Global Surveillance and Economic Espionage

Tim Wellhausen
Department of Computer Science
University of British Columbia

April 18, 1999

Contents

1 Introduction

After the Cold War ended, many people thought that the new epoch would also change the role of intelligence agencies and the need for espionage. This role has indeed changed, but in a different way than expected. The agencies are better funded than ever, and their focus had changed.

Many cases are known in which intelligence agencies and similar institutions have tried to keep parts of a population under surveillance. The purpose of some agencies is to get to know more about the whole population of its own country (as the Stasi did in Eastern Germany, for example), other agencies kept only suspicious people under surveillance (the American FBI may be an example for that).

Now that technology has improved significantly, it is possible to build bigger systems that are capable to keep an arbitrary number of people under surveillance. Echelon is the name of such a system, and I will try to provide a good overview how this system works.

The traditional duties of intelligence agencies like surveillance are still important, but the agencies had to redefine the reason for their own existence in a changed world.

Nowadays, economic and political security are closely related. Thus, to stabilize the political situation, it is important to improve the economic situation. As a result, economic espionage became part of the daily work of many agencies.

Because the area of surveillance and espionage is much bigger than anything I could cover within this paper, I decided to focus on two aspects: global surveillance and economic espionage. Although they are different, they are closely related. Surveillance is an important means to gain information used directly or indirectly for economic espionage.

Without computer scientists, it is not possible to build the systems needed, and the technologies used are at the cutting edge of research. This raises many issues in the area of ethics. I am aware of them, but it is not possible to cover these in this paper.

At first, I have to address several issues about the accuracy of the information given in this paper. Section two gives some background information for a better understanding of the main part of the paper. Section three explains methods and requirements for surveillance and espionage with focus on computer technologies. Section four covers issues about surveillance. In section five, I will write about economic espionage, and section six concludes my paper.

1.1 Accuracy of information

For this paper I only searched for information on the Internet. There, I already found enough references, web sites, articles, and papers, so that I did not attempt to use other media to gain more information.

Although I have always tried to double-check the information I found, I have to emphasize that some of the content of this paper may not be accurate! Both the cases of Crypto AG and the Echelon system are officially not only not commented on, but one is denied information on them. Therefore, I had to use second hand information. I found in both cases many references, but all of them refer to the same sources which I also found at first.

As I already wrote in my last paper about "Social Impact of Y2k", articles written in newspapers or any other medium need not be accurate. Even if the New York Times writes about Echelon, they have very much the same sources as I have. I got the impression that what I was able to find seemed to be credible and accurate, but that does not have to be true.

2 Background Information

To fully understand many issues described in the following sections I first want to give some historic background information. Furthermore, I give a brief overview of what is called "Information Warfare" and about the roles of intelligence.

2.1 Historic background

During the second world war, it was crucial for every engaged party to get to know as much information as possible about the opponent. Without going into detail, an important success for the Allies was to break the code of the German Enigma machines. Achieving this resulted in detailed information about the German forces and probably shortened the war.

It shows both how important it is to have proper protection against opponents trying to gain secret information and how important it is to try to obtain these secrets.

A secret agreement in 1943 between Britain and the United States lead to an alliance to exchange cryptographic systems and knowledge about German and Japanese ciphers. In 1947, this was supplemented by the UKUSA (United Kingdom - USA) Agreement which enclosed besides the USA and Britain Canada, Australia, and New Zealand. This agreement still exists today and is the foundation for the Echelon system I will describe in section 4.4 ([15], cited in [22]).

During the Cold War both the Western and Eastern countries engaged mainly in military espionage against the other side. With the existence of more modern technology the systems became more sophisticated. Most of the current systems were designed and implemented during that time.

2.2 Information warfare

Computer systems all over the world are linked and connected to each other. This shows on the one hand the achievements of modern technology. On the other hand, such connections and resultant dependencies create vulnerabilities that can be exploited if the systems and data are not adequately protected.

Unfortunately, awareness of these dangers is still not very common. Both governments and private companies have systems running that are at risk of being penetrated. Penetration tests, performed by the FBI on government systems, show that in many cases the attacks succeed, and most of them were not detected.

If those weak points are exploited intentionally by competitors (both political and economic competitors) this is called Information Warfare. In the article [4], Information Warfare is defined as "the technique of attacking critical infrastructures by electronically interfering with industry and government computers".

For the U.S. intelligence community, potential hackers range from national intelligence and military organizations, terrorists, and criminals to industrial competitors, hackers, and disloyal insiders. For that reason, the intelligence agencies try to prepare themselves for the next generation of war.

From a business point of view, Information Warfare has slightly different aspects. In [3], the author explains that "Information Warfare involves achieving and maintaining an information advantage over competitors or adversaries." The author states that Information Warfare constitutes of information collection, protection, denial, management, and transport. These elements define options, risks, and opportunities for an organization. The organization's strategy is defined by how it chooses to implement and prioritize these elements.

