before in the history of journalism have more people and organizations been engaged in fact checking and verification. Never before has it been so easy to expose an error, check a fact, crowdsource and bring technology to bear in the service of verification. A politician or public figure who publicly asserts a falsehood is likely to be called out by fact-checking organizations such as FactCheck.org.

The problem is that rumors and falsehoods spread just as quickly, if not faster than, facts. In many cases they prove more compelling, more convincing, and more are more clickable. This development threatens democratic values and the electoral outcome of political elections, the argument goes. Research by Nyhan and Reifer (2015) suggests the internet may be ineffective at reducing public misperceptions about controversial issues. That is, once a false perception has rooted itself it is difficult to correct it. Thus the argument of legislation for more restricted use of the internet against such practices becomes important not only to guarantee a higher degree of truth in the information that is spread but also for political stability. China and other countries that were early to regulate the internet see this as a victory for their approach.

From the above a number of issues are identified and presented as a discussion in the next section where the aim is to present a series of theses based on arguments.

4. DISCUSSION

By looking at the different cases of economic and industrial espionage used as examples in the literature through history some patterns become clear. The first is that those who engage in economics of industrial espionage are often the scientifically and industrially weaker party, the party that is learning or trying to catch up.

At the turn of the 19th century the USA was the student. In 1811 an American by the name of Francis Cabot Lowell almost singlehandedly stole the knowledge of how to build a textile industry from Britain (Mendell, 2003). England a few generations earlier wanted to learn how to make their own tea instead of buying it from China. In 1789 Robert Fortune smuggled thousands of tea plants and seeds to Darjeeling in British imperial India. Also the French stole secrets from China. The process of making true porcelain was also stolen from the Chinese and introduced in Europe by Père Francois Xavier d'Entrecolles (Bergier, 1975). The Jesuit travelled to China in 1698 and the theft can be seen in letters dated 1712 and 1722 (Bergier, 1977). For early self-educated industrialists travelling was the standard way of learning. Actually, learning by travelling has been a well-used method for acquiring a competitive advantage throughout history (Solberg Søilen, 2016). A classic is Charlers Dupin's six volume "voyages dans la Grande-Bretagne (1821-22). In the late 1960s and early 1970s when the Japanese were trying to gain a competitive advantage, a government sponsored system of industrial espionage was set up through The Japanese External Trade Organization (JETRO) partially funded by the government. JETRO train people to look for new technologies (Fialka, 1997). Japan is one of the few well documented cases of a country that was systematically spied upon by the US, especially before and during trade negotiations (Solberg Søilen, 2005). American disrespect for the privacy of Japanese citizens and companies makes an interesting case as both the US and Japan are dependent on good relations in Asia to counter Chinese dominance in the region. It may be because the US considers Japan to be

the weaker part and that they are entitled to treat Japan in this way due to atrocities committed by Japanese soldiers during the Second World War. Japan has few alternatives to American cooperation as they have not even apologized for the atrocities they committed in China during the same war.

Today it is not the Japanese as much as Chinese who fill the role of student in many industries in countries like England and the US. One of the well-known examples of Chinese espionage is Tenhong Lee from Taiwan (also called the glue man) who worked in an American company making glue-based products. He performed industrial espionage for a Taiwanese competitor (Ferdinand and Simm, 2007). One of the reasons the case is well know is that it went to court where we learned about the complex motives behind Lee's actions.

Thus we have come full circle when it comes to industrial espionage within a few centuries and there is nothing to suggest that these alternating roles of who stand to profit from spying and who stand to lose will remain static. Instead we may assume that this will continue to change with the alternations in the competitive advantage of nations, unless a better set of international laws and agreements can be established.

