EUROPEAN PARLIAMENT

TEMPORARY COMMITTEE ON THE ECHELON INTERCEPTION SYSTEM

DIRECTORATE-GENERAL FOR COMMITTEES AND DELEGATIONS

BRUSSELS MEETING, 22-23 JANUARY 2001

INTERCEPTION CAPABILITIES - IMPACT AND EXPLOITATION

Paper 1

Echelon and its role in COMINT

ECHELON AND ITS ROLE IN COMINT

1. Since the publication of the 1997 STOA report on the "Technology of Political Control" (TPC) and the 1998 STOA report "Interception Capabilities 2000" (IC2000), hundreds of pages of newspaper and magazine articles and many hours of television have been published and broadcast around the world concerning "Echelon". Very few of these reports have added original new information. The majority of reports have enlarged on the actual nature of interception systems and their capabilities in ways which are not supported by the original reports on which they purport to rely. These enlarged claims have often been distorted further by tertiary and other derivative reportage.

2. An inevitable consequence of this media phenomenon is that the nature of Echelon has been widely misunderstood and misreported. Essentially, the word now has two contexts. The first meaning is the strict and specific sense in which original writers have used it to refer to a sub-sub-component of the Signals Intelligence (Sigint) system run by the United States and its allies. Its secondary meanings are as a generic term for COMSAT intelligence collection, and/or for all Sigint, and/or for the English speaking signals intelligence alliance (UKUSA). In its extreme form, it has become a quasi-mythological icon for all forms of technological surveillance, and hence a focus for technophobic opposition to perceptions of uncontrolled state power. For example, we have had one internationally organised "Jam Echelon Day"; there may be more.[1]

3. The same multiple and enlarged meanings have also confused and misled detractors who have criticised the concerns expressed by some Europeans and by the European Parliament. Many of these responses, which have often been sneering and/or ill-informed in character, have been published in the U.S. press. With some exceptions, these criticisms have been directed at the highly enlarged and mainly mythical and unsourced accounts of its capabilities appearing in secondary or tertiary reporting. They are thus of as little value as the reporting that they attack.

4. It is appropriate to point out that the "IC2000" report which I wrote was <u>not</u> a report on Echelon. It was a report on Comint, and covered many other types of interception including from satellite platforms, land cables, on the seabed, by high frequency radio and so on.

5. In this report, I will use "Echelon" only in the strictest sense. I define this as follows:

   (i) Echelon stations are COMSAT interception sites, which used ground-based antennae to monitor downlinks from commercial communications satellites and process the received signals for intelligence purposes. They are part of an integrated international network;

   (ii) Echelon stations are run by some nations belonging to the five-nation UKUSA sigint alliance. However, not all COMSAT stations run by UKUSA countries are known as Echelon. Published documents indicate that stations in the U.S., Canada and New Zealand are called Echelon. The Australian government has stated that,

[1] One irony of "Jam Echelon Day" was that it displayed a deep misunderstanding of how Echelon and similar systems operate. The key component of such intelligence systems is filtering software intended to throw away most of the messages that are intercepted. Any standard message intended to "jam" the system by including a long list of supposed key words would in fact be readily identified as noise of no value, and could easily be discarded automatically.

while one of its COMSAT intercept stations (Geraldton) fully participates in what it is publicly known as the "Echelon network", the name Echelon is not used in Australia. There is no evidence as to whether or not the UK government calls its main COMSAT intercept station (at Morwenstow, Cornwall) by this or another name. Echelon stations are therefore only part of the COMSAT interception system of the UKUSA alliance.

(iii) COMSAT interception is only one of many methods used by UKUSA countries and agencies to intercept international and other communications. Intelligence can also be collected by tapping cables, by monitoring other radio signals, or by using satellites to intercept communications on the ground.

(iv) Besides the UKUSA nations, around 30 other countries have substantial sigint capabilities, including COMSAT interception. In this context, Echelon is therefore only one part – although an important part – of the risks to privacy or national or industrial security posed by global electronic suveillance.