More information about Information Warfare and Info War can be found at [1]. This web site offers a huge collection of articles on this topic.

2.3 Intelligence

Intelligence agencies already exist for a long time. It has always been very important to gain as much information about adversaries as possible. In ancient China, for example, the best war was a war that didn't have to be fought because of the efforts done by the own intelligence agencies.

Nowadays, nations are no longer divided into two camps of allies and adversaries. For the work of intelligence agencies, this means that for economic espionage one's potential adversaries could well be one's military and political allies. This leads to situation in which different agencies have both to compete and cooperate at the same time. A nation's commercial interests and the military and political interests it shares with its allies may explain several conflicts.

3 Methods and Technologies

Although surveillance and espionage are two different things, they have in common that information has to be gathered that is not available otherwise.

In the case of intelligence agencies, many technologies have been developed during the Cold War, conceived for the defense and intelligence sectors. After the end of the Cold War these technologies have quickly spread to the law enforcement and private sectors.

At least some of these methods are not restricted to government organizations but could also be used by private organizations. In this section, I want to show which technologies are generally used.

3.1 Traditional methods

Surveillance and espionage are nothing new. A long time before the current technologies existed, there were already numerous methods to gain information more or less legally.

Perhaps the easiest way to get proprietary information has always been to steal it. As long as this information is stored on a medium that can be removed, it is not protected against somebody taking it.

Some people always exist that know information that is not stored anywhere or that is out of reach. In that case, it may be promising to black mail a person over using the service of a prostitute who may have been hired for that purpose. A variant of this involves an attractive woman or man who forms a close personal relationship with an employee with access to the desired secrets.

If this doesn't help, it might be possible to hire a competitor's employee who has valuable knowledge, or to bribe a supplier or employee.

Finally, if it is not possible to get the desired information from somebody who is part of the organization an agent can try in infiltrate this organization.

3.2 New methods

A legal method to obtain information about new technology are patent offices. A technology for which a patent has been issued is publicly available. Thus, it is relatively easy to make copies of patent documents. Although it is not legal to use such a technology without paying royalties, it is almost impossible to persecute the violator if it is a foreign company in, for example, an Asian country.

Interestingly, in the U.S., there is a Law called Freedom of Informations Act, which can also be abused. In [14], the author describes the case of a Japanese company, which was about to enter the space industry in 1986. To gather information in this area, this company filed many requests under this act to

get information from the NASA. In this case, in 1987 alone, the company filed about 1500 requests.

If these opportunities are not available, there are many ways to exploit modern technologies to obtain information. These range from eavesdropping by wiretapping, bugging offices or capturing cellular telephone conversations to penetrating computer networks.

3.2.1 Vulnerability of modern telecommunication systems

Many papers and books have already been written about security issues of modern telecommunication systems. Although the availability of networks is very important for every organization to stay in business, they are also their Achilles' heel.

Many security holes exist both in software and in hardware, from unprotected wires to high-end software with bugs. Although companies selling the systems are able to fix many security holes immediately, it may take a while until these fixes are applied everywhere. Meanwhile, these security holes leave a system wide open to penetrators.

If somebody really wants to break into a computer system it is almost always possible to some extent. Some organizations are not aware of these problems, others do not care for them, and yet others know about it but are not able to protect themselves adequately.

And even if private companies are able to protect themselves against single attacks of competing firms, they often don't have the technology or know-how to combat the type of advanced technologies governments can throw at them. In a Canadian Security Intelligence Service publication ([6]), a businessman is cited that they can handle the ordinary industrial spy, but in case of spy satellites and sophisticated strategic espionage, only governments are able to combat that.

3.2.2 Net tapping

The Internet is the most important network world-wide. Therefore, it is the most important target for all kind of attacks. The method of choice for protection of sensible data transmitted over public parts of the Internet is cryptography. So-called strong cryptography enables everybody to protect data in a way that nobody without access to the key is able to read the message.

For that reason, many countries restrict the access to this technology. In countries like France cryptography is prohibited in general, countries like the U.S. allow domestic companies and individuals to use strong cryptography but doesn't allow the export. Other countries have been quite liberal up to now, like Germany and other European countries, for example.

Unfortunately, even in these more liberal countries, the views are changing. The Wassenaar treaty is the first try to unify the North American and European

countries on the use of cryptography. Because of space constrains, I won't go into detail. For more information, see [40].

Another approach to control cryptography to remain able to tap world-wide communication is the American "clipper chip", which allows the government to decrypt encrypted documents easily ([6], see [41]).

