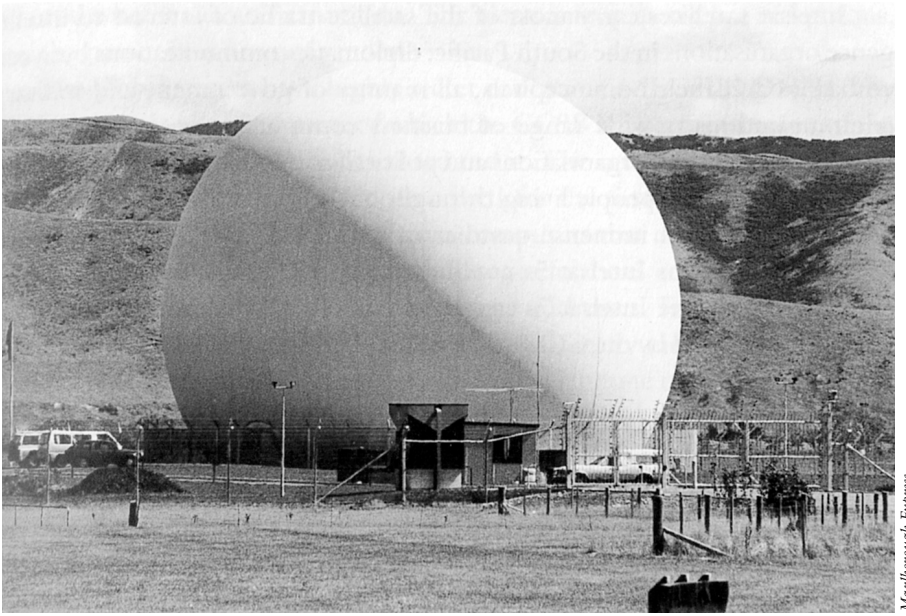
Chapter Two

Hooked Up to the Network
The UKUSA System

Ten years later, on Saturday, 15 January 1994, technicians in satellite earth stations around the Pacific were busy tuning their equipment to a new satellite. The first of the new generation of Intelsat 7 series satellites, it had been launched several weeks before, from the European Kourou air base in French Guyana, and then manoeuvred into position far out in space above the Equator at 174 degrees east, due north of New Zealand above Kiribati.

The 20 Intelsat (International Telecommunications Satellite Organisation) satellites that ring the world above the Equator carry most of the world's satellite-relayed international phone calls and messages such as faxes, e-mail and telexes. The new satellite, Intelsat 701, replaced the 10-year-old Intelsat 510 in the same position. The changeover occurred at 10 pm New Zealand time that summer evening.

At the GCSB's station at Waihopai, near Blenheim in the north of the South Island, the radio officer staff were just as busy that evening, setting their special equipment to intercept the communications which the technicians in legitimate satellite earth stations would send and receive via the new satellite. These specially trained radio officers, who learned their skills at the



Marlborough Express

The Waihopai station — part of a super-secret global system called ECHELON — automatically intercepts satellite communications for the foreign allies. The Labour government that approved the station was not told about these links.

Tangimoana station, usually work day shifts, but on 15 January 1994 they worked around the clock, tuning the station's receivers to the frequency bands the GCSB wanted to intercept, selecting the specific channels within each band that would yield the types of messages sought within the UKUSA network and then testing that the high-tech intelligence collection system was working smoothly. That satellite changeover was a very significant event for the Waihopai station and the GCSB. Although it would always be only a small component of the global network, this was the moment when the station came into its own.

There have been various guesses and hints over the years about what the Waihopai station was set up to monitor—'sources' in one newspaper said foreign warship movements; a 'senior Telecom executive' told another newspaper it was most likely 'other countries' military communications'—but, outside a small group of intelligence staff, no one could do more than theorise. Waihopai was established specifically to target the international satellite traffic carried by Intelsat satellites in the Pacific region and its target in the mid-1990s is the Intelsat 701 that came into service in January 1994, and is the primary satellite for the Pacific region.