4.1 The moral dimension and regulations

Are economic and industrial espionage theft? Or, is it simply learning, as some of the literature suggests? Larcenous learning (LL) is adapted in organizations and countries in early stages of development. It's a rational strategy as it is faster than developing your own R&D capabilities, and it's also cheaper. Can economic and industrial espionage be justified when one considers that many of those companies holding secrets are monopolies and that the spread of industries to new countries helps fight poverty and prepares the way for a large middle class in those countries? Throughout history it can be shown how industrial espionage has helped fight poverty. China is only the latest example, bringing 500 million people from the poor classes to the middle class. How much is due to economic and industrial espionage is difficult to say, but we can assume that it has had a positive effect. Learning countries often start by making cheap copies of established brands and products. As their sales increase they are able to improve the quality of their products which again raises the possibility of charging a higher price. This is the way for Japan, China and all of the four Asian Tigers. In addition we have seen that research also suggests that certain forms of espionage can make the market more effective. When the information system (IS) quality is the private information of the entrant, the incumbent is better off with an IS of high expected precision while the entrant benefits from one of high quality (Barrachina et al., 2014, p. 127). There are several arguments for why economic espionage is improving both markets and societies. We suggest here that economic and industrial espionage can be seen as a form of *involuntarily sharing,* which can be good on the macro scale but is devastating on the micro scale. For the individual company and the country where that company is taxed, economic and industrial espionage is an economic loss. It is a crime and it is an intrusion on individual life.

All nations try to protect their own secrets by making laws that protect them, laws that are difficult to enforce outside of their own sovereign territory. There are no written rules in espionage between countries and foreign services, at best an understanding and form of balance. For some offenses there is a logic of guaranteed retaliation, a bit à la Mutual Assured Destruction (MAD) to use a parallel from the Cold War. We see this in examples of cyberwarfare. Moral and legal questions should be discussed further within the framework of moral philosophy and the study of international law. It is a dangerous moment for man when we accept the premises that stealing and treason are just the way of the world. It may be a part of human nature, it most certainly is a part of our history and as shown here it can have positive effects on the macro level, but agreements about conduct are necessary and countries can show political will by standing behind international laws and agreements.

If we are to catch agents we must know what motivates them. The "glue man" was motivated by ego and power not money, and he also suffered from divided loyalties, as he wanted to help both companies. To assume that agents simply look for the money then is an oversimplified view of reality which can make us look in the wrong directions. If companies can better understand the agents' motives they can also more easily stop them, or persuade

them to act differently. Risk profiles can be identified in any company. Even the term agent needs to be broken down into subcategories as it has been suggested that most industrial espionage is carried through by employees already employed or leaving a company (in large companies). They may or may not be working with a foreign state or a competitor. Many employees simply take information because it is easy and they know it is valuable, but without knowing what they will do with it. Others, like Mr. Martin who worked for Booz Allen Hamilton, major contractor to the NSA, knew what to do with it before he was caught, but had not made the contact with competitors yet. It was the opportunity, or the occasion, that made him a thief. Thus we can speak about the following motives in economic and industrial espionage: the employee who *needs money*, has *split loyalties*, *leaves angry*, the *occasional thieve* and the *professional spy*. For cases of economic espionage where foreign states are involved in hacking the situation is different and clearer. Most spies here have a monthly salary. They are employed by the state to spy and are simply doing their job. Others are contractors or sub-suppliers. We must assume that fewer spies are motivated by political conviction today as the political divide (ideologies) between countries play a less significant role, but this may of course change.

A general problem in the literature, as briefly discussed in the methods, is the one-sidedness of the perspectives presented, especially when it comes to dealing out blame. When a book on industrial espionage is written in the UK today, then everyone else is considered to be the bad guys, for example the Chinese and Russians. The people interviewed in these books (and more worryingly, the author) want us to believe that the world's largest surveillance systems developed in the Western world are never used aggressively, but put in place only to defend our information and freedom. The same sources that are interviewed have no reservations about lying to elected politician in our national assemblies, and not only in the US. Leakages by Edward Snowden and others have confirmed suspicion. For example, the heads of American intelligence have all been caught lying before the Senate about spying on Americans. Obama lied when he said that PRISM was only used to spy on foreigners (or he too was seriously misled, which is not less worrying). PRISM showed that state organizations have a side door to the software we buy and how private data that is gathered about us on the internet is used. Snowden showed that the US is a major aggressor.

