GlobalResearch
Center for Research on Globalization

ECHELON: Exposing the Global Surveillance System

By Nicky Hagar
Global Research, April 25, 2012
Covert Action Quarterly and nickyhagar.info
1 February 1997

Theme: Intelligence, Police State & Civil Rights

This important article was published more than 15 years ago (February 1997) in Covert Action Quarterly

In the late 1980′s, in a decision it probably regrets, the U.S. prompted New Zealand to join a new and highly secret global intelligence system. Hager's investigation into it and his discovery of the Echelon dictionary has revealed one of the world's biggest, most closely held intelligence projects. The system allows spy agencies to monitor most of the world's telephone, e-mail, and telex communications.

For 40 years, New Zealand's largest intelligence agency, the Government Communications Security Bureau (GCSB) the 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 the knowledge of the New Zealand public or many of its highest elected officials. What the NSA did not know is that by the late 1980s, various intelligence staff had decided these activities had been too secret for too long, and were providing me with interviews and documents exposing New Zealand's intelligence activities. Eventually, more than 50 people who work or have worked in intelligence and related fields agreed to be interviewed.

The activities they described made it possible to document, from the South Pacific, some alliance-wide systems and projects which have been kept secret elsewhere. Of these, by far the most important is ECHELON.

Designed and coordinated by NSA, the 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 the codenames.

The ECHELON system is not 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 the major components of the international telecommunications networks. 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 the communications on the planet.

The computers at each station in the ECHELON network automatically search through the millions of messages intercepted for ones containing pre-programmed keywords. Keywords include all the 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 a specific telephone number or e-mail address is on the list.

The thousands of simultaneous messages are read in “real time” as they pour into the station, hour after hour, day after day, as the computer finds intelligence needles in telecommunications haystacks.

SOMEONE IS LISTENING: The computers in stations around the globe are known, within the network, as the ECHELON Dictionaries. Computers that can automatically search through traffic for keywords have existed since at least the 1970s, but the ECHELON system was designed by NSA to interconnect all these computers and allow the stations to function as components of an integrated whole. The NSA and GCSB are bound together under the 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 the world’s business occurring by fax, e-mail, and phone, spying on these communications receives the bulk of intelligence resources. For decades before the introduction of the ECHELON system, the UKUSA allies did intelligence collection operations for each other, but each agency usually processed and analyzed the intercept 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, the 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 headquarters of the agency concerned. No one in New Zealand screens, or even sees, the intelligence collected by the New Zealand station for the foreign agencies. Thus, the stations of the junior UKUSA allies function for the NSA no differently than if they were overtly NSA-run bases located on their soil.

The first component of the ECHELON network are stations specifically targeted on the international telecommunications satellites (Intelsats) used by the telephone 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 the Atlantic, Europe, and, inclined almost to the horizon, the 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 the ECHELON network, allowing analysts to recognize at which station the interception occurred.

New Zealand intelligence staff has been closely involved with the NSA's Yakima station since 1981, when NSA pushed the 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 the Waihopai station in 1989, its share of the Japanese communications was intercepted at Yakima and sent unprocessed to the GCSB headquarters in Wellington for decryption, translation, and writing into UKUSA-format intelligence reports (the NSA provides the codebreaking programs).

"COMMUNICATION" THROUGH SATELLITES: The next component of the ECHELON system intercepts a range of satellite communications not carried by Intelsat.In addition to the UKUSA stations targeting Intelsat satellites, there are another five or more stations homing in on Russian and other regional communications satellites. These stations are Menwith Hill in northern England; Shoal Bay, outside Darwin in northern Australia (which targets Indonesian satellites); Leitrim, just south of Ottawa in Canada (which appears to intercept Latin American satellites); Bad Aibling in Germany; and Misawa in northern Japan.

A group of facilities that tap directly into land-based telecommunications systems is the final element of the ECHELON system. Besides satellite and radio, the other main method of transmitting large quantities of public, business, and government communications is a combination of water cables under the oceans and microwave networks over land. Heavy cables, laid across seabeds between countries, account for much of the world's international communications. After they come out of the water and join land-based microwave networks they are very vulnerable to interception. The microwave networks are made up of chains of

microwave towers relaying messages from hilltop to hilltop (always in line of sight) across the countryside. These networks shunt large quantities of communications across a country. Interception of them gives access to international undersea communications (once they surface) and to international communication trunk lines across continents. They are also an obvious target for large-scale interception of domestic communications.