Intelsat satellites carry most of the satellite traffic of interest to intelligence organisations in the South Pacific: diplomatic communications between embassies and their home capitals, all manner of government and military communications, a wide range of business communications, communications of international organisations and political organisations and the personal communications of people living throughout the Pacific. The Intelsat 7 satellites can carry an immense number of communications simultaneously. Where the previous Intelsat 5s could carry 12,000 individual phone or fax circuits at once, the Intelsat 7s can carry 90,000. All 'written' messages are currently exploited by the GCSB. The other UKUSA agencies monitor phone calls as well.

The key to interception of satellite communications is powerful computers that search through these masses of messages for ones of interest. The intercept stations take in millions of messages intended for the legitimate earth stations served by the satellite and then use computers to search for pre-programmed addresses and keywords. In this way they select out manageable numbers (hundreds or thousands) of messages to be searched through and read by intelligence analysis staff.

Until the Intelsat 701 satellite replaced the older 5 series, all the communications intercepted at Waihopai could already be got from two existing UKUSA stations covering the Pacific. But, unlike their predecessors, this new generation of Intelsat 7s had more precise beams transmitting communications down to the southern hemisphere. The existing northern hemisphere-based stations were no longer able to pick up all the southern communications, which is why new stations were required.

Eleven months later, on 3 December 1994, the other old Intelsat satellite above the Pacific was replaced by Intelsat 703. Since then Waihopai and its sister station in Australia constructed at the same time have been the main source of southern hemisphere Pacific satellite communications for the UKUSA network.

Many people are vaguely aware that a lot of spying occurs, maybe even on them, but how do we judge if it is ubiquitous or not a worry at all? Is someone listening every time we pick up the telephone? Are all our Internet or fax messages being pored over continuously by shadowy figures somewhere in a windowless building? There is almost never any solid information with which to judge what is realistic concern and what is silly paranoia.

What follows explains as precisely as possible—and for the first time in public—how the worldwide system works, just how immense and powerful

it is and what it can and cannot do. The electronic spies are not ubiquitous, but the paranoia is not unfounded.

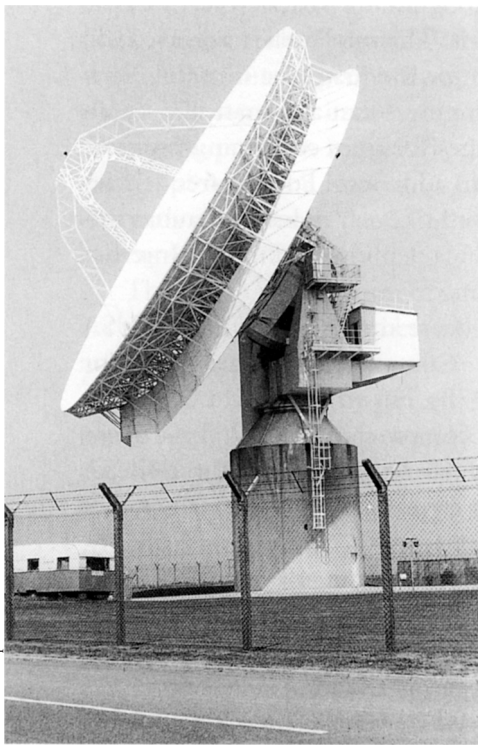
The global system has a highly secret codename—ECHELON. It is by far the most significant system of which the GCSB is a part, and many of the GCSB's daily operations are based around it. The intelligence agencies will be shocked to see it named and described for the first time in print. Each station in the ECHELON network has computers that automatically search through the millions of intercepted messages for ones containing pre-programmed keywords or fax, telex and e-mail addresses. For the frequencies and channels selected at a station, every word of every message is automatically searched (they do not need your specific telephone number or Internet address on the list).

All the different computers in the network are known, within the UKUSA agencies, as the ECHELON Dictionaries. Computers that can search for keywords have existed since at least the 1970s, but the ECHELON system has been designed to interconnect all these computers and allow the stations to function as components of an integrated whole. Before this, the UKUSA allies did intelligence collection operations for each other, but each agency usually processed and analysed the intercept from its own stations. Mostly, finished reports rather than raw intercept were exchanged.

Under the ECHELON system, a particular station's Dictionary computer contains not only its parent agency's chosen keywords, but also a list for each of the other four agencies. For example, the Waihopai computer has separate search lists for the NSA, GCHQ, DSD and CSE in addition to its own. So each station collects all the telephone calls, faxes, telexes, Internet messages and other electronic communications that its computers have been pre-programmed to select for all the allies and automatically sends this intelligence to them. This means that the New Zealand stations are used by the overseas agencies for their automatic collecting—while New Zealand does not even know what is being intercepted from the New Zealand sites for the allies. In return, New Zealand gets tightly controlled access to a few parts of the system.