After these leakages much of the trust between state and citizens was broken, to say nothing about the trust between the American state and other nationals. After a series of unjustified wars in the Middle East, America is now close to moral bankruptcy in the sphere of international politics, discredited from outside and more worryingly from within. That is not a good thing for world stability.

A major problem with much of the existing literature on economic espionage is not only the one-sidedness but also the obvious extent of "moralism", blatant and uncritical condemnation of what other countries are doing. For example it is said that only China and Russia are engaged in economic espionage, how it was China who pioneered the use of computer espionage to target Western companies for economic gain or we are given excuses such as that the difference between intelligence and information is less clearly defined in China. Another approach is to recognize that all major services are engaged in economic and industrial espionage, but that some are more active than others. We may assume that countries that have the most to gain by economic espionage are more active and that those espionage capabilities that are being built will be used. There is no evidence that suggests otherwise.

Stories of moral superiority are spread to strengthen the conviction that one side has the moral high ground. Once citizens are convinced that their own state has that high ground they can do all sort of things and get away with it, like engaging in economic espionage or starting wars. The intelligence apparatus is part of this logic that spread stories of us-and-them, also for their own advantage to get larger intelligence budgets.

Experience so far has shown that good books on economic and industrial espionage are based more on leaked sources than on interviews with people under oath who have signed secrecy papers. We should always listen to the executive or politician who has nothing to lose, who has been fired or suffered from injustice. In the quest for objective information Open Source will continue to play an important role here.

Technology is both an opportunity for better information and a threat to the same development as we have seen. Going from

surveilling our computers to mobile phones is a great leap for intelligence organizations and private organizations alike. We can now follow people (targets/customers) in real time. For example with the help of beacons we can see when a customer is in the store and what he looks at. This information can later be used to send highly targeted advertising. The same technology can be used to gather information about terrorists' whereabouts.

For intelligence organizations planting bugs in homes was always risky. Now we carry those bugs around with us all of the time and our microphones and video cameras can be tuned on and operated remotely by others. As a species we have taken a major step into *the total surveillance state,* so it is surprising that more citizens are not reacting. The reason for why more are not reacting should be studied by psychologists.

The increase in false information is a product of this new technology. As we have seen it now spreads rapidly on the internet and is difficult to correct. Voters are willing to disregard more serious and objective news sites when they make up their mind about whom to vote for and why. At the same time it has never been easier to find good and reliable information. The problem is that correct information takes so much training and demand that we are more critical as readers. This has put a new layer of responsibility on our learning institutions which they have not been able to handle so far. If we as societies do not develop a more critical ability towards what is published on the internet then manipulators will get the upper hand. We have been there before in history, when demagogues ruled and it never ended well. That in itself is a reason to regulate publications on the internet. How this is different from censorship is a challenge for scholars to show before policies are decided and implemented. The principle of freedom of press works only as long as there is someone responsible and is therefore a poor parallel for the world of the internet. It seems clear that a solution will have to include more legislation, policing and enforcement.

Our companies are just as vulnerable as the general public to misinformation and internet attacks. They don't normally know when they are being attacked, when a part of their own network traffic is due to intrusions. Foreign states continuously look for intelligence in connection with companies' mergers and acquisitions activity, joint venture intentions, and strategies. Companies surveille each other or their customers like when auction houses look for signs that art collectors are getting older and may be willing to sell. Criminals try different scams to get access to credit cards and other valuables. In the end they are only protected by the expertise they have developed within their own organization.

4.2 Cyberwars and challenges faced by government institutions for signal intelligence

In 2014 Sony Corporation was attacked to the point where servers and computers were all cleaned of data. The company had to pay its employees in paper checks and there was no contingency plan. In this case the company got some help, at least afterwards. A few months later the NSA shut down the entire internet and mobile phone data in North Korea for a short time as a direct retaliation. Cyberwar is a threat that can strike any private organization, not only suppliers of infrastructure, but any company that infuriates another country or its rulers. Moreover the companies attacked do not know if they are been harmed because of something they have done or something they could have done as many attacks are mere exercises. These exercises can be initiated by a foreign country's intelligence apparatus, but may also come from universities, even from within their own country.

