# Inside Echelon

## By Duncan Campbell

*Heise Online*
**July 25, 2000**

The history, structure and function of the global surveillance system known as Echelon

Since 1998, much has been written and spoken about the so-called Echelon system of international communications surveillance. Most of what has been written has been denied or ignored by US and European authorities. But much of what has been written has also been exaggerated or wrong. Amongst a sea of denials, obfuscations and errors, confusion has reigned. This review by Duncan Campbell, author of the European Parliament's 1999 "Interception Capabilities 2000" report[1] , is intended to help clear up the confusion, to say what Echelon is (and isn't), where it came from and what it does. Echelon, or systems like it, will be with us a long time to come.

Echelon is a system used by the United States National Security Agency (NSA) to intercept and process international communications passing via communications satellites. It is one part of a global surveillance systems that is now over 50 years old. Other parts of the same system intercept messages from the Internet, from undersea cables, from radio transmissions, from secret equipment installed inside embassies, or use orbiting satellites to monitor signals anywhere on the earth's surface. The system includes stations run by Britain, Canada, Australia and New Zealand, in addition to those operated by the United States. Although some Australian and British stations do the same job as America's Echelon sites, they are not necessarily called "Echelon" stations. But they all form part of the same integrated global network using the same equipment and methods to extract information and intelligence illicitly from millions of messages every day, all over the world.

The first reports about Echelon in Europe[2] credited it with the capacity to intercept "within Europe, all e-mail, telephone, and fax communications". This has proven to be erroneous; neither Echelon nor the signals intelligence ("sigint") system of which it is part can do this. Nor is equipment available with the capacity to process and recognise the content of every speech message or telephone call. But the American and British-run network can, with sister stations, access and process most of the worlds satellite communications, automatically analysing and relaying it to customers who may be continents away.

The world's most secret electronic surveillance system has its main origin in the conflicts of the Second World War. In a deeper sense, it results from the invention of radio and the fundamental nature of telecommunications. The creation of radio permitted governments and other communicators to pass messages to receivers over transcontinental distances. But there was a penalty - anyone else could listen in. Previously, written messages were physically secure (unless the courier carrying them was ambushed, or a spy compromised communications). The invention of radio thus created a new importance for cryptography, the art and science of making secret codes. It also led to the business of signals intelligence, now an industrial scale activity. Although the largest surveillance network is run by the US NSA, it is far from alone. Russia, China, France and other nations operate worldwide networks. Dozens of advanced nations use sigint as a key source of intelligence. Even smaller European nations such as Denmark, the Netherlands or Switzerland have recently constructed small, Echelon-like stations to obtain and process intelligence by eavesdropping on civil satellite communications.

During the 20th century, governments realised the importance of effective secret codes. But they were often far from successful. During the Second World War, huge allied codebreaking establishments in Britain and America analysed and read hundreds of thousands of German and Japanese signals. What they did and how they did it remained a cloely-guarded secret for decades afterwards. In the intervening period, the US and British sigint agencies, NSA and Government Communications Headquarters (GCHQ) constructed their worldwide listening network.

The system was established under a secret 1947 "UKUSA Agreement," which brought together the British and American systems, personnel and stations. To this was soon joined the networks of three British commonwealth countries, Canada, Australia and New Zealand. Later, other countries including Norway, Denmark, Germany and Turkey signed secret sigint agreements with the United States and became "third parties" participants in the UKUSA network.

Besides integrating their stations, each country appoints senior officials to work as liaison staff at the others' headquarters. The United States operates a Special US Liaison Office (SUSLO) in London and Cheltenham, while a SUKLO official from GCHQ has his own suite of offices inside NSA headquarters at Fort Meade, between Washington and Baltimore.