When analysts at the agency headquarters in Washington, Ottawa, Cheltenham and Canberra look through the mass of intercepted satellite communications produced by this system, it is only in the technical data recorded at the top of each intercept that they can see whether it was intercepted at Waihopai or at one of the other stations in the network. Likewise, GCSB staff talk of the other agencies' stations merely as the various 'satellite links' into the integrated system. The GCSB computers, the stations, the

headquarters operations and, indeed, the GCSB itself function almost entirely as components of this integrated system.



Duncan Campbell

One of two dishes at a British spy station in Cornwall that between them intercepted all Atlantic and Indian Ocean satellite phone and telex until the early 1980s.

In addition to satellite communications, the ECHELON system covers a range of other interception activities, described later. All these operations involve collection of *communications intelligence*,[1] as opposed to other types of signals intelligence such as electronic intelligence, which is about the technical characteristics of other countries' radar and weapon systems.

Interception of international satellite communications began in the early 1970s, only a few years after the first civilian communications satellites were launched. At this time the Intelsat satellites, located over the Atlantic, Pacific and Indian Oceans, simply beamed all their messages down to the entire hemisphere within their view.

Throughout the 1970s only two stations were required to monitor all the Intelsat communications in the world: a GCHQ station in the south-west of England had two dishes, one each for the Atlantic and Indian Ocean Intelsats, and an NSA station in the western United States had a single dish covering the Pacific Intelsat.

The English station is at Morwenstow, at the edge of high cliffs above the sea at Sharpnose Point in Cornwall. Opened in 1972-73, shortly after the introduction of new Intelsat 4 satellites, the Morwenstow station was a joint British-American venture, set up using United States-supplied computers and communications equipment, and was located only 110 kilometres from the legitimate British Telecom satellite station at Goonhilly to the south. In the 1970s the Goonhilly dishes were inclined identically towards the same Atlantic and Indian Ocean satellites.[2]

The Pacific Intelsat satellite was targeted by an NSA station built on a high

basalt tableland inside the 100,000-hectare United States Army Yakima Firing Centre, in Washington State in the north-west United States, 200 kilometres south-west of Seattle. Also established in the early 1970s, the Yakima Research Station initially consisted of a long operations building and the single large dish. In 1982, a visiting journalist noted that the dish was pointing west, out above the Pacific to the third of the three Intelsat positions.[3]

Yakima is located between the Saddle Mountains and Rattlesnake Hills, in a desert of canyons, dunes and sheer rock cliffs, where the only vegetation is grass. The Army leases the land to ranchers who herd their cattle in the shadow of the dishes. When visited in mid-1995 the Yakima station had five dish antennae, three facing westwards over the Pacific Ocean and two, including the original large 1970s dish, facing eastwards. Besides the original operations building there were several newer buildings, the largest of them two-storey, concrete and windowless.

Two of the west-facing dishes are targeted on the main Pacific Intelsat satellites; the Yakima station has been monitoring Pacific Intelsat communications for the NSA ever since it opened. The orientation of the two east-facing dishes suggests that they may be targeted on the Atlantic Intelsats, intercepting communications relayed towards North and South America. One or both may provide the link between the station and the NSA headquarters in Washington. The fifth dish at the station is smaller than the rest and faces to the west. Given its size and orientation, it appears to be the UKUSA site for monitoring the Inmarsat-2 satellite that provides mobile satellite communications in the Pacific Ocean area. If so, this is the station that would, for example, have been monitoring Greenpeace communications during the nuclear testing protests in the waters around Moruroa Atoll in 1995.

The GCSB has had important links with the Yakima station since 1981, when the GCSB took over a special, highly secret area of intelligence analysis for the UKUSA network (see Chapter 6). Telexes intercepted using Yakima's single dish were first sorted by the Yakima computers, and then subjects allocated to New Zealand were sent to the GCSB for analysis. The Yakima station had been using Dictionary-type computers for this searching work for many years before the full ECHELON system was operating.