Economic and industrial espionage over the internet (preventing it, and even carrying it out) is the business of signals intelligence (SINGINT). In the US this means the National Security Agency (NSA), in England the GCHQ and in Sweden the FRA.

Information warfare has become very real. The Cyberarmy is to the 21st century what the air force was to the 20th century. It is now the fourth army group next to the army, navy, and air force. As a consequence militaries all over the world are building their own cyber-armies, some of them like Iran after having suffered from massive attacks by other countries (US, Israel and UK primarily).

The US, England and Israel showed that they can take control of a country's nuclear facilities even in a closed computer system not connected to the internet by getting an agent to put in a simple USB drive with an operation known as "Olympic Games", but better known after the name given to the malware: Styxnet.

What they did not foresee was that this triggered a massive response by Iran. Iran answered with two major attacks, one against Aramco and another against American banks. In 2012 Iran took down the computer network of the Saudi oil giant Aramco for 8 days. A few weeks after they showed they can take down customer services offered by the Bank of America (Corera, p. 280-1). This led to an American-Iranian deal of de-escalation that left Israel infuriated and the UK uncertain that they should have entered the cooperation in the first place, according to Corera's sources.

Cyberwar and cyber armies are a reality after Styxnet, and this and similar codes have since spread to many countries. A problem is that we do not know the extent of other countries' capabilities for cyber warfare as they have not been fully tested. In a worst case scenario countries and companies must assume that all they do online can be stolen and stopped if they do not have a vigorous security system in place, which also takes into account the possibility that an employee may be used as a vehicle, even involuntarily. Needless to say this degree of security is hardly found in any organization.

The problem with cyberattacks is that it's difficult to know who is attacking you, whether it's your own state, another state or another company.

Michael Hayden defined the types of attackers as states, criminals and a third groups consisting of "hactivists", "anarchists" and "nihilists" (Corera, p. 301).

During the last American presidential election we witnessed how Russian intelligence was able to influence the outcome of the election by hacking the email account of Clinton's campaign manager and leaking the information, bluntly exposing the Clinton campaign's strategies but also portraying the candidate and her staff as cynical and unconcerned about voters' interests. The real damage of these intrusions is still being evaluated. Their significance is still difficult to oversee aside from the obvious fact that they may have helped Donald Trump win the American presidential election. On one side there is nothing new with these intrusions. Both Russia and the US have been interfering in other countries' elections for more than a century, as other great powers have done before them. However, this may be the first time Russia has succeeded with such an operation in the US and the first time the US got a taste of some of its own medicine, after having meddled systematically in political election all over the world since the Second World War.

Hacking is all about getting access to source code, so the attacker can identify how a system is made and where the weaknesses or hacking opportunities are. Hindering spying is about checking the source code for backdoors, which can be used by foreign governments. For example Microsoft has to show at least some of the code for its products to be sold in China as China knows that Microsoft is obliged through American law to alter their software to allow for American spying.

These episodes are often portrayed as a conflict between states and private companies, like when Facebook's Mark Zuckerberg lashed out against the American president for PRISM. In reality many private technology companies live in a form of symbiosis with national intelligence organizations. They exchange employees/expertise and do business with each other. Both are also in much the same business, in the information industry, where the primary aim is the gathering and exploitation of data. They also cooperate.

In the first half of 2014 Google received 15,000 government request for user data from different countries. They complied in 65% of the cases (Corera, p. 380). Social media and Google are themselves in the spying business, selling private information to companies for advertising. The main difference is that it is done by consent (at least formally, but no one reads the fine print) and that customers can opt-out. Further research should aim to show the extent to which this cooperation is done.

For those citizens fearing a total surveillance state, it is sometimes argued that intelligence organization are selling security. The privacy debate exists but is not strong today. Instead states do what they can and lie about the rest. For example they claim that they are not surveilling their own citizens, but in reality they cannot separate this data from other foreign data. Instead all is collected. The NSA are wiretapping the whole world and we as world citizens are to believe that this is for our own best interest as America will protect us all. It is a hard sell today. The major reason why other nations and their elites comply is that the NSA is also sharing a part of this information, with other countries like Germany and France that do not have the same technological capabilities. The intelligence that is passed on by the NSA to other countries is sometimes invaluable for catching terrorists.