6. In summary: "Echelon" is a code name given by the NSA (U.S. National Security Agency) to a system that collects and processes information derived from intercepting civil satellite communications. The information obtained at Echelon stations is fed into the global communications network operated jointly by the Sigint organisations of the United States, United Kingdom, Australia, Canada and New Zealand. Echelon stations operate automatically. Most of the information that is selected is automatically fed into the world-wide network of sigint stations.

7. A key feature of the Echelon system is that they use computer systems called "Dictionary". Dictionary computers are much more prevalent in Sigint or electronic surveillance systems than stations called Echelon. They perform the critical task of holding lists of intelligence targets and search criteria, matching them to customers requirements. They operate the filter systems. Dictionary computers thus hold full lists of general and specific targets, and the names of organisations who should receive such information when it is detected. [2]

The nature of UKUSA

This section focuses on questions put by the Committee.

8. **What is known about the existence of the UKUSA agreement?**

- The UKUSA security agreement has been officially acknowledged by participating governments in two member countries.
- In a May 1995 report, the Canadian Parliamentary Security and Intelligence committee stated
    - "Canada collaborates with some of its closest and long-standing allies in the exchange of foreign intelligence... These countries and the responsible agencies in each are the U.S. (National Security Agency), the U.K. (Government

[2] Nicky Hager, "Secret Power", Craig Potton Publishing, New Zealand, 1996

Communications Headquarters), Australia (Defence Signals Directorate), and New Zealand (Government Communications Security Branch (*sic – Communications Security Bureau*))"

- Canada has also published a number of official statements confirming basic aspects of the five power relationship. According to the Auditor-General, "CSE [the Communications Security Establishment] has access to allied SIGINT through reciprocal sharing agreements … Intelligence products, including analyses and assessments are exchanged, and technical assistance is provided by each to the others. These, and other relationships, provide Canada with information and technological resources that would otherwise be unobtainable with current resources".[3]

- In March 1999, the director of the Australian Sigint organisation, the Defence Signals Directorate (DSD) stated that DSD "does co-operate with counterpart signals intelligence organisations overseas **under the UKUSA relationship**. Both DSD and its counterparts operate internal procedures to satisfy themselves that their national interests and policies are respected by the others" (*emphasis added)* [4] This was the first occasion on which any UKUSA country had used the name officially. At the time, the Australian government privately anticipated that their revelation might upset "old-timers".[5]

- The agreement is also listed in an official publication of the U.S. Navy, where it is described as the "United Kingdom-USA (5-nation SIGINT agreement)" [6]

- Press reports and publications about the UKUSA agreement between 1975 and 1990 were based almost exclusively on interviews with former Sigint personnel, who reported that they had been told in initial briefings that the agreement dated from 1947. This is the date given, for example, by me in 1976[7] and Bamford in 1982.[8]

- Hager, in his detailed account of Echelon, says that the agreement is formally known as the United Kingdom – United States Security Agreement, and was signed in 1948.[9] Formally, it is an agreement only between the UK and the United States. However, at this time there was in being a British Commonwealth Sigint Organisation (CSO) providing arrangements for Britain's GCHQ to control Sigint stations in Canada, Australia and New Zealand. Hager says that the original bipartite agreement became a five-nation alliance as a result of additional protocols joining the three Commonwealth nations to the UK and the US. He states with conviction that this took place in 1948. He suggests that the reason for the discrepancy with earlier reports may be that the original two nation instrument was signed in 1947, but that the necessary further protocols were not completed until 1948. Many other secret intergovernmental security

---

[3] Auditor-General of Canada, Report on the Canadian Intelligence Commuinity – Control and Accountability", Ottawa, November 1996

[4] Statement by Martin Brady, Director of DSD, Canberra 16 March 1999. Issued to and broadcast on the *Sunday Programme*, Channel 9 TV (Australia), 11 April 1999

[5] Private communication

[6] "Terms/Abbreviations/Acronyms", published by the U.S. Nave and Marine Corps Intelligence Training Centre (NMITC), available at http://www.cnet.navy.mil/nmitc/training/u.html

[7] Duncan Campbell and Mark Hosenball, "The Eavesdroppers", *Time Out*, London, 22 May 1976

[8] James Bamford, "The Puzzle Palace", Sidgwick and Jackson , 1982.

