When new technologies revolutionize spying activities. What do we have to fear ?

by Mathieu DESCHAMPS

- *Context.*
- *Echelon birth and historical.*
- *How does it works.*
- *Information well kept, the wall of silence.*
- *Some experts begin to speak, Interview.*
- *The power of Echelon : interconnected networks around the world.*
- *A few words about french capacities : « Frenchlon ».*
- *Known and supposed limits.*
- *Mystification and information manipulation.*

Forewords

Thanked to espionage, the knowledge of capital informations during wars has certainly saved numbers of lives. The nowadays economy is currently the theater of a **secret war**, a war of espionage through the Net and telecommunications. **The victory returns to whom knows** first what commercial agreements will be undertaken, what decision of such government will take on such action, when such influent personality will meet such other. **A listenning system exists for forty years, designed by Americans it is nammed Echelon**. Laudable at the beginning, it has become a powerful tool handed by co-contracting contries notably to be first « on the take » in commercial businesses. **This system process huge amount of data** in order to, by discriminating some keywords, select such a message for its content and led it to the concerned spying agency. There is number of dictionnaries each containning hundred of thousands keywords, each specialized in a specific matter.

While information becomes accessible worldwide in a few second and counts increasingly in our choice and actions, **who today held this power ?** What is the real power of Echelon ? Several contries are to get involved in it, but secret is hard to break. Those who speak about it says it become relatively easy and cheap, scaled to a country especially thanks to computeurs low maintenance costs.

The real power of Echelon is to be an multinationnal interconnected network, this is to say that several contries are working pairs in it. **France has developped its Echelon called Frechlon** to repel spying effort. Experts disagrees talking about Echelon, some intent to say that Internet in every houses could be an inquisitive eye whereas other demonstrate that Echelon means are too limited. The fact is that, the willing to keep information private is growing and lot's of crytographic software are sold by those whom seems to curiosly get involved in Echelon project. **And what if this was only a machiavellian manipulation ?** The essential of documentation about Echelon seemed to come from the same source.

Context

1940. The espionage of allies gives a decisive advantage on forces of 3rd Reich. Historians and governments agree both to tell that technological innovations such as the radar and the radio have helped for a lot.

In the late 1980, in a decision it probably regrets, the U.S prompted new Zealand to join a new and highly secret global intellignece system : **Echelon**. Investigations into it and the discovery of its dictionnnary has revealed one of the world's biggest, most closely held intelligence projects, this system allow spy agencies to monitor most of the world's telephone, e-mail, and telex communications.

Echelon birth and historical

For 40 years, New Zealand's largest intelligence agency, the Government Communications Security Bureau (GCSB), nation's equivalent of the US' National Security Agency (NSA), had been helping its Western allies to spy on countries throughout the Pacific region, without New Zealand's people been aware neither many of its highest elected officials. What NSA did not know is that by the late 1980s, various intelligence staff had decided theses activities had been too secret for too long, and were providing noone with interviews and documents exposing New Zealand's intelligence activities. More than fifty people who work or have worked in intelligence and related fields agreed to be interviewed.

Activities they described made it possible to document, from the South Pacific, some Alliance-wide systems and projects which have been kept secret elsewhere. In those, by far the most important is **ECHELON**.

Designed and coordinated by NSA, **ECHELON system is used to intercept ordinary e-mail, fax, telex, and telephone communications carried over the world's telecommunications networks**. Unlike many of the electronic spy systems developed during the Cold War, ECHELON is designed primarily for non-military targets: governments, organizations, businesses, and individuals in virtually every country. It potentially **affects every person communicating** between (and sometimes within) countries **anywhere in the world**.

It is, of course, not a new idea that intelligence organizations tap into e-mail and other public telecommunications networks. What was new in the material leaked by the New Zealand intelligence staff was precise information on where the spying is done, how the system works, its capabilities and shortcomings, and many details such as codenames.