Sometimes the intelligence is passed on as part of intelligence swaps (getting access to data the other party does not have) and sometimes it is simply goodwill. Of course they only swap between friends. It would be of interest to know what other countries think about these issues and the extent to which new intelligence alliances are formed.

The NSA was the result of a need for a more centralized intelligence system after the disaster of Pearl Harbor and failings in the Korean War (Corera, 2016, p. 51). In the shadow of what President Eisenhower called the 'military-industrial complex', there emerged a spy-industrial complex centered in Washington, DC and northern California. By the early 1960s, over 50,000 Americans were involved in signals intelligence (Corera, p. 62-64). Today the US has a total dominance of the infrastructure of the internet. Bluffdale Ohio is the strategy to gather and save it all, every piece of digital trace a person leaves; not only surfing, but financial records, tickets, photos, chats, phone calls and GPS data.

The major security risk with this project is that it is done by non-military and private contractors. At the NSA less than 50% of staff today is military and much has been out sourced to a few big contractors of which Booz Allen Hamilton is the best known. It was the employer of Edward Snowden and more recently Harold Thomas Martin. Spy-hunting has been outsourced to private firms and private employees are receiving top security clearance:

"Booz Allen is one of five corporations that together employ nearly 80 percent of the private-sector employees contracted to work for US spy and surveillance agencies. Booz itself deploys an intelligence workforce of 12,000 personnel with security clearances, a figure I found is equivalent to nearly 27 percent of the 45,000 contractors employed in US civilian and military intelligence" (Shorrock, 2016).

Martin was recently arrested, suspected of taking the highly classified source code developed by the agency to break into computer systems of adversaries like Russia, China, Iran and North Korea.

We started the introduction of this paper by saying that governments were lagging far behind in technology. Today governments have built up their technological abilities, but these rely heavily on private contractors. This has given rise to a new problem and a new level of risk.

What is more worrying for businesses is that it is just as easy and natural and often more lucrative for the same NSA staff to take on assignments for a private company, and the risk is not exclusive to the US. The same competence is found among IT consultants in many countries around the world.

Companies will need to push for more security and encryption. In extreme cases it has meant going back to the typewriter and holding meetings while going for a walk in the park. For that which cannot be protected it means companies should not write it down, at least not on anything that is connected to the internet. This is a radically different world from the one I started to study only a decade ago when I wrote a dissertation on industrial espionage.

5. FUTURE STUDIES

It would be interesting to see if findings from the National Intelligence Service (NIS) referred to in Lee (2015) about who leaks (employees, former employees) and in what size companies (small, medium and large) are applicable to countries other than South Korea. If they are, spy catchers' attention at small and medium sized companies can be put mainly on ex-employees and mainly larger and multinational companies need focus on leakage among current employees.

Based on Meyersson and Glitz (2016) study of the DDR it would be of interest to define which countries and which industries and companies are better served by espionage economically.

Following from Polanyi (1967) we want to know what else an organization needs to acquire to become competitive besides the secret information and hiring key personnel who know how to use it. There is capital and the material component as in the case of the Iranian nuclear project, but other ingredients may have been overlooked that are essential for making use of the secret information that the organization has come across. In other words, it seems too narrow to only focus on the information itself when we want to understand the process by which secret information is turned into a competitive advantage. One suggestion is made by Cotte (2005), namely technological eve. How is technological eve performed effectively? What besides reengineering, buying the products of competitors and picking them apart to find out how each part is made and how it brings value to the end-product, are essential for this

operation? In the French literature there has been a keen focus on eve more in general ("*veille*") during the past decade. In Sweden universities still give courses in "*omvärldsanalys*", meaning "surrounding world analysis".

Building on the research of Sivanesan (2011) we want to know more about how spies are recruited from universities, but also what motivates them. How much of the information passed on is open source and published material? Academics on the cutting edge of a technical or natural science field can sometimes refrain from publishing to avoid coping and in order to prepare for patents.