To make it even easier to intercept all public communication, there are many efforts to make network operators change the infrastructure. A newspaper article [35] reports that governments on both sides of the Atlantic seek to redesign the infrastructure of the Internet to make instant access net tapping a legal requirement. The U.S. passed the Communications Assistance to Law Enforcement Act and in Europe, a document called Enfopol 98 proposes similar actions. Section 4.2.1 covers this in more detail.

3.2.3 Backdoors

There are two different kind of backdoors: backdoors installed by intruders in a system to get back into the machine even if the administrator tries to secure it, for example, by changing all the passwords. The other kind of backdoors are mechanisms included in a program by the manufacturer.

In this context, the later case is more interesting. It allows the manufacturer or somebody else who knows about this backdoor to get access to installations of or data produced with this software. Sometimes, it is known that such a backdoor exists, but in most cases, this is a secret.

A known case is Lotus Notes. According to [22], in 1996, a backdoor was installed in the export version of Lotus Notes. The export was approved in exchange of having Lotus Notes turn in the key to the backdoor. Thus, the U.S. has the ability to read all encrypted messages written with Lotus Notes export version.

Although this was not kept secret, one should assume that there are certainly similar cases with other software packages exported by American companies.

Another example is cited in [6]. The American NSA (National Security Agency) "has been accused of getting confidential information from the World Bank and other international banks via a software trap the banks did not know existed". In 1992, an American House Judiciary Committee concluded that "there was a substantive evidence that software with the alleged trap door was illegally sold during the 1980s".

The most serious case I found described the encryption systems manufactured by the Swiss company Crypto AG. This company is one of the leaders in encryption systems, and its products have been bought by many governments all over the world, including countries like Iran and Libya. According to several reports (see [16], [17], [18]), these systems have a backdoor in form of a universal decryption key. This was also forced by the NSA which is in possession of this key. The author in [16] describes a number of cases in which the NSA was able to decrypt

important messages from foreign governments which were protected by Crypto AG's systems. Whether or not this is true, it shows how easy it may be to intercept secret messages when the system used is manipulated.

4 Surveillance

Surveillance can occur in different forms. But they all have in common that there is an organization that collects and evaluates information secretly. Surveillance technology can be defined as devices or systems which can monitor, track and assess the movements of individuals, their property, and other assets.

In history, there have been many examples for surveillance systems and organizations. It is not my intention to give an broad overview of these past organizations. I rather focus on some current aspects of national surveillance systems and global surveillance.

4.1 Modern Surveillance

New technologies which were originally conceived for the defense and intelligence sectors, have, after the Cold War, rapidly spread into the law enforcement and private sectors. It is one of the areas of technological advance where outdated regulations have not kept pace with an accelerating pattern of abuses.

An report to the European Parliament by the British human rights organization Omega Foundation ([28]) gives an good overview of the current status of and an outlook on surveillance in Europe. It both addresses incidents in European countries and gives an description of the American Echelon system, which I address in section 4.4.

According to that report, in the last few years many governments have spent huge sums on the development of new technologies for surveillance systems for their police and security forces.

While the adoption of these technologies may have legitimate law enforcement functions and may be relatively harmless when accompanied by strong regulation mechanisms, "without such democratic controls they provide powerful tools of oppression", the report states.

This "parallels a political shift in targeting", the report adds. Instead of investigating crime, law enforcement agencies are now increasingly "tracking certain social classes and races of people living in the red-lined areas before any crime is committed".

4.1.1 Purpose of Surveillance

On the one hand, surveillance has a crucial role in fighting terrorist activities, drug trafficking and organized crime. It is an important tool for the protection of national interest, in particular national security and the investigation of serious crime. Today's police wouldn't be able to fight against these crimes without such means. On the other hand, democratic control of gathered information is essential.

For military use, more sophisticated systems already exist for a long time. But

systems like Echelon are not designed for military targets only. Rather, it can also be used for arbitrary non-military targets: governments, organizations, and businesses in virtually every country ([31]).

In 1992, for example, several British agents told the London Observer that they "could no longer remain silent regarding that which we regard to be gross malpractice and negligence within the establishment we operate". These agents, employees of the Government Communications Headquarters, the British version of the NSA, said that Amnesty International and a group called Christian Aid were routinely targeted (found in [23]).

The use of intelligent services in such a case has no longer something to do with national security, but rather with keeping tabs on critics. Surveillance systems can be used to track down virtually all activity of citizens, may they be accused of a special crime or not. It is a matter of democratic self-understanding and control whether this is really done.

Although some people may think that nobody has to be worried who doesn't have anything to hide, there is a need to determine to what extent these new technologies are about political and social control, rather than citizen protection.

4.1.2 Legal issues

In different countries, different legislation exists that regulates the extent to which authorities are allowed to use surveillance means.