Under the UKUSA agreement, the five main English-speaking countries took responsibility for overseeing surveillance in different parts of the globe[3] . Britain's zone included Africa and Europe, east to the Ural Mountains of the former USSR; Canada covered northern latitudes and polar regions; Australia covered Oceania. The agreement prescribed common procedures, targets, equipment and methods that the sigint agencies would use. Among them were international regulations for sigint security[4] , which required that before anyone was admitted to knowledge of the arrangements for obtaining and handling sigint, they must first undertake a lifelong commitment to secrecy. Every individual joining a UKUSA sigint organisation must be "indoctrinated" and, often "re-indoctrinated" each time they are admitted to knowledge of a specific project. They are told only what they "need to know", and that the need for total secrecy about their work "never ceases".

Everything produced in the sigint organisations is marked by hundreds of special codewords that "compartmentalise" knowledge of intercepted communications and the systems used to intercept them. The basic level, which is effectively a higher classification than "Top Secret" is "Top Secret Umbra". More highly classified documents are identified as "Umbra Gamma"; other codewords can be added to restrict circulation still further. Less sensitive information, such as analyses of telecommunications traffic, may be classified "Secret Spoke".

The scale and significance of the global surveillance system has been transformed since 1980. The arrival of low cost wideband international communications has created a wired world. But few people are aware that the first global wide area network (WAN) was not the internet, but the international network connecting sigint stations and processing centres. The network is connected over transoceanic cables and space links. Most of the capacity of the American and British military communications satellites, Milstar and Skynet, is devoted to relaying intelligence information. It was not until the mid 1990s that the public internet became larger than the secret internet that connects surveillance stations. Britain's sigint agency GCHQ now openly boasts on its web site that it helps operate "one of the largest WANs [Wide Area Networks} in the world" and that "all GCHQ systems are linked together on the largest LAN in Europe ... connected to other sites around the world". The same pages also claim that "the immense size and sheer power of GCHQ's supercomputing architecture is difficult to imagine".

The UKUSA alliance's wide area network is engineered according to the same principles as the internet[5] , and provides access from all field interception stations to and from NSA's central computer system, known as Platform. Other parts of the system are known as Embroidery, Tideway and Oceanfront. The intelligence news network is Newsdealer. A TV conference system, highly encrypted like every other part of the network, is called Gigster. They are supported by applications known as Preppy and Droopy. NSA's e-mail system looks and feels like everybody else's e-mail, but is completely separate from the public network. Messages addressed to its secret internal internet address, which is simply "nsa", will not get through.

The delivery of NSA intelligence also now looks and feels like using the internet. Authorised users with appropriate permissions to access "Special Compartmented Intelligence"[6] use standard web browsers to look at the output of NSA's Operations Department from afar. The system, known as "Intelink", is run from the NSA's Fort Meade HQ. Completed in 1996, Intelink connects 13 different US intelligence agencies and some allied agencies with the aim of providing instant access to all types of intelligence information. Just like logging onto the world wide web, intelligence analysts and military personnel can view an atlas on Intelink's home page, and then click on any country they choose in order to access intelligence reports, video clips, satellite photos, databases and status reports.[7]

In the early post war years, and for the next quarter century, there was little sign of this automation or sophistication. In those years, most of the world's long distance communications - civil, military or diplomatic - passed by high frequency radio. NSA and its collaborators operated hundreds of remote interception sites, both surrounding the Soviet Union and China and scattered around the world. Inside windowless buildings, teams of intercept operators passed long shifts listening into silence, interspersed with sudden periods of frenetic activity. For the listening bases on the front line of the cold war, monitoring military radio messages during the cold war brought considerable stress. Operators at such bases often recall colleagues breaking down under the tension, perhaps fleeing into closets after believing that they had just intercepted a message marking the beginning of global thermonuclear war.

The Second World War left Britain's agency GCHQ with an extensive network of sigint outposts. Many were fixed in Britain, while others were scattered around the then Empire. From stations including Bermuda, Ascension, Cyprus, Gibraltar, Iraq, Singapore, and Hong Kong, radio operators tracked Soviet and, soon, Chinese political and military developments. These stations complemented a US network which by 1960 included thousands of continuously operated interception positions. The other members of the UKUSA alliance, Australia, Canada and New Zealand contributed stations in the South Pacific and arctic regions.