How does it works

The ECHELON system is not typically designed to eavesdrop on a particular individual's e-mail or fax link. Rather, the system works by indiscriminately intercepting very large quantities of communications and using computers to identify and extract messages of interest from the mass of unwanted ones. **A chain of secret interception facilities has been established around the world to tap into all international telecommunications networks' major components**. Some monitor communications satellites, others land-based communications networks, and others radio communications. ECHELON links together all these facilities, providing the US and its allies with the ability to intercept a large proportion of planet's communications.

The computers at each station in ECHELON's network automatically search through millions of messages, somes are intercepted when containing pre-programmed keywords. Keywords include all names, localities, subjects, and so-on that might be mentioned. Every word of every message intercepted at each station gets automatically searched whether (or not) such specific telephone number or such e-mail address is listed. The thousands of simultaneous messages are read in "real time" as they pour into the station, hour after hour, day after day, as computer finds intelligence needles in telecommunications haystacks.

Information well kept, the wall of silence

Intelligence mission's objective has been considered as difficult by all speakers met by reporters, some congratulating however Parliament's intervention; and considers that all debate on a such subject was healthy. Most important difficulties have concerned encounters that reporters wished to have with intelligence services' responsibles. In France, “le ministère de l'intérieur” has allowed reporters to meet two responsibles of “la direction de la surveillance du territoire”(DST) whose director himself and the minister of Defense has accepted an audition of external security's minister. More, the general Delegation to the armament has presented to reporters some of its searchers in the area of listen.

Overseas, **reporters hurt themselves to a non-receive principle by both of the American and British authority**.

It is first of all interesting to underline that British's refusal has been based on the fact that reporters was not even member of a representative's parliamentary delegation to control of intelligence's services. This attitude can only reinforce Defense's Commission in the idea that a proposoition of law aiming to create a such structure from the national Assembly is more than ever necessary.

To United States, **administration's reticences**, despite **repeated revivals of french Embassy** in Washington, are difficultly comprehensible. It has been explained **that it did not concern an inquiry commission but an intelligence's mission in order to collect American responsible's opinion**. This refusal's decision to receive reporters taken, it seems at the highest level after many deliberations, has as consequence to relaunch all suspicions of Echelon's role and United States especially. What is more surprising is that responsibles or ex-federal agency's responsibles have expressed publicly on the subject. All speakers in the matter met in Washington have elsewhere expressed their incomprenhension about this refusal.

Some experts begin to speak, Interview

Telecommunications security expert in Germany, Manfred Fink, tells exactly what individuals and companies have to fear from covert surveillance

How long have you known about Echelon?
Fink: Experts have known for years that we are systematically being monitored. It's the first time, however, that the problem is being perceived as a reality, now that the European Parliament and Deutscher Bundestag -- German Parliament -- are getting involved.

What reasons lie behind the secrecy surrounding Echelon?
Fink: There are two reasons: on the one side, prosecutors have no interest in having their entire operation laid out in the open. There is no disclaimer. One simply doesn't say anything.
On the other side, any... German officials with the power to say something has until now remained quiet in order to prevent putting any inter-governmental projects at risk. The government didn't want to jeopardise the NATO alliance. But both France and England have their own spy satellites, as does China. This... weighs greatly upon EU partnerships.

What makes a person a target? Who is likely to be spied on?
Fink: There is a lot of abuse in the relationships between European allies. Ordinary individuals are unlikely to be a target, but companies will be. The size of the firm being targeted is relatively unimportant, but international companies will be monitored no matter what.
Whether you own a small company of just 20 employees, have a specific product that only you offer worldwide or have only one competitor who sits in the US, you are bound to be of interest.

Is there anyway of knowing you are being monitored?
Fink: No.

To whom do you recommend the installation of high-tech security?
Fink: I recommend that all companies set up solid security. One must ask the question: "Would it be serious if they got hold of a third of the information in this communication?" Whoever replies "Yes" should make a security decision.