[9] Nicky Hager, "Secret Power", Craig Potton Publishing, New Zealand, 1996, pps 61-62

agreements are known to date from about this time, such as CANUKUS and NZAUSCANUKUS. These may have implemented the protocols needed to supplement UKUSA.

- Richelson cites 1948 as the date of the agreement, although he gives no sources.[10] Andrew, in an academic work, says that the UKUSA agreement came fully into effect in June 1948, having been "initially negotiated" in March 1946.[11]

- The best summary that can be made at this time is that, as a five power agreement, the UKUSA agreement dates from 1948. But the two-nation initial agreement was negotiated in 1946 and may have been signed in 1947.

- The UKUSA agreement is not an international "treaty", although this misdescription commonly appears in print. Treaties are registered with the United Nations.

9. **Which countries signed the agreement?**

- The United Kingdom and the United States (see above)

10. **What is the content of this agreement?**

- The text of the UKUSA agreement remains secret and has never been published. However it has been identified as the direct successor to the BRUSA ("Britain-United States of America") agreement, dated 17 May 1943. The complete text of BRUSA, including its appendices, was released by NSA in 1995 and published two years later.[12] Many of its terms appear similar to those reportedly included in UKUSA.

- Under the UKUSA agreement, the five countries agreed that they would follow common procedures, and use the same target identification systems, equipment and methods. They would normally share raw Sigint as well as "end product" reports and analyses. There are unified security and operational procedures, including reporting.

- For example, each station in the UKUSA network, including ships, has a unique addresss consisting of letters and figures, and known as a SIGAD (Sigint Activity Designator). Within this system, for example, Menwith Hill in the UK is USD1000. All intercepted signals are described in a system of "case notation" which identifies the network being intercepted. An Iraqi army message would be denoted as IQM, followed by figures; intercepted French diplomatic messages are designated FRD. All output is called "serialised reporting", and is identified by a year, a production agency, a channel, and a serial number.

---

[10] Jeffrey Richelson, "The U.S. intelligence establishment", 4th edition, Westview Press, Colorado, 1999, p 293

[11] Christopher Andrew, "The Making of the Anglo-American SIGINT Alliance," in "In the Name of Intelligence: Essays in Honor of Walter Pforzheimer", eds. Hayden B. Peake and Samuel Halpern, NIBC Press, Washington D.C., 1994, pps 95-109

[12] "The BRUSA Agreement of May 17, 1943," *Cryptologia*, Vol 21, no. 1 (Jan. 1997): 30-38

11. **How is the surveillance network organised?**

- The agreement assigns responsibility for overseeing surveillance in different parts of the globe[13]. Britain's zone included Africa and Europe, east to the Ural Mountain; Canada covered northern latitudes and Polar regions; Australia covered Oceania. New Zealand monitors the south Pacific.

12. **What does "First", "Second" and "Third" parties mean?**

- Among the five powers, each national Sigint organisation refers to itself and its own material as "First Party". The four others are the Second Parties. These terms are commonly used in referring to the provenance (origin) of Sigint material. Material originated by one of the other four countries is called "Second Party". Sigint from any other source is called "Third Party".

- "First Party" thus means the Sigint organisation or country to which a given speaker or writer belongs.