Between them, the Morwenstow and Yakima stations covered all Intelsat interception during the 1970s. But a new generation of Intelsat satellites launched from the late 1970s required a new configuration of spy stations. The Intelsat 4A and 5 series satellites differed from earlier ones in that they did not transmit only to the whole of the side of the world within their view; they now also had 'east and west hemispheric' beams that transmitted

separately.[4] For example, Intelsat 510, which operated above the Pacific until its replacement in December 1994, had one 'global' beam covering the whole region, but all the other transmissions went either to the east or to the west Pacific. Yakima was not within the 'footprint' of any hemispheric beams covering Australasia, South East Asia and East Asia, making interception of these signals difficult or impossible.

These changes to Intelsat design meant that the UKUSA alliance required at least two new stations to maintain its global coverage. Again the GCHQ provided one and the NSA one. A new NSA station on the east coast of the United States would cover Atlantic Intelsat traffic beamed down towards North and South America (Morwenstow covered the eastern Atlantic), and a GCHQ station in Hong Kong would cover both the western hemisphere of the Pacific Intelsats and the eastern hemisphere of the Indian Ocean Intelsats.

The site chosen for the new NSA station was hidden in the forested South Fork Valley in the mountains of West Virginia, about 250 kilometres south-west from Washington DC, on the edge of the George Washington National Forest, near the small settlement of Sugar Grove. The site had been used in the 1950s and early 1960s for a failed attempt to spy on Russian radio communications and radars by means of reflections from the moon. The current satellite interception station was developed during the late 1970s, when a collection of new satellite dishes (from 10 to 45 metres in diameter) and the new windowless Raymond E. Linn Operations Building were constructed. It also incorporated a two-storey underground operations building already at the site. It started full operations about 1980.[5]

Like Morwenstow and Yakima, Sugar Grove is only 100 kilometres from an international satellite communications earth station, making it easy to intercept any 'spot' beams directed down to the legitimate stations. In this case it is the Etam earth station, the main link in the United States with the Intelsat satellites above the Atlantic Ocean.

The other new station, in Hong Kong, was constructed by the GCHQ also in the late 1970s. The station, which has since been dismantled, was perched above the sea on the south side of Hong Kong Island, across Stanley Bay from the British Stanley Fort military base and right next to high-rise apartments and luxury housing. In crowded Hong Kong the station's anonymity was assured simply because there are so many satellite dishes scattered over the island. What helped to give away this one was the sign, on the entrance to an exclusive housing enclave across the bay, saying that taking photographs is strictly forbidden. When one of the Indian guards on the gate

was asked why it was forbidden to take photos of a housing area, he pointed across the bay and said in serious tones, 'Communications facility—very, very secret'.

The Hong Kong station had several satellite dishes and buildings, including a large windowless concrete building (similar to the ones at Yakima and Sugar Grove) and a collection of administration and operations buildings running down the hill into the base from the gates. Intelsat communications intercepted at the station were seen regularly by GCSB operations staff in Wellington.[6]

When visited in August 1994, the station fitted the requirements of the Intelsat monitoring network. It had one dish pointing up east towards the Pacific Intelsats, another towards the Indian Ocean Intelsats and a third, for the station's own communications, pointing up to a United States Defence Satellite Communications System satellite above the Pacific. Other dishes had perhaps already been removed. Dismantling of the station began in 1994—to ensure it was removed well before the 1997 changeover to Chinese control of Hong Kong—and the station's staff left in November that year. News reports said that the antennae and equipment were being shipped to the DSD-run Shoal Bay station in Northern Australia, where they would be used for intercepting Chinese communications.

It is not known how the Hong Kong station has been replaced in the global network. One of the Australian DSD stations—either Geraldton or Shoal Bay—may have taken over some of its work, or it is possible that another north-east Asian UKUSA station moved into the role. For example, there were developments at the NSA's Misawa station in northern Japan in the 1980s that would fit well with the need for expanded Intelsat monitoring.[7]