If the secret services have such efficient hacking machines, does it make any sense at all to use cryptography?
Fink: Information is perishable. If it takes months or years to obtain it, it often loses its value. This is the absolute starting point for defence: setting the threshold so high that the circumstances no longer require the information to be obtained.

Is it true that the radiation generated by monitors can be picked up and reproduced from as far as a hundred metres away?
Fink: Yes, whether it is a Word document with twelve point text font, an Excel spreadsheet or a CAD-image, you can pick it up via the monitor's radiation. Equipment to do this is available for DM250,000 (£8,000).
To prevent this you can either shield your monitor and hard drive or isolate entire rooms. This is how it is done in large calculus centres. Another method is to overwrite the emissions with a jamming signal so that the receiver will see nothing but a snow flurry on the screen.

Mobile phones must be easy to monitor. Is this true?
Fink: Mobile phones are actually better than we think. The air interface to base station is quite safe unless you happen to be standing opposite a news station. The rest runs on directional radio and public networks. These are indeed relatively easy to pick up.

Rumours from the US secret services claim there is a transantlantic fibreglass cable that picks up and retrieves data. Is this a modern fairy-tale or is it true?
Fink: No. In fact it's an entire underwater station held by cables made of copper. Other than that, it's correct. I have seen photos of it and these were no fakes.

The Power of Echelon : interconnected networks around the world

Computers in stations around the globe are known, within the Network, as ECHELON's Dictionaries. Computers that can automatically search through traffic for keywords have existed since at least the 1970s, but ECHELON system was designed by NSA to interconnect all thoses computers and allow stations to function as components of an integrated whole. **NSA and GCSB** (German's intellignce's services) are **together bound under five-nation UKUSA signals intelligence agreement**. **The other three partners**, all with equally obscure names, are the **Government Communications Headquarters (GCHQ)** in Britain, the **Communications Security Establishment (CSE)** in Canada, and the **Defense Signals Directorate (DSD)** in Australia.

The alliance, which grew from cooperative efforts during World War II to intercept radio transmissions, was **formalized into the UKUSA agreement in 1948** and **aimed primarily against the USSR**. The five UKUSA agencies are today the largest intelligence organizations in their respective countries. With much of world's business occurring by fax, e-mail, and phone, spying on thoses communications receives the bulk of intelligence resources. For decades before ECHELON system's introduction, UKUSA's allies did intelligence collection operations for each other, but **each agency usually processed and analyzed interception's bulk from its own stations**.

Under ECHELON, a particular station's Dictionary computer contains not only its parent agency's chosen keywords, but also has lists entered in for other agencies. In New Zealand's satellite interception station at Waihopai (in the South Island), for example, computer has separate search lists for the NSA, GCHQ, DSD, and CSE in addition to its own. Whenever the Dictionary encounters a message containing one of the agencies' keywords, it automatically picks it and sends it directly to the concerned agency's headquarter. No one in New Zealand screens, neither even sees, collected intelligence by New Zealand station for foreign agencies. Thus, stations of junior **UKUSA allies function for NSA no differently than if they were officially NSA-run bases located on its soil**.

The first component of ECHELON network is stations specifically targeted on international telecommunications' satellites (Intelsats) used by phone companies of most countries. A ring of Intelsats is positioned around the world, stationary above the equator, each serving as a relay station for tens of thousands of simultaneous phone calls, fax, and e-mail. **Five UKUSA stations have been established to intercept the communications carried by the Intelsats**.

The British GCHQ station is located at the top of high cliffs above the sea at Morwenstow in Cornwall. Satellite dishes beside sprawling operations buildings point toward Intelsats above Atlantic, Europe, and, inclined almost to horizon, Indian Ocean. An NSA station at Sugar Grove, located 250 kilometers southwest of Washington DC, in the mountains of West Virginia, covers Atlantic Intelsats transmitting down toward North and South America. Another NSA station is in Washington State, 200 kilometers southwest of Seattle, inside the Army's Yakima Firing Center. Its satellite dishes point out toward the Pacific Intelsats and to the east.