Because the facilities required to intercept radio and satellite communications use large aerials and dishes that are difficult to hide for too long, that network is reasonably well documented. But all that is required to intercept land-based communication networks is a building situated along the microwave route or a hidden cable running underground from the legitimate network into some anonymous building, possibly far removed. Although it sounds technically very difficult, microwave interception from space by United States spy satellites also occurs.4 The worldwide network of facilities to intercept these communications is largely undocumented, and because New Zealand's GCSB does not participate in this type of interception, my inside sources could not help either.

NO ONE IS SAFE FROM A MICROWAVE: A 1994 expos of the Canadian UKUSA agency, Spyworld, co-authored by one of its former staff, Mike Frost, gave the first insights into how a lot of foreign microwave interception is done (see p. 18). It described UKUSA "embassy collection" operations, where sophisticated receivers and processors are secretly transported to their countries' overseas embassies in diplomatic bags and used to monitor various communications in foreign capitals.

Since most countries' microwave networks converge on the capital city, embassy buildings can be an ideal site. Protected by diplomatic privilege, they allow interception in the heart of the target country. *6 The Canadian embassy collection was requested by the NSA to fill gaps in the American and British embassy collection operations, which were still occurring in many capitals around the world when Frost left the CSE in 1990. Separate sources in Australia have revealed that the DSD also engages in embassy collection. On the territory of UKUSA nations, the interception of land-based telecommunications appears to be done at special secret intelligence facilities. The US, UK, and Canada are geographically well placed to intercept the large amounts of the world's communications that cross their territories.

The only public reference to the Dictionary system anywhere in the world was in relation to one of these facilities, run by the GCHQ in central London. In 1991, a former British GCHQ official spoke anonymously to Granada Television's World in Action about the agency's abuses of power. He told the program about an anonymous red brick building at 8 Palmer Street where GCHQ secretly intercepts every telex which passes into, out of, or through London, feeding them into powerful computers with a program known as "Dictionary." The operation, he explained, is staffed by carefully vetted British Telecom people: "It's nothing to do with national security. It's because it's not legal to take every single telex. And they take everything: the embassies, all the business deals, even the birthday greetings, they take everything. They feed it into the Dictionary." What the documentary did not reveal is that Dictionary is not just a British system; it is UKUSA-wide.

Similarly, British researcher Duncan Campbell has described how the US Menwith Hill station in Britain taps directly into the British Telecom microwave network, which has actually been designed with several major microwave links converging on an isolated tower connected underground into the station.

The NSA Menwith Hill station, with 22 satellite terminals and more than 4.9 acres of

buildings, is undoubtedly the largest and most powerful in the UKUSA network. Located in northern England, several thousand kilometers from the Persian Gulf, it was awarded the NSA's "Station of the Year" prize for 1991 after its role in the Gulf War. Menwith Hill assists in the interception of microwave communications in another way as well, by serving as a ground station for US electronic spy satellites. These intercept microwave trunk lines and short range communications such as military radios and walkie talkies. Other ground stations where the satellites' information is fed into the global network are Pine Gap, run by the CIA near Alice Springs in central Australia and the Bad Aibling station in Germany. Among them, the various stations and operations making up the ECHELON network tap into all the main components of the world's telecommunications networks. All of them, including a separate network of stations that intercepts long distance radio communications, have their own Dictionary computers connected into ECHELON.

In the early 1990s, opponents of the Menwith Hill station obtained large quantities of internal documents from the facility. Among the papers was a reference to an NSA computer system called Platform. The integration of all the UKUSA station computers into ECHELON probably occurred with the introduction of this system in the early 1980s. James Bamford wrote at that time about a new worldwide NSA computer network codenamed Platform "which will tie together 52 separate computer systems used throughout the world. Focal point, or `host environment,' for the massive network will be the NSA headquarters at Fort Meade. Among those included in Platform will be the British SIGINT organization, GCHQ."

LOOKING IN THE DICTIONARY: The Dictionary computers are connected via highly encrypted UKUSA communications that link back to computer data bases in the five agency headquarters. This is where all the intercepted messages selected by the Dictionaries end up. Each morning the specially "indoctrinated" signals intelligence analysts in Washington, Ottawa, Cheltenham, Canberra, and Wellington log on at their computer terminals and enter the Dictionary system. After keying in their security passwords, they reach a directory that lists the different categories of intercept available in the data bases, each with a four-digit code. For instance, 1911 might be Japanese diplomatic cables from Latin America (handled by the Canadian CSE), 3848 might be political communications from and about Nigeria, and 8182 might be any messages about distribution of encryption technology.