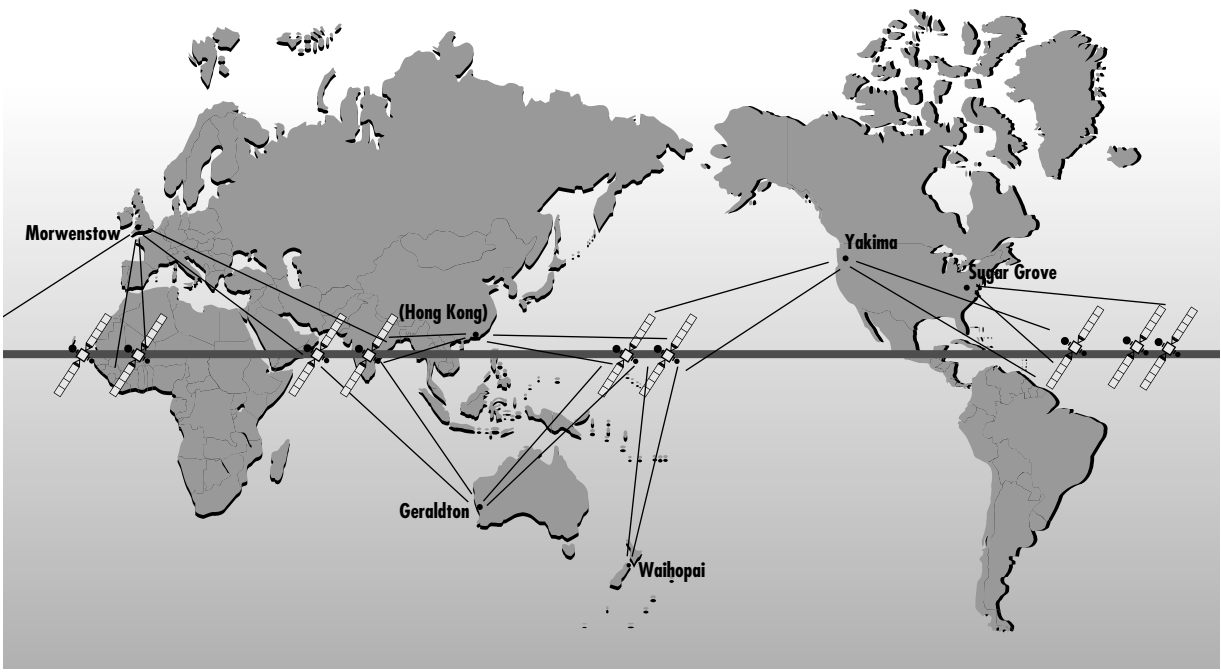
Throughout the 1980s a series of new dishes was also installed at the Morwenstow station, to keep up with expansion of the Intelsat network. In 1980 it still required only the two original dishes, but by the early 1990s it had nine satellite dishes: two inclined towards the two main Indian Ocean Intelsats, three towards Atlantic Ocean Intelsats, three towards positions above Europe or the Middle East and one dish covered by a radome.

The Morwenstow, Yakima, Sugar Grove and Hong Kong stations were able to provide worldwide interception of the international communications carried by Intelsat throughout the 1980s. The arrangement within the UKUSA alliance was that, while the NSA and GCHQ ran the four stations, each of the five allies (including the GCSB) had responsibility for analysing some particular types of the traffic intercepted at these stations.

Then, in the late 1980s, another phase of development occurred. It may have been prompted by approaching closure of the Hong Kong station, but a more likely explanation is that, as we have seen, technological advances in the target Intelsat satellites again required expansion of the network.

Two UKUSA countries were available to provide southern hemisphere coverage: Australia and New Zealand. One of the new southern hemisphere stations would be the GCSB's Waihopai station and the other would be at Geraldton in West Australia. (Both stations are described in detail later.) The new stations were operating by 1994 when the new Intelsat 7s began to be introduced. Waihopai had opened in 1989, with a single dish, initially covering one of the older generation of Intelsat satellites.

The positioning of the Geraldton station on Australia's extreme west coast was clearly to allow it to cover the Indian Ocean Intelsats (they all lie within 60 degrees of the station, which allows good reception). Geraldton opened in



Six UKUSA stations target the Intelsat satellites used to relay most satellite phone calls, internet, e-mail, faxes and telexes around the world. They are part of a network of secret stations and spy satellites which, between them, intercept most of the communications on the planet.

1993, with four dishes, covering the two main Indian Ocean Intelsats (at 60 degrees and 63 degrees) and possibly a new Asia-Pacific Intelsat introduced in 1992. It also covers the second of the two Pacific Intelsats, Intelsat 703.