- "Third Party" sigint material can be and is obtained *ad hoc* from other nations and sources outside the five power alliance. However, a number of non English-speaking countries have made security agreements for the exchange of Sigint raw material and end product reports. These arrangements are supplementary to the UKUSA five power arrangements and integrate, to a greater or lesser degree, the third parties into the UKUSA network. Acccording to Richelson,[14] ten countries have formally made "third party" agreements with the United States:

    - Norway
    - Denmark
    - Germany
    - Italy
    - Greece
    - Turkey
    - Austria
    - Japan
    - South Korea
    - Thailand

- The amount of information that is known publicly about these agreements is variable. Such information as is available suggests that most or all of the agreements are bilateral agreements with the United States, to which the UKUSA sigint agencies gain access under the UKUSA agreement and its associated protocols. Detailed information has been published about the two NORUSA agreements which created a SIGINT alliance between the U.S. and Norway. The first Norway – U.S. Communications Intelligence agreement was signed on 10 December 1954, and the second on 1 August 1979. By

[13] These arrangements are sometimes called "TEXTA Authority". TEXTA stands for "Technical Extracts of Traffic Analysis" and is 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, such as cryptosystems in use.
[14] Jeffrey Richelson, "The U.S. intelligence establishment", 4th edition, Westview Press, Colorado, 1999, p 293

1957, according to a recent study, Norwegian intelligence was delivering 1000 intercepts, 350 radio journals, 500 direction finding reports, and 4-5 tapes of intercepted voice signals every day to the U.S. embassy in Oslo, for passing on to NSA.[15]

- The Danish Sigint service, *Forsvarets Central Radio*, was also active at the same time, and fed the U.S. data from 8 stations located from Greenland to Bornholm. But U.S. payments to Denmark and Norway were cut off in 1992, resulting in extensive closures and job losses. At this time, these Scandinavian countries reportedly planned to move into COMSAT interception.[16]

- During the cold war, other nations are known to have had less formal arrangements for exchanging raw and finished Sigint and cryptologic information with NSA. These include Tawain, the Netherlands, Sweden and Finland. Although not included in this list, Spain also has security agreements with the United States, and continues to host one at least NSA Sigint base.[17]

- Within the Union, the countries not significantly involved in Sigint exchanges with the United States appear to be Belgium, Luxembourg, Portugal, Ireland and France. However, some recent reports have suggested that the NSA and France's DGSE do share cryptologic information and materials from time to time.

- If this information is accurate, then one nation in the 15 is a full member of UKUSA, five are Third Parties to UKUSA and three others (Spain, Sweden and Finland) have or have had Sigint arrangements with NSA or GCHQ. However, the significance of some Third Party arrangements in Europe may have abated since the end of the Cold War. For example, NSA is said to have discontinued payments to the Danish government in 1992.

- Canadian government policies also require CSE :

    - "to conduct their operational activities in strict recognition of, and adherence to, federal legislation governing the protection of the rights, privacy and freedoms of Canadians. The policies affirm CSE's commitment to respect the corresponding procedures of its close and longstanding allies, Australia, New Zealand, the United Kingdom and the United States (also known as the Second Parties). However, these procedures must conform first to the laws of Canada".[18]

    - "CSE undertakes explicitly to treat the communications of Second Party nationals in a manner consistent with the procedures issued by the agency of that country, provided such procedures do not convene the laws of Canada. This is a reciprocal undertaking to ensure that the Second Parties do not target each other's communications or circumvent their own legislation by targeting

---

[15] Alf Jakobsen, "Scandinavia, Sigint and the Cold War", in Conference on "Importance of Sigint in Western Europe in the Cold War", Amsterdam, 27 November 1999

[16] *Ibid*

[17] At Rota, near Cadiz. Rota is not believed to be an Echelon site.

[18] Annual report of the Communications Security Establishment Commissioner, 1997-1998, Ottawa, May 1998, p2

communications at each other's behest. In other words, they do not do indirectly what would be unlawful for them to do directly"[19]

13. **What is the function of liaison staff** ? **Does every Sigint station include staff from NSA?**

- Sigint staff may be appointed to liaison posts, or they may have reciprocal postings. In reciprocal postings, the staff assigned to a field station are employed on the same terms and within the same structures as local staff. Liaison officers, as the name implies, manage and organise bilateral relationships, either in headquarters organisations or in jointly run field stations.