In the U.S., the NSA is the most powerful intelligence agency. In addition to monitor all foreign communications, it still has the legal authority to intercept any communication that begins in the U.S., as well as use American citizens' private communications as fodder for trainee spies (according to [23]).

The same article reports that there is a way to circumvent the prohibition on spying on the own population. UKUSA partners (see 2.1) have used each other several times to intercept communications in their countries. After finding useful results, these data were passed back to the requesting authority.

According to a reference in [22], Norway, for example, has an interesting standpoint: the Norwegian defense department sees no reason to comment on Echelon since it is designed to intercept civilian traffic, and thus it is not a military issue.

4.2 National surveillance

As I already explained, every government has an interest in keeping the own population under surveillance. It is well-known that countries like Iraq or China suppress and control their citizens. But the democratic European and American countries also keep their citizens under surveillance. The difference is the extent to which this is done.

Because I want to focus on global surveillance I only give a brief example of the

current European attempt to increase the surveillance on Europeans.

4.2.1 Example Europe

Beginning in 1991, new plans have emerged in Europe to create an European-wide surveillance system. Currently, in April 1999, these surveillance plans, called Enfopol 98, are about to become law in all countries of the European union. Most of the following information is found on [29].

Enfopol surveillance plans target any form of telecommunications - be it data, encrypted or in clear form, mobile telephony, the new Iridium system and other satellite mobile phone services that may follow. If these plans pass as proposed Enfopol will be able to monitor almost every communication.

Currently, Enfopol is not reality but merely a proposal drawn up by a working group for police collaboration. But before November 1998, this new system was not known to the public. At that time a German magazine published the first draft of the final Enfopol proposal and initiated a public discussion.

It is interesting to note that the Enfopol proposal resembles legal draft papers that were already put to work in Germany and Austria, but finally dismissed because of an outcry in the public.

As far as I could see, this system should only be used for European-internal purposes. Whether it is designed only to track suspects, or to filter all communications without special suspicion, is something I don't know.

4.3 Global surveillance

Global surveillance differs from national surveillance only in its goals. Instead of keeping the own population under surveillance, other nations and foreign companies are the targets. Thus, this is not the responsibility of law enforcement authorities but intelligence agencies.

According to the official position of the U.S., surveillance is only used to track terrorists and criminals all over the world and as a means for counter-espionage.

There is one known system that is capable of global surveillance - Echelon. This system is described in detail in the following section. Besides Echelon, I only found references to two similar systems.

One of these systems is operated by France. I have only found two references, but not even the name of the system. Nevertheless, the sources seem to be quite credible ([24] and [42]). According to this information, France maintains several stations for eavesdropping all over the world in countries that were former colonies. Besides several stations in France, there are stations in the Central African Republic, Guadeloupe, on Reunion, in Guyana, and in the United Arabic Emirates.

Whereas that system might exist and work, there are plans to launch a global

surveillance system by the European Union and the FBI (see [22], [30], [31], [34]).

In 1995, the European countries signed a memorandum of understanding, which still remains classified, to set up a new international telephone tapping network. The EU governments agreed to cooperate closely on this issue with the Federal Bureau of Investigation. Actually, it seems the requirements set by the Europeans for such a system agree with the requirements set by the FBI earlier.

These requirements cover the real-time surveillance of phone-calls, faxes, and e-mails. This includes both traditional communication technology (land and sea lines) and new satellite based systems. All details concerning e-mails accounts and mobile phone subscriptions have to be handed over by the respective providers.

The current proposal has never been discussed or reviewed in any parliament, neither national nor the European. When this draft is signed by the 15 EU member states, it has to be ratified by the national parliaments, but they are not allowed to change anything. I did not find any reference as to whether this already has happened.

4.4 Echelon

Echelon is the name of the system that made me being interested in the current status of surveillance. I got to know something about it because of media coverage after the report to the European Parliament, which I already mentioned, was published ([28]). Although I will try to describe this system as accurately as possible, I have to repeat that most information I found is based mainly on two sources: that report and a book by an journalist from New Zealand ([21]). This journalist also wrote a summary of his book, which can be found at [20].

4.4.1 Overview

Echelon is designed to intercept communication in form of fax, telex, e-mail messages, and phone calls. It is maintained by five nations: The U.S., Britain, Canada, Australia and New Zealand. Together they control a network of computers and interception facilities. The interception stations are placed all over the world so that most communication can be eavesdropped.

Intercepted messages are processed by computer systems that use filters to find relevant material. These filters consist of keyword lists that are maintained by the intelligence agencies of the involved countries. One of those keyword lists exists for each category of interest. Once a message is filtered and assigned to a specific category it is passed to the according central database.

Those persons with the permission to view the stored data are able to see the messages saved in a category. Several rules regulate which agencies are allowed to get to know what kind of information. Generally, all intercepted messages

for a specific category are passed to that agency that created this category.