Studies should continue from the research of Ferdinand and Simm (2007) that use external learning (EL) without collaboration, or larcenous learning (LL) to describe this process. It may be different in different cultures and the perception of LL may also be different. The difference between LL and EL, like attending a foreign university, may then be one of time: LL is fast while EL is slow. From a strategic perspective this raises the question of what mix is optimal for the competitive advantage of a rising nation, or any nation.

There is a need to gather data through interviews from non-Western intelligence organizations, like the Russians and Chinese, to balance and check the numerous stories coming from the Western world.

There is also a need to create case studies with individual stories of economic espionage. A number of these stories already exists in other forms and need to be extended. The great challenge in a case with two counterparts, two companies or countries, is to get the story from both sides.

From the discussion and syntheses it would be good if a historian could gather the examples we have of economic and industrial espionage through history and present them as unsentimentally as possible. A similar project for a broad discussion based in moral philosophy and international law does not exist either from what I can see. The consequences of cyberwarfare for companies are not sufficiently described and understood. More generally, the danger that the intelligence services can be used more intensively for economic espionage is real and should be addressed. How can companies protect themselves in this reality? How are state intelligence services going to solve the situation they have gotten into with the hiring of private contractors who leak information about us and how are internet companies going to convince customers that they are the good guys when they very much are locked into a symbiosis with the services, forced by law and otherwise persuaded to cooperate? Will we see new (national) systems of internet and will this make business less global and less efficient?

6. CONCLUDING REMARKS

Much has changed since I defended my doctoral thesis in industrial espionage at the University of Leipzig some ten years ago. We have moved from break-ins à la Watergate to theft by hacking. This period has also seen the beginning of cyberespionage even though the notion of information warfare was well known before. The conclusions of the empirical work in my thesis has stood the test of time and since then been confirmed regularly: companies do not disclose when they have been attacked as that only makes things worse. Instead they take the break-ins as a *fait accompli* and move on, unless they are the dominant player in the industry and the intruder is a smaller player, then they may decide to punish. The dissertation introduces the theory of *Diversification of Moral Risk* (DMR) built on the principle agent problem and the notion of portfolio risk diversification, showing how companies hire agents to perform actions they deem immoral to reduce the risk and consequences of being caught. For example oil companies outsource bribery to other companies to facilitate the handling of loading oil in high risk harbors. Weapons manufacturers hire other companies who hire other companies for their sales activities. Observations of these phenomena have only increased with new technology due to increased opportunities, lower risk of being caught and smaller consequences when caught.

Spying and snooping has become an activity that engages everyone today, on all levels. State intelligence organizations and internet and technology companies work much in symbiosis. For example Facebook is an indispensable starting point also for intelligence organizations that look for suspects as they will typically cross index our friends list with our financial transactions and flight itineraries over the past years. The same goes for individuals. A major motive for anyone to turn on Facebook is voyeurism, which is a form of snooping on people we know or even don't know but whose information we can get access to. We install cameras to keep track of

our kids and place trackers on our spouse's car. It is all part of the same phenomenon.

There is a risk that western intelligence organizations will turn to economic espionage to help their major corporations gain a competitive advantage as the technology and the facilities are already put in place. It very much depends on the country and who is head of state. The strategy of those countries who can afford to build these systems will be to catch it all and store it all, all data, and forever. The US is the first country to achieve this, but they are not going to be the only one. With the new complex at Bluffdale the US can not only search in all metadata, but also go down in detail and search all data (Deep Packet Inspections). Metadata is simply the best way to start a search because otherwise you would get too much. It is not where the search stops. This system is already giving the US an information advantage today, but responses are to be expected. China for one is bound to follow.

The internet, the ultimate symbol of freedom and knowledge, has become the ultimate surveillance tool. We as citizens have accepted walking around with a mobile phone, which is the spy's dream tool. Can the internet be recreated in its former self or was it naïve to think that the state would let it be uncontrolled? For companies it will have to mean a more encrypted reality.