- Each country appoints senior officials to work as liaison staff at the others' headquarters. Thus, the United States has offices for the Special U.S. Liaison Officer (SUSLO) in London and Cheltenham, while a SUKLO official from GCHQ has his own offices inside NSA headquarters at Fort Meade. Similar arrangements are made between each allied agency, so that there are also SCALO, SNZLO and SAUSLO posts at Fort Meade. The senior SUKLO and SUSLO posts in London and Washington are of very high seniority. For example, the current SUSLO in London is Barbara A McNamara, formerly the Deputy Director of NSA.

- Most Sigint stations do not have liaison staff as such, although nationals of other UKUSA countries frequently work at other stations.

14. **Are the stations of the surveillance network operated by the participating countries or by the USA or by two countries together?**

- Some UKUSA stations are jointly run. Most are not, even though Second Party nationals may be present. The two known examples of jointly run stations are Pine Gap, Australia and Menwith Hill in the UK. The UK Sigint station at Digby, Lincolshire also hosts NSA units.

15. **Are there stations with specific tasks (for example only military targets, no civil communication)?**

- Stations or systems that mainly or entirely collect HF, VHF and UHF signals are focussed on military targets. Stations intercepting COMSAT signals are primarily or exclusively focussed on civil or commercial communications. Stations operating Sigint satellites in space cover all types of targets.

16. **Are the data processed in every station of the surveillance network or do the individual stations provide the raw material to one (or more) central stations?**

- Some large stations do substantial analysis of the signals they collect and produce signigificant finished intelligence. Menwith Hill and Bad Aibling are examples of such stations. Other stations, such as those processing radio messages, work in small groups

[19] Annual report of the Communications Security Establishment Commissioner, 1997-1998, Ottawa, May 1998, p3.

and collectively produce end product reports. Echelon stations and Dictionary sites mainly collect and filter raw material, and the relay this to one or more customer groups for analysis. At the extreme, Remotely Operated Facilities may have no staff at all, or only maintenance staff, and pass all that they receive to distant locations.

17. **Do the participating countries have access to the intercepted material?**

- At Echelon stations, the selected intelligence is mostly not examined locally before being sent to U.S. or other intelligence sites. This does not mean that the host government is denied access to the data, just that since they are not requesting the same data, they do not get to see what is sent. At the DSD station at Geraldton, Australia it has been officially stated that about 80% of the intelligence is passed directly to the U.S. without being seen by Australian staff. The position of the Australian government is that, since they control the "tasking" of the Dictionary, they supervise the broad types of intelligence that may be collected, without examining the collected messages in detail. They hold that this is adequate supervision from the point of view of Australia.

18. **How many and which stations do belong to the UKUSA surveillance network?**

- I will supply a more exhaustive list, if required. The locations of major UKUSA stations – including all known Echelon or COMSAT intercept stations - are shown in Table 1 (below).

19. **Which forms of communication (telex, fax, phone, etc) are intercepted by the surveillance network and how?**

- Every type of radio communication can be intercepted at suitable stations. At Echelon stations, thousands of channels of communications are broken down into "streams" for examination and selection. One stream is for voice messages (telephone calls), another for fax, and a third for data. Each is handled and processed separately. Descriptions of and references to equipment for separating and processing these signals was included in the technical annexe to the IC2000 report, particularly in relation to the products made by the Applied Signals Technology corporation (AST). A description of how Echelon stations performed these tasks in the1980s can be obtained from the NSA papers of project P377, also known as CARBOY II.[20]

- Many articles in the press have overstated the capability of both Echelon and the UKUSA Sigint system. While the UKUSA Sigint system has immense capacity, it is not normally able to intercept telephone, fax, or e-mail traffic within Europe if these do not travel by satellite or microwave link.

20. **Which methods for the processing of the intercepted data exist?**

- The Dictionary computers of the UKUSA system can target e-mails, faxes and data communications based on their contents as well as the (telecommunications) address of

[20] Published at www.cryptome.org

the sender and the recipient. These descriptions can be very detailed, and logically structured (in the same way as searches in a database or on Internet search engines).