Such a system can hardly be used to keep a particular person under constant surveillance. But it is useful for special areas of interest, for example to get to know all communication about an organization whose name appears in messages about it. Because the keywords and related filter rules can be as complex as necessary it is possible to get quite accurate results.

But it has also to be said that on the one hand, Echelon has the potential to intercept millions of communications and can be used to violate privacy, but on the other hands, sorting and reading all the data is a real problem. There are simply not enough analysts to sort through everything.

4.4.2 Historic development

Beginning with the UKUSA Agreement of 1947, the five participating countries worked closely together in the area of signals intelligence, or SIGINT. In the beginning, this included mainly exchange of information gained by one of agency and needed by another agency. This exchange had to be done manually.

In the 1970s, the first computer systems to intercept and eavesdrop messages and phone calls were created and used. But this was apparently still done independently in each country.

A newspaper article from August 7, 1980 that I couldn't find wrote about a U.S. satellite and communications base at Menwith Hill. near Harrogate in Yorkshire. According to this report, "it is run undercover by the NSA and taps into all Britain's main national and international communications networks" (reference found in [26]).

In [23], I found a remark, that in the early '80s, the NSA was developing a system called Platform, which would integrate at least 52 separate SIGINT agency computer systems into one central network.

Another article from August 12, 1988 ([26]) reported details about a global surveillance system called "Project 415". This system seems to be closely related to the Echelon which was about to be implemented. The article states that in Britain, the GCHQ had 15,000 staff and a budget of 500 million pounds.

When exactly Echelon was created as it exists today is hard to tell. Probably, the system Platform eventually became Echelon. The earliest definite date I found was about New Zealand joining Echelon in 1989 ([20]).

4.4.3 Detailed description

The detailed description in this section is mainly based on two sources: [20] and [36].

Echelon consists of several components. The first component are five stations that are distributed all over the world targeted to all important telecommunica-

tion satellites (Intelsats). A station in England is targeted against the Atlantic, Europe, and the Indian Ocean. Two stations in the U.S. intercept communications of North and South America and parts of the Pacific, and two more stations are located in Australia and New Zealand to ensure global interception.

The next component of Echelon intercepts a range of satellite communication not carried by Intelsat. At least five more stations exist in England, Australia, Canada, Germany, and Japan.

The final component of Echelon are stations that tap into land-based telecommunication systems. This covers both cables and microwave networks. One of these facilities, for example, is located in London and taps into most communication across the Atlantic based on land and sea cables.

The computers in each station are called Dictionaries. They are connected via highly encrypted communications with the headquarters of the five agencies. All messages intercepted by one of the Dictionaries is sent to one of the headquarter for further processing.

To handle the huge amount of messages sent each day, each agency maintains a list of categories of interest. For each category a number of keywords are selected. These keywords may include names of people, organizations or objects.

These lists of categories are sent to the Dictionary computers which filter the incoming messages according to them. Whenever a relevant message is found it is sent to the headquarter that defined the according category. Essentially, an agency only sees those messages that they wanted to have filtered for themselves. Other filtered messages, even if it's done on one of their own Dictionary computers, are not visible. If an agency wants to have access to data gathered by Echelon for another agency, they need to apply for that.

The software used for Echelon is built with products from Memex ([27]), an American company.

The core of all products from Memex is called "Memex Information Engine" (MIE). MIE is essentially a library used for information retrieval and management. It has very powerful functions to collect, analyze, and compare data. Furthermore, sophisticated search tools are provided that produce accurate hit lists.

Further applications made with MIE include CRIMINT (Criminal Intelligence System), used, for example, by the London Metropolian Police Force or the Scottish Criminal Intelligence Office. This software is a data management system that allows fast data retrieving and referencing between old and current operational data.

Another system is called PATHFINDER. It is a system to analyze and filter huge amounts of data, made in particular for the American army.

4.4.4 Political consequences

After release of the already cited report to the European Parliament ([28]) a broad news coverage and debates began in Europe, mainly because Echelon is also used to intercept all European communications. That this is done by allies upset not only the national parliaments.

On September 19, 1998 the European Parliament debated both the EU's relationship with the United States and the existence and uses of Echelon. Martin Bangemann, member of the European commission, stated that as long as the commission does not have official information from the U.S. about the existence of this system, they cannot react. Even if media reports about such a system, it does not necessarily mean it exists.

An article in Wired ([32]) reported that the European Parliament had "swept aside concerns about alleged surveillance and spying activities conducted in the region by the US government". But they also cite a member of the parliament stating that the "decision on Echelon, pending further investigation, was influenced by pressure from the US government, which has tried to keep the system secret".

According to [22], the newspaper Le Figaro found out that some "EU governments have known of the existence of Echelon. They have chosen to make no public complaint but instead warn companies of the dangers of transmitting sensitive information on international telephone lines".