The logic of the system suggests that, at the same time as the Waihopai and Geraldton stations were added to the network, a seventh, as yet undiscovered, station may have been installed in the South Atlantic. This station, probably located on Ascension Island, would complete the 1990s network by intercepting the Atlantic Intelsats' southern hemisphere communications.[8]

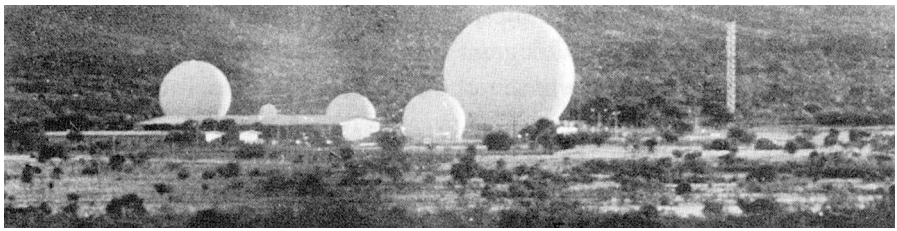
New GCSB operations staff attend training sessions that cover the ECHELON system, showing how the GCSB fits into the system and including maps showing the network of UKUSA stations around the world. The sessions include briefings on the Intelsat and the maritime Inmarsat satellites — their locations, how they work, what kinds of communications they carry and the technical aspects of their vulnerability to spying. This is because these are primary targets for the UKUSA alliance in the Pacific.

But the interception of communications relayed by Intelsat and Inmarsat is only one component of the global spying network co-ordinated by the ECHELON system. Other elements include: radio listening posts, including the GCSB's Tangimoana station; interception stations targeted on other types of communications satellites; overhead signals intelligence collectors (spy satellites) like those controlled from the Pine Gap facility in Australia; and secret facilities that tap directly into land-based telecommunications networks.

What Waihopai, Morwenstow and the other stations do for satellite communications, another whole network of intercept stations like Tangimoana, developed since the 1940s, does for radio.

There are several dozen radio interception stations run by the UKUSA allies and located throughout the world. Many developed in the early years of the Cold War and, before satellite communications became widespread in the 1980s, were the main ground signals intelligence stations targeting Soviet communications. Some stations were also used against regional targets. In the Pacific, for example, ones with New Zealand staff were used to target groups and governments opposed by Britain and the United States through a series of conflicts and wars in South East Asia.

A recent new radio interception station is the Australian DSD station near Bamaga in northern Queensland, at the tip of Cape York. It was set up in 1988 particularly to monitor radio communications associated with



The controversial Pine Gap base in central Australia is a major ground station for United States electronic spy satellites. It has kept expanding after the Cold War; today there are 12 'golf balls'. It plays a key role in United States military strategies.

the conflict between Papua New Guinea and the secessionist movement in Bougainville.[9] GCSB staff are also aware of Australian intercept staff posted in the early 1990s to the recently opened Tindal Air Force base in northern Australia, suggesting that an even newer—as yet undisclosed—DSD intercept station may have been established there.

Most of this network of stations target long-range high frequency (HF) radio. A powerful HF radio transmitter can transmit right around the world, which is why HF radio has been a major means of international communications and is still widely used by military forces and by ships and aircraft. Other stations target short-range communications—very high frequency and ultra high frequency radio (VHF and UHF)—which, among other things, are used extensively for tactical military communications within a country.

There is a wide variety of these radio interception operations. Some are very large, with hundreds of staff; others are small—a few staff hidden inside a foreign embassy bristling with radio aerials on the roof; others (like the Bamaga station) are unstaffed, with the signals automatically relayed to other stations. Because of the peculiarities of radio waves, sometimes stations far from the target can pick up communications that closer ones cannot.

Each station in this network—including the GCSB's Tangimoana station—has a Dictionary computer like those in the satellite intercept stations. These search and select from the communications intercepted, in particular radio telexes, which are still widely used, and make these available to the UKUSA allies through the ECHELON system.

The UKUSA network of HF stations in the Pacific includes the GCSB's Tangimoana station (and before it one at Waiouru), five or more DSD stations in Australia, a CSE station in British Columbia, and NSA stations in Hawaii, Alaska, California, Japan, Guam, Kwajalein and the Philippines. The

NSA is currently contracting its network of overseas HF stations as part of post-Cold War rationalisation. This contraction process includes, in Britain, the closure of the major Chicksands and Edzell stations.