- There is no evidence that the Dictionary computers can target telephone calls based on their content – what the participants say to each other. It can easily target the numbers of the sender and the recipient of a call. Also, individual voices can be recognised and targeted.

The evidence for Echelon

This section focuses on the documentary evidence for the existence of the Echelon system. This is now quite abundant.

21. Echelon is the codename for the SATCOM intercept component of the US SIGINT system. Australia doesn't use that name, but runs part of the system under a different name. New Zealand and Canada have Echelon stations. It isn't known whether the British station uses the name. One U.S. station in the SATCOM intercept system (Misawa) uses a different codename, LADYLOVE.

22. The name Echelon was first used in the 1970s, in the early stages of the COMSAT intercept programme. The first document mentioning Echelon in an NSA document appears in my IC2000 report. It is dated 1979 and refers to Menwith Hill using the "Echelon 2" database. At the time that was published, that was a fragment rather than a full sheet. That was done to protect the source. In January 2000, Margaret Newsham, a former employee of Lockheed Space and Missiles Systems Organisation, said she was willing to be identified as the source of that information. I am now therefore able to provide a full copy of this sheet and make it available to the committee.

23. Ms Newsham worked at Menwith Hill and then in California on a series of projects to greatly expand the Echelon system. Extensive technical details of the original plan for the component parts of the Echelon system at this time, known as Project 377 or CARBOY II have also become available. According to the P-377 specifications,[21] the project provided for the "commonality of automated data processing equipment (ADPE) in the **Echelon** system" (my emphasis).

24. CARBOY II included all the units needed to break down satellite links into component parts of telephone and telegraph channels. The telegraphy components could be either analogue or digital. Their output was fed to the "telegraphy message processing subsystem". Other Echelon components were a "facsimile processing subsystem", a "voice processing subsystem", a "voice collection module" and a"[voice] Tape Production Facility".

25. By the time the IC2000 report was published in 1999, the US intelligence specialist Dr Jeff Richelson had located and obtained US Navy and Air Force documents from the 1990s, giving many details of US Echelon sites. This material is in fact referenced in the IC2000 report, which says that the documents provide "original new documentary and other evidence about the Echelon system and its involvement in the interception of communication satellites". They are references 47-51 in the report.

[21] Available at www.cryptome.org

26. Although these references were not on-line when IC2000 was first published, Dr Richelson has now put them and other official documents on-line in the NSA section of the National Security Archive.[22] They show, for example, that the first task of the commander of the US Naval Security Group satellite station at Sugar Grove, West Virginia is to "maintain and operate an **ECHELON site**" (*emphasis added)).* For the sake of the avoidance of doubt, this does not mean "echelon" in its military meaning of "formation". This is made clear by other documents referring to Echelon units, training departments and related functions.[23]

27. Other documents obtained from the US Air Force Intelligence Agency gave further details of more units, and describe a plan developed in 1994 for the Air Force to post groups of its intelligence specialists into Sugar Grove and other bases for the "activation of Echelon units".[24]

28. A description of what Echelon units actually do can be found among the same documents. They refer to the US Air Force component of the Echelon network, the 544th Intelligence Group, based in Colorado Springs. Their 1995 reports describe Sugar Grove as a COMSAT intercept station. That description is still current in 2001, and is repeated on their web site.[25] This says

> "Detachment 3, 544th Intelligence Group is fully integrated with Naval Security Group Activity, located at Sugar Grove, W. Va. Its mission is to direct satellite communications equipment supporting research and development for multi-service national missions. It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded field stations. This is achieved by embedding personnel into field station operations and by providing a trained cadre of collection system operators, analysts and managers for AIA.
>
> Det. 3's vision is to provide AIA a highly trained cadre of people to capitalize on emerging technologies to meet consumer requirements and to establish itself as a leader in the COMSAT environment by remaining on the cutting edge well into the 21st century.
>
> Det. 3 is comprised of four 1N2 signal analysts, a superintendent and a commander. The personnel of Det. 3 are expected to be on the forefront of technologic advances in communications."