On the other hand, keeping in mind the cooperation between the European Union and the FBI, I am not sure how serious the European countries' complaint about Echelon is. Echelon and the proposal by the EU and FBI are independent, but complementary. The EU/FBI proposal sets requirements for technical changes to current networks that allow or make it easier, respectively, to tap in. Echelon, on the other hand, is able to filter all content that gets through it. Together, these systems, could give the owners enormous power of control and surveillance.

5 Economic Espionage

The last section was about surveillance and current systems for it. This section covers one of the possible uses of surveillance: Gaining economic information, also called economic espionage.

Since the Cold War is over, at least for the Western world, the threat is no longer communists, but competing capitalists. Therefore, many of the existing systems are now reused for the purpose of getting an advantage over competitors.

5.1 Definitions

According to [5], "economic espionage can be described as clandestine or coercive attempts by foreign entities to obtain commercially or policy relevant economic information".

In [6], several further definitions are made:

Economic security is defined as the maintenance of those conditions necessary to encourage long-term relative improvements in labour and capital productivity and thus a high and rising standard of living for a nation's citizens.

Economic intelligence is commercially relevant economic information the possession of which could assist the relative productivity or competitive position of the owner. If economic security is the goal, economic intelligence is an important element in achieving that goal.

Economic espionage can thus be seen as the use of illegal means by a foreign government to acquire economic intelligence.

Finally, industrial espionage is the use of illegal means by a private sector organization to acquire economic intelligence.

5.2 Reasons for economic espionage

There are several reasons why many countries engage in economic espionage.

There is an analogy between the impact of economic espionage and the impact of more familiar espionage. In this way, economic espionage could be seen to be as important to a country's economic security as more familiar types of espionage are to its more traditional security interests.

Furthermore, a big advantage of economic espionage is its potential cost effectiveness. A few well directed operations could achieve the same effect as a large investment or subsidy for the relatively low cost of an economic espionage operation.

In a world in which economic interdependencies are increasing and international competition is getting rougher, tensions and conflicts between nations are also increasing. Driven by high unemployment and industrial displacement, many

countries consider their economic situation as a primary concern. For them, economic espionage is a means by which to be able to compete. This applies to all countries, whether they are rich or poor.

Thus, it is not a surprise that among the information spies are most seeking after are research and development strategies, manufacturing and marketing plans, and even customer lists (see [11]).

5.3 Official statements and legal issues

While economic espionage is considered a threat to national security, it does not necessarily involve an illegal act. Often, economic espionage acts within a grey zone, which explains to a certain extent why countering this activity is the duty of intelligence services rather than enforcement authorities such as the police.

In this section, I show standpoints and statements of different countries on this topic.

5.3.1 USA

Several agencies engage in counter-espionage, but officials of the agencies insist that official U.S. policy bars spying on foreign companies and governments.

On the other hand, President Clinton has been giving priority to economic intelligence in foreign policy. Intelligence sources claim that the CIA has scored several successes in commercial spying (see [11]).

In [5], Stansfield Turner, an intelligence director during the Carter administration, is cited as: "If economic strength should be now recognized as a vital component of national security, parallel with military power, why should America be concerned about stealing and employing economic secrets?" This shows that despite official denials economic espionage has also for the U.S. always been an important topic.

This is strengthened by a presidential statement, U.S. President Clinton made 1994 ([7]): "[...] the intelligence community must track political, economic, social and military developments in those parts of the world [...] where overt collection of information from open sources is inadequate. Economic intelligence will play an increasingly important role in helping policy-makers understand economic trends. [...]"

5.3.2 Canada

The same reference as above states that the Canadian intelligence community seems to have also an increased interest in the economic and commercial world. Until July 1995, when this report was written, the Canadian government has made no official statements concerning offensive economic intelligence activities.

Nevertheless, the article reports that Canada's Communications Security Establishment (CSE) is seeking for university graduates in the fields of economics and international business.

5.3.3 European countries

The situation in Europe is very similar to the situation in North America. Cases of espionage happen on both sides of the Atlantic, as I will show in section 5.4.

In Britain, for example, there was no legislation before 1994 that prohibited private surveillance and industrial/economic espionage. Under former law, penalties only applied to the theft of government military secrets. After several serious incidents, a new legislation was proposed that would make it an offense to gain information through deception.

France is one of those countries that is said to have a very active intelligence service for economic espionage. The report [6], which was written July 1994, tells about an embarrassing release of information about those activities targeted against American companies. It turned out that the companies responsible for leaking the information were unhappy with the French intelligence service (DGSE). They argued that the DGSE favored some companies in distributing material gained by economic espionage.

The situation in Russia is quite similar. A report ([14]) from 1996 states that Russian President Yeltsin had "ordered top Russian officials to close the technology gap with the West and told them to make better use of industrial intelligence to do so".