After the signing of the UKUSA pact, a new chain of stations began operating along the boundaries of the western sphere of influence, monitoring the signals of Soviet ground and air forces. British sigint outposts were established in Germany and, secretly in Austria and Iran. US listening posts were set up in central and southern Germany and later in Turkey, Italy and Spain. One major US sigint base - Kagnew Station at Asmara in Eritrea - was taken over from the British in 1941 and grew to become, until its closure in 1970, one of the largest intercept stations in the world. One of its more spectacular features was a tracking dish used to pass messages to the United States by reflecting them off the surface of the moon.

By the mid 1960s, many of these bases featured gigantic antenna systems that could monitor every HF (High Frequency) radio message, from all angles, while simultaneously obtaining bearings that could enable the position of a transmitter to be located. Both the US Navy and the US Air Force employed global networks of this kind. The US Air Force installed 500 metre wide arrays known as FLR-9 at sites including Chicksands, England, San Vito dei Normanni in Italy, Karamursel in Turkey, the Philippines, and at Misawa, Japan. Codenamed "Iron Horse", the first FLR-9 stations came into operation in 1964. The US Navy established similar bases in the US and at Rota, Spain, Bremerhaven, Germany, Edzell, Scotland, Guam, and later in Puerto Rico, targetted on Cuba.

When the United States went to war in Vietnam, Australian and New Zealand operators in Singapore, Australia and elsewhere worked directly in support of the war. Britain; as a neutral country was not supposed to be involved. In practice, however British operators at the GCHQ intercept station no UKC201 at Little Sai Wan, Hong Kong monitored and reported on the North Vietnamese air defence networks while US B52 bombers attacked Hanoi and other North Vietnamese targets.

Since the end of the cold war, the history of some cold war signals intelligence operations have been declassified. At the US National Cryptologic Museum, run by NSA at its headquarters, the agency now openly acknowledges many of its cold war listening operations. It also describes the controversial use of ships and aircraft to penetrate or provoke military defences in operations that cost the lives of more than 100 of its staff. But another longstanding aspect of sigint operations remain unacknowledged. During the second world war as well as in the cold war and since, British and US intelligence agencies monitored the signals and broke the codes of allies and friends, as well as of civilians and commercial communications around the world. The diplomatic communications of every country were and are attacked.

The stations and methods were the same as for military targets. Within the intelligence agencies, the civilian target was known as "ILC". ILC stood for "International Leased Carrier", and referred to the private companies or telecommunications administrations operating or administrating long range undersea cables or radio stations. Some ILC circuits were rented to governments or large companies as permanent links. The majority were used for public telegraph, telex or telephone services.

Many details of the operation of the English-speaking sigint axis were revealed by two NSA defectors at a press conference held in Moscow on 6 September 1960. There, two NSA analysts, Bernon Mitchell and William Martin, told the world what NSA was doing:

*We know from working at NSA [that] the United States reads the secret communications of more than forty nations, including its own allies ... NSA keeps in operation more than 2000 manual intercept positions ... Both enciphered and plain text communications are monitored from almost every nation in the world, including the nations on whose soil the intercept bases are located.*

*New York Times, 7 September 1960.*

The revelations were reported in full in the US, but their impact was soon buried by security recriminations and accusations. Martin and Mitchell revealed that NSA's operations division included two key groups. One group covered the Soviet Union and its allies. The second analysis division was known as ALLO, standing for "all other [countries]". This part of NSA's production organisation was later renamed ROW, starting for "Rest of the World".