No company secrets that are written electronically are safe unless protected by severe encryption. Very few companies have so far moved to safe encryption. Competitive industries must move to system awareness where employers have full control of what is downloaded to employees' computers. From the perspective of business studies we want to know what this costs and how it can be done. We also want to know about employees' reactions. Besides this we have suggested several new studies in the form of research gaps as summarized under the headline future studies.

7. REFERENCES

Andrijcic, E. & Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk analysis*. Volume: 26, Issue: 4. Pages: 907-923.

Anonymous (2007). Lawyers warn of increased risk of industrial espionage. *Professional engineering*. Volume: 20, Issue: 12. Pages: 10.

Anonymous (2002). Industrial espionage attempt thwarted by sting operation. *Computers & security*. Volume: 21, Issue: 3. Pages: 202.

Bergier, J. (1975). *Secret armies: The growth of corporate and industrial espionage*. Indianapolis: Bobbs-Merrill.

Bachman, D. (2014) Chinese Industrial Espionage: Technology Acquisition and Military Modernization. *China quarterly*. Volume: 219, Pages: 874-875.

Barrachina, A., Tauman, Y.; Urbano, A. (2014). Entry and espionage with noisy signals. *Games and economic behavior* Volume: 83 Pages: 127-146

Baum, J. A. C., Li. S. X., Usher, J.M. (2000). Making the next move: how experiential and vicarious learning shape the locations of chains' acquisitions. *Administrative Science Quarterly*, 45(4), pp. 766-801.

Bapuji, H., Crossan, M. (2004). From questions to answers: reviewing organizational learning research. *Management Learning*, 35(4): 397-417.

Bergier, J. (1977). *Vieux comme l'homme: L'espionage industriel*. Historia (368), pp. 84-95.

Cotte. M. (2005). *De l'espionnage industriel à la veille technologique*. Belfort-Montbéliard: Presses Universaires de France Comté.

Cipolla, M. (1993). *Before the industrial revolution: European Society and Economy 1000-1700*. New York: Norton

Condon, R. (2007). We've been expecting you, Mr Bond. *Infosecurity*, 4 (7), pp. 26-27.

Corera, G. (2015). *Intercept – The secret history of computers and spies*. London: Weidenfeld & Nicolson.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons*, 48 (3), pp. 233-240.

De Camp, L. S. (1974). *The ancient engineers*. London: Ballantine.

Ferdinand, J. & Simm, D. (2007). Re-theorizing external learning - Insights from economic and industrial espionage. Conference: 1st Interntional Conference on Organizational Learning, Knowledge and Capabilities Location: Warwick Univ, Warwick, England.

Fialka, J. (1997). *War by other means: economic espionage in america*. New York, N.Y.: W. W. Norton.

Gaidelys, V., Valodkiene, G. (2011). The methods of selecting and assessing potential consumers

used of by competitive intelligence. *Engineering Economics*, 22 (2), pp. 196-202.

Gillispie, C. C. (2006). From industrial espionage to the old technology. *Technology and culture,* Volume: 47, Issue: 4. Pages:839-840.

Greve, H. (1998). Performance, aspirations, and risky organizational change. *Administrative Science Quarterly,* 43: pp. 58-86.

Hamon, V. (2015). Android botnets for multi-targeted attacks. *Journal in computer virology and hacking techniques*, Volume: 11, Issue: 4. Pages: 193-202.

Harrer, J., Wald, A. (2016). Levers of enterprise security control: a study on the use, measurement and value contribution. *Journal of Management Control*, 27 (1), pp. 7-32.

Heickero, R. (2015). Industrial Espionage and Theft of Information. Conference: 14th European Conference on Cyber Warfare and Security (ECCWS) Location: Univ Hertfordshire, Hatfield, England.

Hvistendahl, M. (2016). Industrial espionage 3d printers vulnerable to spying. *Science*, Volume: 352, Issue: 6282. Pages: 132-133.

Jameson, D.A. (2011). The rhetoric of industrial espionage: The case of Starwood V. Hilton. *Business Communication Quarterly*, 74 (3), pp. 289-297.