They select their subject category, get a "search result" showing how many messages have been caught in the ECHELON net on that subject, and then the day's work begins. Analysts scroll through screen after screen of intercepted faxes, e-mail messages, etc. and, whenever a message appears worth reporting on, they select it from the rest to work on. If it is not in English, it is translated and then written into the standard format of intelligence reports produced anywhere within the UKUSA network either in entirety as a "report," or as a summary or "gist."

INFORMATION CONTROL: A highly organized system has been developed to control what is being searched for by each station and who can have access to it. This is at the heart of ECHELON operations and works as follows.

The individual station's Dictionary computers do not simply have a long list of keywords to search for. And they do not send all the information into some huge database that participating agencies can dip into as they wish. It is much more controlled.

The search lists are organized into the same categories, referred to by the four digit numbers. Each agency decides its own categories according to its responsibilities for

producing intelligence for the network. For GCSB, this means South Pacific governments, Japanese diplomatic, Russian Antarctic activities, and so on.

The agency then works out about 10 to 50 keywords for selection in each category. The keywords include such things as names of people, ships, organizations, country names, and subject names. They also include the known telex and fax numbers and Internet addresses of any individuals, businesses, organizations, and government offices that are targets. These are generally written as part of the message text and so are easily recognized by the Dictionary computers.

The agencies also specify combinations of keywords to help sift out communications of interest. For example, they might search for diplomatic cables containing both the words "Santiago" and "aid," or cables containing the word "Santiago" but not "consul" (to avoid the masses of routine consular communications). It is these sets of words and numbers (and combinations), under a particular category, that get placed in the Dictionary computers. (Staff in the five agencies called Dictionary Managers enter and update the keyword search lists for each agency.)

The whole system, devised by the NSA, has been adopted completely by the other agencies. The Dictionary computers search through all the incoming messages and, whenever they encounter one with any of the agencies' keywords, they select it. At the same time, the computer automatically notes technical details such as the time and place of interception on the piece of intercept so that analysts reading it, in whichever agency it is going to, know where it came from, and what it is. Finally, the computer writes the four-digit code (for the category with the keywords in that message) at the bottom of the message's text. This is important. It means that when all the intercepted messages end up together in the database at one of the agency headquarters, the messages on a particular subject can be located again. Later, when the analyst using the Dictionary system selects the four- digit code for the category he or she wants, the computer simply searches through all the messages in the database for the ones which have been tagged with that number.

This system is very effective for controlling which agencies can get what from the global network because each agency only gets the intelligence out of the ECHELON system from its own numbers. It does not have any access to the raw intelligence coming out of the system to the other agencies. For example, although most of the GCSB's intelligence production is primarily to serve the UKUSA alliance, New Zealand does not have access to the whole ECHELON network. The access it does have is strictly controlled. A New Zealand intelligence officer explained: "The agencies can all apply for numbers on each other's Dictionaries. The hardest to deal with are the Americans. … [There are] more hoops to jump through, unless it is in their interest, in which case they'll do it for you."

There is only one agency which, by virtue of its size and role within the alliance, will have access to the full potential of the ECHELON system the agency that set it up. What is the system used for? Anyone listening to official "discussion" of intelligence could be forgiven for thinking that, since the end of the Cold War, the key targets of the massive UKUSA intelligence machine are terrorism, weapons proliferation, and economic intelligence. The idea that economic intelligence has become very important, in particular, has been carefully cultivated by intelligence agencies intent on preserving their post-Cold War budgets. It has become an article of faith in much discussion of intelligence. However, I have found no evidence that these are now the primary concerns of organizations such as NSA.

QUICKER INTELLIGENCE, SAME MISSION: A different story emerges after examining very detailed information I have been given about the intelligence New Zealand collects for the UKUSA allies and detailed descriptions of what is in the yards-deep intelligence reports New Zealand receives from its four allies each week. There is quite a lot of intelligence collected about potential terrorists, and there is quite a lot of economic intelligence, notably intensive monitoring of all the countries participating in GATT negotiations. But by far, the main priorities of the intelligence alliance continue to be political and military intelligence to assist the larger allies to pursue their interests around the world. Anyone and anything the particular governments are concerned about can become a target.