Thus, in 1965, while intercept operators at the NSA's Chicksands station in England focussed on the radio messages of Warsaw Pact air forces, their colleagues 200 kilometres north at Kirknewton, Scotland were covering "ILC" traffic, including commercially run radio links between major European cities. These networks could carry anything from birthday telegrams to detailed economic or commercial information exchanged by companies, to encrypted diplomatic messages. In the intercept rooms, machines tuned to transmission channels continuously spewed out 8-ply paper to be read and marked up by intelligence analysts. Around the world, thousands of analysts worked on these mostly unencrypted communications using NSA 'watch lists' - weekly key word lists of people, companies, commodities of interest for the NSA watchers to single out from 'clear' traffic. Coded messages were passed on immediately. Among the regular names on the watch lists were the leaders of African guerrilla movements who were later to become their countries' leaders. In time, many prominent Americans were added to the list. The international communications of the actress Jane Fonda, Dr Benjamin Spock and hundreds of others were put under surveillance because of their opposition to the war in Vietnam. Black power leader Eldridge Cleaver and his colleagues were included because of their civil rights activities in the US.

A short distance to the north at Cupar, Scotland, another intercept station was operated by the British Post Office, and masqueraded as a long distance radio station. In fact, it was another GCHQ interception site, which collected European countries' communications, instead of sending them.

In time, these operations were integrated. In 1976, NSA set up a special new civilian unit at its Chicksands base to carry out diplomatic and civilian interception. The unit, called "DODJOCC" (Department of Defense Joint Operations Centre Chicksands) was targeted on non-US Diplomatic Communications, known as NDC. One specific target, known as FRD, stood for French diplomatic traffic. Italian diplomatic signals, known similarly as ITD, were collected and broken by NSA's counterpart agency GCHQ, at its Cheltenham centre.

Entering Chicksands' Building 600 through double security fences and a turnstile where green and purple clearance badges were checked, the visitor would first encounter a sigint in-joke - a copy of the International Telecommunications Convention pasted up on the wall. Article 22 of the Convention, which both the United Kingdom and the United States have ratified, promises that member states "agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence".

Besides intercepting ILC communications at radio stations, NSA, GCHQ and their counterparts also collected printed copies of all international telegrams from public and commercial operators in London, New York and other centres. They were then taken to sigint analysts and processed in the same way as foreign telegrams snatched from the air at sites like Chicksands and Kirknewton. Britain had done this since 1920, and the United States since 1945. The joint programme was known as Operation Shamrock, and continued until it was exposed by US Congressional intelligence investigations in the wake of the Watergate affair.

On 8 August 1975, NSA Director Lt General Lew Allen admitted to the Pike Committee of the US House of Representatives that : "NSA systematically intercepts international communications, both voice and cable" He also admitted that "messages to and from American citizens have been picked up in the course of gathering foreign intelligence". At a later hearing, he described how NSA used "'watch lists" an aid to watch for foreign activity of reportable intelligence interest". [8]

US legislators considered that these operations might have been unconstitutional. During 1976, a Department of Justice team investigated possible criminal offences by NSA. Part of their report was released in 1980. It described how intelligence on US citizens, known as MINARET "was obtained *incidentally* in the course of NSA's interception of aural and non-aural (e.g, telex) international communications and the receipt of GCHQ-acquired telex and ILC (International Leased Carrier) cable traffic (SHAMROCK)" (emphasis in original).

As in the United Kingdom, from 1945 onwards NSA and its predecessors had systematically obtained cable traffic from the offices of major cable companies - RCA Global, ITT World Communications and Western Union. Over time, the collection of copies of telegrams on paper was replaced by the delivery of magnetic tapes and eventually by direct connection of the monitoring centres to international communications circuits. In Britain, all international telex links and telegram circuits passing in, out or through the country were and are connected to a GCHQ monitoring site in central London, known as UKC1000.

By the early 1970s, the laborious process of scanning paper printouts for names or terms appearing on the "watch lists" had begun to be replaced by automated computer systems. These computers performed a task essentially similar to the search engines of the internet. Prompted with a word, phrase or combination of words, they will identify all messages containing the desired words or phrases. Their job, now performed on a huge scale, is to match the "key words" or phrases of interest to intelligence agencies to the huge volume of international communications, to extract them and pass them to where they are wanted. During the 1980s, the NSA developed a "fast data finder" microprocessor that was optimally designed for this purpose. It was later commercially marketed, with claims that it "the most comprehensive character-string comparison functions of any text retrieval system in the world". A single unit could work with:

*trillions of bytes of textual archive and thousands of online users, or gigabytes of live data stream per day that are filtered against tens of thousands of complex interest profiles"*[9] .