Jerrard, M. (2015). The G & K O'Connor lockout (1999) and its aftermath: A case study of a union avoidance campaign in the Australian meat processing industry. *Labour History*, 109 (1), pp. 131-148.

Kraatz, M. S. (1998). Learning by association? Interorganizational networks and adaptation to environmental change. *Academy of Management Journal*, 41(6), pp. 621-643.

Lee, C-M. (2015). Criminal profiling and industrial security. *Multimedia tools and applications*, 74, 5. 1689-1696.

Mendell, R. L. (2003). *The quiet threat: fighting industrial espionage in America.* Springfield, Ill.: Charles C. Thomas.

Mietzner, M., Schiereck, D., Schweizer, D. (2015). The role of sovereign wealth funds as activist or passive fund managers. *Journal of Asset Management*, 16 (5), pp. 303-315.

Nasheri, H. (2005). *Economic espionage and industrial spying*. Cambridge: Cambridge University Press.

Nickisch, C. (2016). Defend your research industrial espionage is more effective than r&d. *Harvard Business Review*, Volume: 91, Issue: 11. Pages: 30-31

Nyhan, B., & Reifler, J. (2015). The effect of fact-checking on elites: A field experiment on U.S. state legislators: the effect of fact-checking on elites. *American Journal of Political Science, 59*(3), pp. 628-640.

Polanyi, M. (1967). *The tacit dimension*. New York: Anchor Books.

Reisch, M. (2011). Industrial espionage Former Dow scientist admits to theft of trade secrets. *Chemical & engineering news,* Volume: 89, Issue: 39. Pages: 7-7

Reisman, A. (2006). A taxonomic view of illegal transfer of technologies: A case study. *Journal of Engineering and Technology Management - JET-M*, 23 (4), pp. 292-312.

Schofield, J. (2016). Chinese Industrial Espionage: Technology Acquisition and Military Modernisation. *Canadian journal of political science-revue canadienne de science politique*, Volume: 49, Issue: 1. Pages: 182-183

Schultz, E. (2001). Security views. *Journal of computers and security*, Vol. 21, Iss 1, pp. 201-211.

Shorrock, T. (2016). A New Spy Scandal Exposes the Corruption of Privatized Intelligence. *The Nation. October 14.* At https://www.thenation.com/article/a-new-spy-scandal-exposes-the-corruption-of-privatized-intelligence/

Silverman, C. (2012). A new age for truth. *Nieman Reports, 66*(2), 4.

Sinha, S. (2012). Understanding industrial espionage for greater technological and economic security. *IEEE Potentials*, 31 (3), art. no. 6193307, pp. 37-41.

Smith, A.D. (2007). Strategic aspects of electronic document encryption. *International Journal of Services and Standards,* 3 (2), pp. 203-221.

Solberg Søilen, K. (2016). A research agenda for intelligence studies in business. *Journal of Intelligence Studies in Business*, 6(1), pp. 21-36.

Solberg Søilen, K. (2005). *Wirtschaftsspionage in Verhandlungen aus informationsökonomischer und wirtschaftsethischer Perspektive - Eine interdisziplinäre Analyse*. Doctoral Thesis , 341 Pages. Full text at http://www.diva-portal.org/smash/get/diva2:534515/FULLTEXT01.pdf

Sivansan, G. (2011). The human factor in espionage. *Computer Fraud & Security*, 2011 (2), 15-16.

Stadler, W.A. (2012). The quiet threat: Fighting industrial espionage in America. *Security journal*, 25, 1, 90-93.

Thorleuchter, D. & Van den Poel, D. (2013). Protecting research and technology from espionage. *Expert systems with applications,* Volume: 40, Issue: 9. Pages: 3432-3440.

Vashisth, A., Kumar, A. (2013). Corporate espionage: The insider threat. *Business Information Review*, 30 (2), pp. 83-90.

West, N. (2015). Chinese industrial espionage: Technology Acquisition and Military Modernization. *Asian Security Studies*. *Pacific affairs,* Volume: 88, Issue: 1. Pages: 178-180.