With capabilities so secret and so powerful, almost anything goes. For example, in June 1992, a group of current "highly placed intelligence operatives" from the British GCHQ spoke to the London Observer: "We feel we can no longer remain silent regarding that which we regard to be gross malpractice and negligence within the establishment in which we operate." They gave as examples GCHQ interception of three charitable organizations, including Amnesty International and Christian Aid. As the Observer reported: "At any time GCHQ is able to home in on their communications for a routine target request," the GCHQ source said. In the case of phone taps the procedure is known as Mantis. With telexes it is called Mayfly. By keying in a code relating to Third World aid, the source was able to demonstrate telex "fixes" on the three organizations. "It is then possible to key in a trigger word which enables us to home in on the telex communications whenever that word appears," he said. "And we can read a pre-determined number of characters either side of the keyword." Without actually naming it, this was a fairly precise description of how the ECHELON Dictionary system works. Again, what was not revealed in the publicity was that this is a UKUSA-wide system. The design of ECHELON means that the interception of these organizations could have occurred anywhere in the network, at any station where the GCHQ had requested that the four-digit code covering Third World aid be placed.

Note that these GCHQ officers mentioned that the system was being used for telephone calls. In New Zealand, ECHELON is used only to intercept written communications: fax, e-mail, and telex. The reason, according to intelligence staff, is that the agency does not have the staff to analyze large quantities of telephone conversations.

Mike Frost's expos of Canadian "embassy collection" operations described the NSA computers they used, called Oratory, that can "listen" to telephone calls and recognize when keywords are spoken. Just as we can recognize words spoken in all the different tones and accents we encounter, so too, according to Frost, can these computers. Telephone calls containing keywords are automatically extracted from the masses of other calls and recorded digitally on magnetic tapes for analysts back at agency headquarters. However, high volume voice recognition computers will be technically difficult to perfect, and my New Zealand-based sources could not confirm that this capability exists. But, if or when it is perfected, the implications would be immense. It would mean that the UKUSA agencies could use machines to search through all the international telephone calls in the world, in the same way that they do written messages. If this equipment exists for use in embassy collection, it will presumably be used in all the stations throughout the ECHELON network. It is yet to be confirmed how extensively telephone communications are being targeted by the ECHELON stations for the other agencies.

The easiest pickings for the ECHELON system are the individuals, organizations, and governments that do not use encryption. In New Zealand's area, for example, it has proved especially useful against already vulnerable South Pacific nations which do not use any

coding, even for government communications (all these communications of New Zealand's neighbors are supplied, unscreened, to its UKUSA allies). As a result of the revelations in my book, there is currently a project under way in the Pacific to promote and supply publicly available encryption software to vulnerable organizations such as democracy movements in countries with repressive governments. This is one practical way of curbing illegitimate uses of the ECHELON capabilities.

One final comment. All the newspapers, commentators, and "well placed sources" told the public that New Zealand was cut off from US intelligence in the mid-1980s. That was entirely untrue. The intelligence supply to New Zealand did not stop, and instead, the decade since has been a period of increased integration of New Zealand into the US system. Virtually everything the equipment, manuals, ways of operating, jargon, codes, and so on, used in the GCSB continues to be imported entirely from the larger allies (in practice, usually the NSA). As with the Australian and Canadian agencies, most of the priorities continue to come from the US, too.

The main thing that protects these agencies from change is their secrecy. On the day my book arrived in the book shops, without prior publicity, there was an all-day meeting of the intelligence bureaucrats in the prime minister's department trying to decide if they could prevent it from being distributed. They eventually concluded, sensibly, that the political costs were too high. It is understandable that they were so agitated.

Throughout my research, I have faced official denials or governments refusing to comment on publicity about intelligence activities. Given the pervasive atmosphere of secrecy and stonewalling, it is always hard for the public to judge what is fact, what is speculation, and what is paranoia. Thus, in uncovering New Zealand's role in the NSA-led alliance, my aim was to provide so much detail about the operations the technical systems, the daily work of individual staff members, and even the rooms in which they work inside intelligence facilities that readers could feel confident that they were getting close to the truth. I hope the information leaked by intelligence staff in New Zealand about UKUSA and its systems such as ECHELON will help lead to change.

Articles by: **Nicky Hagar**