Although different systems are in use, the key computer system at the heart of a modern sigint station's processing operations is the "Dictionary". Every Echelon or Echelon-like station contains a Dictionary. Portable versions are even available, and can be loaded into briefcase-sized units known as "Oratory" [10] . The Dictionary computers scan communications input to them, and extract for reporting and further analysis those that match the profiles of interest. In one sense, the main function of Dictionary computers are to throw most intercepted information away.

In a 1992 speech on information management, former NSA Director William Studeman described the type of filtering involved in systems like ECHELON [11] :

*One [unidentified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence".*

In other words, for every million communications intercepted only one might result in action by an intelligence agency. Only one in a thousand would ever be seen by human eyes.

Supporting the operations of each Dictionary are gigantic intelligence databases which contain tables of information related to each target. At their simplest, these can be a list of telephone, mobile phone, fax or pager numbers which associated with targets in each group. They can include physical or e-mail addresses, names, or any type of phrase or concept that can be formulated under normal information retrieval rules.

Powerful though Dictionary methods and keyword search engines may be, however, they and their giant associated intelligence databases may soon be replaced by "topic analysis", a more powerful and intuitive technique, and one that NSA is developing strongly. Topic analysis enables Comint customers to ask their computers to "find me documents about subject X". X might be "Shakespeare in love" or "Arms to Iran".

In a standard US test used to evaluate topic analysis systems, one task the analysis program is given is to find information about "Airbus subsidies". The traditional approach involves supplying the computer with the key terms, other relevant data, and synonyms. In this example, the designations A-300 or A-320 might be synonymous with "Airbus". The disadvantage of this approach is that it may find irrelevant intelligence (for example, reports about export subsidies to goods flown on an Airbus) and miss relevant material (for example a financial analysis of a company in the consortium which does not mention the Airbus product by name). Topic analysis overcomes this and is better matched to human intelligence.

In 1991, a British television programme reported on the operations of one Dictionary computer at GCHQ's London station in Palmer Street, Westminster (station UKC1000). The programme quoted GCHQ employees, who spoke off the record:

*Up on the fourth floor there, [GCHQ] has hired a group of carefully vetted British Telecom people. [Quoting the ex-GCHQ official:] 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."*

Among the targets of this station were politicians, diplomats, businessmen, trades union leaders, non- government organisations like Amnesty International, and even the hierarchy of the Catholic church.

The Echelon system appears to have been in existence since the early 1970s, and to have gone through extensive evolution and development. The need for efficient processing systems to replace the human operators who performed watch list scans was first foreseen in the late 1960s, when NSA and GCHQ were planning the first large satellite interception sites. The first such station was built at Morwenstow, Cornwall, and utilised two large dish antennae to intercept communications crossing the Atlantic and Indian Oceans. The second was built at Yakima, in the northwestern US state of Washington. Yakima intercepted satellite communications over the Pacific Ocean.

Also in the early 1970s, NSA and CIA discovered that sigint collection from space was far more effective and productive than had been foreseen, resulting in vast accumulations of magnetic tapes that quickly outstripped the available supply of Soviet linguists and analysts. By the end of the 1970s, one of the main sites processing communications intercepted from space was Menwith Hill, in central England. A document prepared there in 1981[12] identifies intelligence databases used at Menwith Hill as "Echelon 2". This suggests that the Echelon network was already into its second generation by 1981.

By the mid 1980s, communications handled by Dictionary computers around the world were heavily sifted, with a wide variety of specifications available for non-verbal traffic. Extensive further automation was planned in the mid 1980s under two top secret NSA Projects, P-377 and P-415. The implementation of these projects completed the automation of the "watch list" activity of pevious decades. Computers replaced the analysts who compared reams of paper intercepts to names and topics on the watch list. In the late 1980s, staff from sigint agencies from countries including the UK, New Zealand and China attended training courses on the new Echelon computer systems.