29. Perusing the rest of the documents referred to in these sites shows that Sugar Grove is part of a network including, for example, the NSA station at Yakima, Washington state. This is exactly the same account of what Echelon is (and isn't) as was published in the IC2000 report and in Nicky Hager's 1996 book *Secret Power.* More recently, Richelson has written an article which separates fact from rumour, distinguishing the factual existence and capabilities of the Echelon stations from the inaccurate enlargement which has marked most of the derivative secondary reporting on the same subject. This appeared in the March-April 2000 edition of the *Bulletin of the Atomic Scientists*.[26] This article makes it clear that while much of what has been published about Echelon in the press or on TV is nonsense, Echelon is shown to be the still

---

[22] http://www.hfni.gsehd.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23
[23] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/09-03.htm
[24] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/12-02.htm; http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/12-03.htm
[25] http://www.aia.af.mil/common/homepages/pa/cyberspokesman/jan/atc7.htm#DET3
[26] http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html

extant name for the SATCOM intercept component of the US SIGINT system - even though the U.S. could have opted to change the name long ago.

30. As explained above, Australia doesn't use the “Echelon” name, but admits running part of the integrated system under a different name. New Zealand and Canada have Echelon stations. References to the Australian government’s confirmation that they participate in the system as Hager describes it (but under a different and as yet undisclosed name) appeared in the IC2000 report. So do references to government documents obtained in Canada (under their FOI provisions), identifying the substantial mid 1990s budget expenditure on Echelon by CSE, the Canadian equivalent of CSE and GCHQ. No-one knows if British SATCOM intercept stations now use the name. We do know from the US that one US SATCOM intercept station (Misawa, Japan) uses a different codename, LADYLOVE.

31. It is also important to note that unlike, say, space Sigint satellites, visual evidence is available which afford a measure of confirmation Pictures of all identified Echelon stations, except Guam, are on the web. They all have windowless buildings and arrays of medium to large satellite dishes aimed at geostationery positions. They have double fences and substantial security arrangements.

32. In summary, the evidence that UKUSA has run a COMSAT intercept system called Echelon is supported by sources from 4 different countries, and includes recent official documents from the United States and Canada, and statements in Australia. There are at least 6 human sources, one of whom is now on the record. This is substantially more evidence than is available for other types of intelligence systems whose existence is not usually challenged by the UK or the U.S. governments. There is authenticated and authenticatable evidence, official documents, and physical observation, as well as named sources with proven access to information on the subject.

January 2001

Table 1 Major UKUSA satellite Sigint stations

Station	Country running Station	COMSAT Intercept site ?	Called ECHELON ?	Est no of antennae
Sugar Grove, West Virginia	USA	Yes	Yes	10
Sabana Seco, Puerto Rico	USA	Yes	Yes	4
Yakima, Washington	USA	Yes	Yes	6
Guam	USA	Yes	Yes	N/a
Misawa, Japan	USA	Yes	No – known as LADYLOVE	14
Leitrim, Ontario	Canada	Yes	Probably	4
Waihopai, Marlborough	New Zealand	Yes	Yes	2
Kojarena, Geraldton, WA	Australia	Yes	No	4
Menwith Hill, Yorkshire*	UK	Possibly	Not since 1980s	29
Pine Gap, NT	Australia	No	No	12
Shoal Bay, NT	Australia	Yes	No – no direct connection to UKUSA network	10
Bad Aibling, Bavaria*	Germany	Possibly	No	14
Ayios Nikolaos, Cyprus	Cyprus (UK run)	Yes	Not known	9
Paramali, Cyprus	Cyprus (UK run)	Probably	Not known	3
Morwenstow, Cornwall	UK	Yes	Possibly	14
Denver, Colorado	USA	No	No	11

* There is no current evidence that either Menwith Hill or Bad Aibling function as part of the Echelon civil COMSAT interception system, although they may do so.