5.3.4 Asian countries

Although I have not been able to find official statements from any Asian country it can be assumed that their position might be quite similar to those of Western countries. In many respects, do they have even more reasons to try to get to know more information about technology by espionage.

The economic situation in many Asian countries is uncertain. Although some countries had already made progress in development of their own industry, the economic crisis from 1998 had shown that they are still far away from the same standards as they exist in the Western world. Therefore, it is not surprising that in [13], China is named as one of the most active countries engaging in espionage in the U.S.

More examples are given in [11] about China, Japan, and South Korea. For the latter country, this article says that "South Korea possesses one of the world's most successful intelligence organizations".

5.4 Everyone is a victim

It was very interesting to see how reports written in different countries gave different views on the issue of economic espionage. Essentially, it was always stated that it was the other nations that try to steal economic secrets from their own country. Because those reports were published in almost every country, always accusing many other countries, this is one more indication that virtually every country is active in this area.

This section should give an impression about incidents that really happened. They show that espionage is a serious threat for every company that is engaged in international business. Apparently, the main targets are high-tech companies that had invested a lot of money in the development of new technologies.

The following examples are taken from: [5], [6], [7], [11], [12], [22].

In one case, the NSA eavesdropped on all faxes and phone calls between the European consortium Airbus, the Saudi national airline, and the Saudi government. After the agency passed this information to Boeing Co. and McDonnell Douglas Corp., these companies won in the $6 billion competition.

American intelligence agents were accused of breaking into computers of the European parliament as part of a campaign aimed at stealing economic and political secrets. Security officials state that the information obtained was used by the Americans in 1995's GATT negotiations.

On the other hand, French intelligence has spied on U.S. companies by wiretapping U.S. business people flying on Air France between New York and Paris.

In one case, even officials in Ghana were concerned about their computers connected to United Nations International Development Organization computers in New York. They were afraid of sensitive economic data being transmitted without their knowledge.

China is reported to be using members of visiting delegations and exchanges to conduct economic espionage in many developed countries.

Furthermore, there were reports of Americans accusing German companies, German articles talking about French and American activities, and stories from France telling how the country was targeted by foreign spies. This list is endless and is necessarily incomplete.

6 Conclusion

In this paper, I showed two main areas of intelligence activity: surveillance and economic espionage. I gave background information, described traditional and modern methods and technologies used for these purposes, and covered main aspects of both areas.

I had decided to cover two related but different areas, because of the current relevance of both of them. Whereas surveillance is more about how to gain information, espionage, especially economic espionage, is more about how to get an advantage out of the information obtained.

Several important issues exist that I could not cover. These include, for example, privacy concerns and means for protection against surveillance and espionage.

Intelligence agencies live in a world of their own. They are not controlled by parliaments but posses technologies that give them potentially emense power. In public, little is known about the activities of the intelligence community. With this paper, I wanted to give an impression of a small part of intelligence agencies' work and how this can potentially affect everybody's life, both as an individual and as part of a company.

References

[1] Website: *Infowar.com*,
URL: www.infowar.com

[2] Webpage: *Economic Espionage Information Links*,
URL: http://pimall.com/nais/econesp.html.

[3] Dr. Myron L. Cramer: *Information Warfare*,
URL: http://iw.windermeregroup.com/Papers/infowar.html.

[4] USIS Washington File: *CIA Official Assesses Information Warfare Threat*, December 10, 1998,
URL: http://jya.com/cia-iwt.htm.

[5] Canadian Security Intelligence Service: *Commentary No. 32: Economic Espionage*, May 1993,
URL: http://www.csis-scrs.gc.ca/eng/comment/com32e.html.

[6] Canadian Security Intelligence Service: *Commentary No. 46: Economic Espionage (II)*, July 1994,
URL: http://www.csis-scrs.gc.ca/eng/comment/com46e.html.

[7] Canadian Security Intelligence Service: *Commentary No. 59: Economic/ Commercial Interests and Intelligence Services*, July 1995,
URL: http://www.csis-scrs.gc.ca/eng/comment/com59e.html.

[8] Patrick W. Kelly: *The Economic Espionage Act of 1996*, FBI,
URL: http://www.fbi.gov/leb/july976.htm.

[9] US Congress: *Industrial Espionage Act of 1996*, February 1, 1996:
URL: http://www.infowar.com/class_2/class2_4.html-ssi.

[10] Webpage: *What is Corporate Espionage?*,
URL: http://www.ozdirectory.com.au/acia/html/espionage.html.

[11] Jack Nelson: *U.S. Firms' '97 Losses to Spies Put a $300 Billion*, Los Angeles Times,
URL: http://www.infowar.com/class_2/class2_012798a.html-ssi.