Project P-415 made heavy use of NSA and GCHQ's global internet to enable remote intelligence customers to task computers at each collection site, and then receive the results automatically. Selected incoming messages were compared to forwarding criteria held on the Dictionary. If a match was found, the raw intelligence was forwarded automatically to the designated recipients. According to New Zealand author Nicky Hager, [13] Dictionary computers are tasked with many thousands of different collection requirements, described as "numbers" (four digit codes).

Details of project P-415 and the plans for the massive global expansion of the Echelon system were revealed in 1988 by Margaret "Peg" Newsham. Ms Newsham a former computer systems manager, worked on classified projects for NSA contractors until the mid 1980s. From August 1978 onwards, she worked at the NSA's Menwith Hill Station as a software co-ordinator. In this capacity, she helped managed a number of Sigint computer databases, including "Echelon 2". She and others also helped establish "Silkworth", a system for processing information relayed from signals intelligence satellites called Chalet, Vortex and Mercury. Her revelations led to the first ever report about Echelon, published in 1988. [14]

In Sunnyvale, California, Peg Newsham worked for Lockheed Space and Missiles Corporation. In that capacity, she worked on plans for the massive expansion of the Echelon network, a project identified internally as P-415. During her employment by Lockheed, she also become concerned about corruption, fraud and abuse within the organisations planning and operating electronic surveillance systems. She reported her concerns to the US Congress House Permanent Select Committee on Intelligence early in 1988. She also told them how she had witnessed the interception of a telephone call made by a US Senator, Strom Thurmond, while working at Menwith Hill.

The full details of Echelon would probably never have come to serious public attention but for 6 further years of research by New Zealand writer Nicky Hager, who assiduously investigated the new Echelon station that started operating at Waihopai on the South Island of New Zealand in 1989. His 1996 book *Secret Power*[15] is based on extensive interviews with and help from members of the New Zealand signals intelligence organisation. It remains the best informed and most detailed account of how Echelon works.

Early in 2000, information and documents leaked to a US researcher [16] provided many details of how Echelon was developed for use worldwide. Under a 1982 NSA plan assigned to Lockheed Space and Missiles Systems, engineers and scientists worked on Project P-377 - also known as CARBOY II. This project called for the development of a standard kit of "ADPE" (automated data processing equipment) parts for equipping Echelon sites. The "commonality of automated data processing equipment (ADPE) in the Echelon system" included the following elements:

- Local management subsystem
- Remote management subsystem
- Radio frequency distribution
- Communications handling subsystem
- Telegraphy message processing subsystem
- Frequency division multiplex telegraphy processing subsystem
- Time division multiplex telegraphy processing subsystem
- Voice processing subsystem
- Voice collection module
- Facsimile processing subsystem
- [Voice] Tape Production Facility

The CARBOY II project also called for software systems to load and update the Dictionary databases. At this time, the hardware for the Dictionary processing subsystem was based on a cluster of DEC VAX mini-computers, together with special purpose units for processing and separating different types of satellite communications.

In 1998 and 1999, the intelligence specialist Dr Jeff Richelson of the National Security Archive [17] Washington, DC used the Freedom of Information Act to obtain a series of modern official US Navy and Air Force documents which have confirmed the continued existence, scale and expansion of the Echelon system. The documents from the US Air Force and US Navy identify Echelon units at four sites and suggest that a fifth site also collects information from communications satellites as part of the Echelon system.