The job of intercepting Pacific Intelsat communications that cannot be intercepted at Yakima went to New Zealand and Australia. Their South Pacific location helps to ensure global interception. New Zealand provides the station at Waihopai and Australia supplies the Geraldton station in West Australia (which targets both Pacific and Indian Ocean Intelsats).

Each of the five stations' Dictionary computers has a codename to distinguish it from others in the network. The Yakima station, for instance, located in desert country between the Saddle Mountains and Rattlesnake Hills, has the **COWBOY Dictionary**, while the Waihopai station has the **FLINTLOCK Dictionary**. These codenames are recorded at the beginning of every intercepted message, before it is transmitted around ECHELON network, allowing analysts to recognize at which station the interception occurred.

New Zealand intelligence staff has been closely involved with NSA's Yakima station since 1981, when NSA pushed GCSB to contribute to a project targeting Japanese embassy communications. Since then, all five UKUSA agencies have been responsible for monitoring diplomatic cables from all Japanese posts within the same segments of the globe they are assigned for general UKUSA monitoring. Until New Zealand's integration into ECHELON with the opening of Waihopai's station in 1989, it shares of Japanese's communications intercepted at Yakima and sent unprocessed to GCSB headquarters in Wellington for decryption, translation, and writing into UKUSA-format intelligence reports (NSA provides codebreaking programs).

Few words about french capacities : "Frenchlon"

France has real capacities of listening whose some are envied and have made their proofs, and their values during recent conflicts (listen for example during Golf's Wars or in Bosnia). French services couldn’t afford to have a full panoply of listening devices. More, current means are terribly solicited meanwhile threat's emergence no one does control. **They are geographically oriented and limited also it can in no manner be compared to Echelon system**.

Moreover, France has left a distance in areas of electronics and data-processing and no computer leader exists in Europe whereas it has excellent means of expertise. **While U.S have invested lately near 3 billion dollars** over three years in favor of information systems' security, **France devotes only 1 % of this amount**. The amount of uphill studies on these questions has been doubled in 2000's budget (approximately 40 millions of Francs) but this endowment remains largely insufficient. Even if the question is not to close the gap taken on partners of Echelon thanks for example to performance of new equipment, means to implement are incompatible with equipment budgets' reduction. Next military's programming law under release provides the opportunity, concerning military equipment, to remedy to an incompatible situation compared to the ambitious policy of information system's security.

Echelon known and supposed limits

It is necessary to remain prudent on potentialities of listening and to figure what suchs systems provides in terms of intercepted messages' quantity. First of all because what imports is processing capacity. Then, among population, listening services' goal is to identify targets that counts (approximately 5 000 persons for example in France) and to follow them : **means of listening are therefore oriented on this personalities**.

Finally, open sources are enough to provide databases. One can thus follow companies' activity and their leaders through technical and specialized press.

The skepticism's thesis, lowers on many factors potentialities of Echelon's listening system :

On one hand, **it is doubtful that the whole planet is constantly covered**, Echelon system for example having been constituted to struggle against the communist block and its satellites, and rests mainly on interception of satelites communications;

On the other hand, **wire communications remain difficult to intercept without that being noticed or without a telecom operator complicity** (Nevertheless, strong suspicions exist on a possible connivance between British Telecom and the GCHQ). **Optical fibers tapping would also be delicate,** because of the necessity (to realize an interception) to have a signal amplifier that amplifies luminous signals to regular intervals, and **mostly due to the fact that all intrusion on the optical fiber is divulged in end of line**. Some experts estimate however that intrusions are possible because o**ptical diversions are achievable by having access directly to fibers**, for example gaining access to distribution centers, or by positioning on fiber's envelope a device and by wining extremely weak waves that are emitted there ;