[12] *CIA spies on Europe?*, London Sunday Times, August 4, 1996,
URL: http://www.infowar.com/class_2/cia.html-ssi.

[13] *Israel Named in US Industrial Espionage Report*,
URL: http://www.infowar.com/class_2/class2_082697a.html-ssi.

[14] Ben N. Venzke: *Economic/Industrial Espionage*,
URL: http://www.infowar.com/class_2/class2_2.html-ssi.

[15] James Bamford: *The Puzzle Palace: A Report on America's Most Secret Agency*, Penguin Books, 1983, chapter 8.

[16] Wayne Madsen: *Crypto AG: The NSA's Trojan Whore?*, Covered Action Quaterly,
URL: http://caq.com/cryptogate.

[17] Laszlo Baranyi: *Crypto AG*,
URL: http://www.qainfo.se/ lb/crypto_ag.htm.

[18] Company Webpage: *Crypto AG*,
URL: http://www.crypto.ch.

[19] Canadian Security Intelligence Service: *1997 Public Report*,
URL: http://www.csis-scrs.gc.ca/eng/publicrp/pub1997e.html.

[20] Nicky Hager: *Exposing the Global Surveillance System*, Covered Action Quaterly,
URL: http://www.mediafilter.org/caq/CAQ59GlobalSnoop.html.

[21] Nicky Hager: *Secret Power - New Zealand's Role in the International Spy Network*, Craig Potton Publishing, 1996

[22] Laszlo Baranyi: *Codename: Echelon*,
URL: http://www.qainfo.se/ lb/echelon.htm.

[23] Jason Vest: *Listening In*, The Village Voice, August 12-18, 1998,
URL: http://www.villagevoice.com/features/9833/vest.shtml.

[24] Erich Moechel: *E-Commerce-Tagung im Schatten Echelons*, in German, November 17, 1998,
URL: http://www.telepolis.de/tp/deutsch/inhalt/te/1585/1.html.

[25] Webpage: *Paul Wolf's Echelon Links*,
URL: http://www.icdc.com/ paulwolf/echelon.htm.

[26] *Somebody's Listening*, New Statesman, August 12, 1988,
URL: http://jya.com/echelon-dc.htm.

[27] Company website: *Memex*,
URL: http://www.memex.com.

[28] Omega Foundation: *An Appraisal of the Technologies of Political Control*, Summary & Options Report For The European Parliament, September 1998,
URL: http://www.infowar.com/class_2/class2_102998a_j.shtml.

[29] Webpage: *Telepolis ENFOPOL papers*, compiled by Telepolis,
URL: http://www.heise.de/tp/english/special/enfo/default.html

[30] *European Union and FBI launch global surveillance system*, Statewatch report, February 1997,
URL: http://www.privacy.org/pi/issues/tapping/statewatch_tap_297.html.

[31] Bruno Giussani: *European Study Paints a Chilling Portrait of Technology's Uses*, New York Times, February 24, 1998,
URL: http://www.icdc.com/ paulwolf/nytimes.htm.

[32] *Europe Ends Debate Over U.S. Techno-surveillance*, Wired, August 10, 1998,
URL: http://www.infowar.com/class_2/class2_101498b_l.shtml.

[33] *EU Urges Debate on U.S. Wiretapping of Foreign Firms*, October 1, 1998,
URL: http://www.infowar.com/class_2/class2_101498a_l.shtml.

[34] *EU-FBI telecommunications surveillance system extended to Internet and satellite phones*, from Statewatch bulletin, November-December 1998,
URL: http://www.statewatch.org/news.html.

[35] Duncan Campbell: *UK: The Arrival of free and unsurveilled global Communcication is anathema*, Guardian, January 1, 1999,
URL: http://www.infowar.com/class_2/99/class2_012299b_j.shtml.

[36] Kai Raven: *Das Ministerium fuer Wahrheit*, in German,
URL: http://home.kamp.net/home/kai.raven/ministry.html.

[37] John Manley: *Nanada's Cryptography Policy*, Presentation to the National Press Club, October 1, 1998,
URL: http://www.jya.com/ca-crypto.htm.

[38] *CBC Newsworld Documentary - US Communication Interception*, Computer Privacy Digest V4#012, January 2, 1994,
URL: http://www.cs.uwm.edu/faculty/levine/cpd.homepage.html.

[39] Christopher Klaus: *Paper on Backdoors*, August 5, 1997,
URL: http://www.clip.dia.fi.upm.es/ alopez/bugs/bugtraq2/0314.html.

[40] Website for: *Wassenaar Arangement*,
URL: http://www.wassenaar.org.

[41] Webpage: *The Clipper Chip*,
URL: http://www.epic.org/crypto/clipper.

[42] Website: *Interception*,
URL: http://www.ii-mel.com/interception/francegb.html.