One of the sites is Sugar Grove, West Virgina US, about 250 miles south-west of Washington in a remote area of the Shenandoah Mountains. It is operated by the US Naval Security Group and the US Air Force Intelligence Agency. An upgraded sigint system called Timberline II was installed at Sugar Grove in the summer of 1990. At the same time, according to official US documents, an "Echelon training department" was established. With training complete, the task of the station in 1991 became "to maintain and operate an ECHELON site". [18]

The US Air Force has publicly identified the intelligence activity at Sugar Grove as "to direct satellite communications equipment [in support of] consumers of COMSAT information ... this is achieved by providing a trained cadre of collection system operators, analysts and managers". The 1998-99 USAF Air Intelligence Agency Almanac described the mission of the Sugar Grove unit as providing "enhanced intelligence support to air force operational commanders and other consumers of COMSAT information." [19] In 1990, satellite photographs showed that there were 4 satellite antennae at Sugar Grove. By November 1998, ground inspection revealed that this had expanded to nine.

Further information published by the US Air Force identifies the US Naval Security Group Station at Sabana Seca, Puerto Rico as a COMSAT interception site. Its mission is "to become the premier satellite communications processing and analysis field station". These and further documents concerning Echelon and COMSAT interception stations at Yakima, Sabana Seco (Puerto Rico), Misawa (Japan) and Guam have been published on the web. [20]

From 1984 onwards, Australia, Canada and New Zealand joined the US and the UK in operating Comsat (communications satellite) interception stations. Australia's site at Kojarena, Geraldton near Perth in western Australia includes four interception dishes. The station's top targets include Japanese diplomatic and commercial messages, communications of all types from and within North Korea, and data on Indian and Pakistani nuclear weapons developments. A second Australian satcom intercept site, at Shoal Bay in the Northern Territories, mainly targets Australia's northern neighbour, Indonesia. Australian sources say however that Shoal Bay is not part of the Echelon system, as Australia is unwilling to allow the US and Britain to obtain raw intercepts directly.

The New Zealand site, Waihopai now has two dishes targeted on Intelsat satellites covering the south Pacific. In 1996, shortly after *"Secret Power"* was published, a New Zealand TV station obtained images of the inside of the station's operations centre. The pictures were obtained clandestinely by filming through partially curtained windows at night. The TV reporter was able to film close-ups of technical manuals held in the control centre. These were Intelsat technical manuals, providing confirmation that the station targeted these satellites. Strikingly, the station was seen to be virtually empty, operating fully automatically.

Before the introduction of Echelon, different countries and different stations knew what was being intercepted and to whom it was being sent. Now, all but a fraction of the messages selected by Dictionary computers at remote sites may be forwarded to overseas customers, normally NSA, without any local knowledge of the intelligence obtained.

Information from the Echelon network and other parts of the global surveillance system is used by the US and its allies for diplomatic, military and commercial purposes. In the post cold war years, the staff levels at both NSA and GCHQ have contracted, and many overseas listening posts have been closed or replaced by Remote Operations Facilities, controlled from a handful of major field stations. Although routinely denied, commercial and economic intelligence is now a major target of international sigint activity. Under a 1993 policy colloquially known as "levelling the playing field", the United States government under President Clinton established new trade and economic committees and told the NSA and CIA to act in support of US businesses in seeking contracts abroad. In the UK, GCHQ's enabling legislation from 1994 openly identifies one of its purposes as to promote "the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands".

Massive new storage and processing systems are being constructed to provide on-line processing of the internet and new international communications networks. By the early 1990s, both GCHQ and NSA employed "near line" storage systems capable of holding more than a terabyte of data[21] . In the near future, they are likely to deploy systems one thousand times larger. Key word spotting in the vast volumes of intercepted daily written communications - telex, e-mail, and data - is a routine task. "Word spotting" in spoken communications is not an effective tool, but individual speaker recognition techniques have been in use for up to 10 years. New methods which have been developed during the 1990s will become available to recognise the "topics" of phone calls, and may allow NSA and its collaborators to automate the processing of the content of telephone messages - a goal that has eluded them for 30 years.

Under the rubric of "information warfare", the sigint agencies also hope to overcome the ever more extensive use of encryption by direct interference with and attacks on targeted computers. These methods remain controversial, but include information stealing viruses, software audio, video, and data bugs, and pre-emptive tampering with software or hardware ("trapdoors").