More, multiplication of communications, **finally on Internet renders materially impossible the interception of all messages, and moreover their stocking and their processing.**

Equally message sorting's possibilities doesn't reduce technical difficulties. Indeed, limits of interception systems are linked to collectd data's processing. Sorting out interesting informations from raw data necessitates selection or extraction techniques that are very perfectionnate and time-consuming. Several countries have competences in these techniques. **Russians hold certainly competence in the area of selection. France has some advantages in technologies of algorithms and the linguistics**, what favors trades of technologies with others country. But the element that is the most important actually remains in computation's power. **Some specialists' estimations tend to show that, despite all their means, partner services of UKUSA no longer are in measure to process collected informations mass**.

Finally, crytography techniques' deployement decreases processing and analysis capacities, because computation's power grows then overwhelming. Despite the extent of its means, **NSA would not have means to process all crypted messages and neither less to analyze them**, even if instaneous tagerted listens still grows and even if sortings capacity still strengthen.

Lately, most of speakers that reporters have met in the United States have informed **overestimatation of system's performances notably in the media**. **They have underlined that federal intelligence agencies submitted to a congressional narrow control (notably on budgetary point) no longer had enough capacities**. Some specialists have even characterized **NSA as a "dinosaur" exceeded by technologies' evolution and the mass of information**. Elsewhere, NSA's responsibles complain to regress in capacities and congressional members do not appreciate the lack of performances of this agency.

In any case, whatever are performances of Echelon's system, it has to be completed by others systems, human or technical. Indeed, analysis capacity is essential, notably concerning terrorism, and **services have to get human competences and a culture that can lack them sometimes, notably in the United States**.

For congressional members and their collaborators met in Washington, as for many American specialists, **security's risks suppose** that capacities of communication interception's systems are concretly strengthened, and that **a new more effective system replaces Echelon system**.

All of speakers has finally pronounced in favor of a precaution principle, in the name of security risks, so as to counter capacities whose appreciation is impossible.

Mystification and information manipulation

Few disturbing facts remains : it has observed that **most of documents published on Echelon seemed to come from the same source**. **Informations notably these extra on Internet are often identical** and give the impression to have been recopied from two or three sources (articles and already quoted works, declassified documents of the NSA etc.) *[Author's note: Whereas precautions have been taken, I can assume that this statement spread-targets also this document]*. **This information similarity** and therefore their relative destitution to the analysis **can testify a deliberated will to orient the debate on interceptions of communications**, will to which the information community would not be foreign.

A first hypothesis, to the limit of the machiavelism, would focus on the **economic actor awareness**, rendered **suspicious face to intrusions** in their systems, and to which **it would then be possible to sell protection systems reliable or not**. **We can return on this hypothesis by evoking defects deliberately introduced in systems and software produced largely in the United States**, notably by the company Microsoft.

An other hypothesis would tend **to decrease the American actor responsibility**, on the one hand by emphasizing **some laudable objectives** (struggle against drug trades and proliferation), on the other hand by insisting on **errors commit even by allied countries** notably concerning **economic corruption**, finally by including others **European countries in the system** as **Ireland, Germany, more recently Denmark or Switzerland** that envisages the installation on its territory of reception stations, perhaps by denouncing the existence of systems by others country and especially US.

A new interrogation can therefore be formulated, about the agreement between intelligence services. **Existence of private hidden clubs** taking concern in intelligence services' informations puts **the fundamental question of the risk of these clubs and their objectives**. In such structures, well of manipulation and orientation possibilities of information are conceivable.

It is necessary furthermore, not to forget that listenning systems led by countries participating to **Echelon have provided Atlantic Alliance in information with unavoidable deformations**, as ones have been able to notice for example in in Bosnia or in the Gulf, **without that there being organic bonds between UKUSA and NATO**.

Sources : ZDNET, Secret Power by Nicky Hager, Mission of information on the spying systems and electronic interception, rapport of deputy Arthur Paecht.