In the information age, we need to re-learn a lesson now a century old. Despite the sophistication of 21st century technology, today's e-mails are as open to the eyes of snoopers and intruders as were the first crude radio telegraph messages. Part of the reason for this is that, over many decades, NSA and its allies worked determinedly to limit and prevent the privacy of international telecommunications. Their goal was to keep communications unencrypted and, thus, open to easy access and processing by systems like Echelon. They knew that privacy and security, then as a century ago, lay in secret codes or encryption. Until such protections become effective and ubiquitous, Echelon or systems like it, will remain with us.

***Click here for a forum discussion on Echelon at Heise Online***

---

[1] ) Available from the European Parliament web site. The report is part of a series of four in a series on the "Development of surveillance technology and risk of abuse of economic information" The report contains a detailed technical account of how different types of communications are intercepted

Back

[2] ) "An appraisal of technologies of political control", report for the European Parliament Scientific and Technological Options office (STOA) by Dr Steve Wright, Omega Foundation, Manchester, UK, January 1998.

Back

[3] ) The arrangements are sometimes called "TEXTA Authority". TEXTA stands for "Technical Extracts of Traffic Analysis" and is in effect a voluminous listing of every communications source identified by each agency. It is catalogued and sorted by countries, users, networks, types of communications system and other features.

Back

[4] ) Called IRSIG

Back

[5] ) TCP/IP, or Transmission Control Protocol/Internet Protocol.

Back

[6] ) "SCI", also known as Special Intelligence, is secret intelligence for which codeword clearance is required. Special regulations also apply to offices in which SCI is examined. They must be physically secure and electromagnetically shielded. These offices are known as SCIFs (SCI Facilities).

Back

[7] ) The US intelligence intranet is described in "Top Secret Intranet: How U.S. Intelligence Built Intelink -- the world's largest, most secure network", by Frederick Martin (Prentice Hall, 1999)

Back

[8] ) *The National Security Agency and Fourth Amendment Rights*, Hearings before the Select Committee to Study Government Operations with Respect to Intelligence Activitities, US Senate, Washington, 1976.

Back

[9] ) By the Paracel Corporation, as the FDF "Textfinder". It claims to be the "fastest, most adaptive information filtering system in the world".

Back

[10] ) Oratory is described in "Spyworld", by Mike Frost and Michel Gratton, Doubleday Canada, 1994. It was used to select messages intercepted at clandestine embassy interception sites.

Back

[11] ) Address to the Symposium on "National Security and National Competitiveness : Open Source Solutions" by Vice Admiral William Studeman, Deputy Director of Central Intelligence and former director of NSA, 1 December 1992, McLean, Virginia.

Back

[12] ) See reference 1, above.

Back

[13] ) Secret Power, by Nicky Hager. Craig Potton Publishing, New Zealand, 1996.

Back

[14] ) New Statesman (UK), 12 August 1988. At the time, Ms Newsham was a confidential source of information and was not identified in the article. In February 2000, living in retirement and facing a serious illness, Ms Newsham, said that she could be identified as the original source of information on Echelon. She also appeared on a CBS television programme about Echelon, *Sixty Minutes* (shown on 27 February 2000).

Back

[15] ) See reference 16.

Back

[16] ) "Echelon P-377 Work Package for CARBOY II", published at http://cryptome.org/echelon-p377.htm

Back

[17] ) An independent organisation that, among other functions. catalogues US government documents obtained under Freedom of Information legislation.

Back

[18] ) Naval Security Group Command Regulation C5450.48A; see note 23.

Back

[19] ) "Desperately Seeking Signals", Jeff Richelson, *Bulletin of the Atomic Scientists*, March-April 2000.

Back

[20] ) The documents relating to Echelon stations can be found at the National Security Archive web site.

Back

[21] ) A million megabytes, or 10 $^{12}$ bytes.

Back

**More Information on Empire?**