The next component of the ECHELON system covers interception of a range of satellite communications not carried by Intelsat. In addition to the six or so UKUSA stations targeting Intelsat satellites, there are another five or more stations targeting Russian and other regional communications satellites. These stations are located in Britain, Australia, Canada, Germany and Japan. All of these stations are part of the ECHELON Dictionary system. It appears that the GCHQ's Morwenstow station, as well as monitoring Intelsat, also targets some regional communications satellites.

United States spy satellites, designed to intercept communications from orbit above the earth, are also likely to be connected into the ECHELON system. These satellites either move in orbits that criss-cross the earth or, like the Intelsats, sit above the Equator in geostationary orbit. They have antennae that can scoop up very large quantities of radio communications from the areas below.

The main ground stations for these satellites, where they feed back the information they have gathered into the global network, are Pine Gap, run by the CIA near Alice Springs in central Australia, and the NSA-directed Menwith Hill and Bad Aibling stations, in England and Germany respectively.[10] These satellites can intercept microwave trunk lines and short-range communications such as military radios and walkie-talkies. Both of these transmit only line of sight and so, unlike HF radio, cannot be intercepted from faraway ground stations.

The final element of the ECHELON system are facilities that tap directly into land-based telecommunications systems, completing a near total coverage of the world's communications. Besides satellite and radio, the other main method of transmitting large quantities of public, business and government communications is a combination of undersea cables across the oceans and microwave networks over land. Heavy cables, laid across the seabed between countries, account for a large proportion of the world's international communications. After they emerge from 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. Intercepting 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—large aerials and dishes—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. For this reason the worldwide network of facilities to intercept these communications is still mostly undocumented.

Microwave communications are intercepted in two ways: by ground stations, located near to and tapping into the microwave routes, and by satellites. Because of the curvature of the earth, a signals intelligence satellite out in space can even be directly in the line of a microwave transmission. Although it sounds technically very difficult, microwave interception from space by United States spy satellites does occur.[11]

A 1994 exposé of the Canadian UKUSA agency called Spyworld,[12] co-authored by a previous staff member, Mike Frost, gave the first insights into how much microwave interception is done. 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 all manner of communications in the foreign capitals.

Since most countries' microwave networks converge on the capital city, embassy buildings are an ideal site for microwave interception. Protected by diplomatic privilege, embassies allow the interception to occur from right within the target country.[13] Frost said the operations particularly target microwave communications, but also other communications including car telephones and short-range radio transmissions.

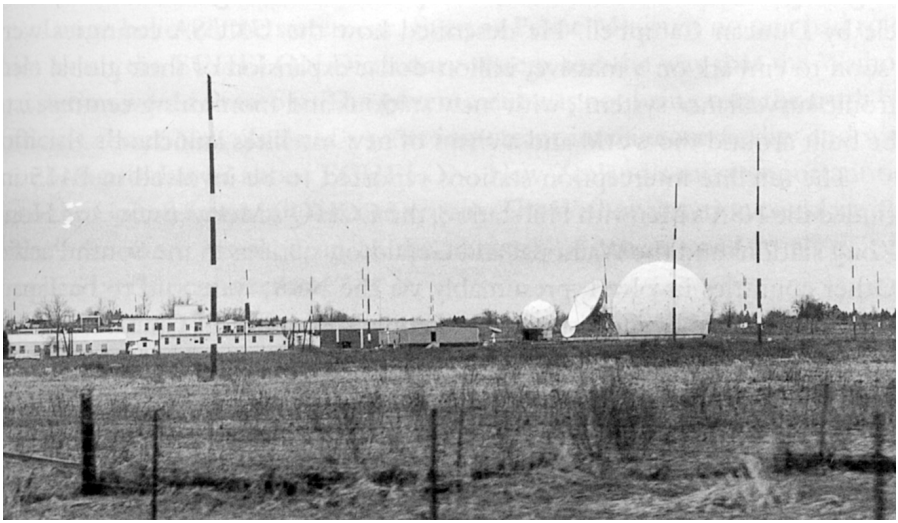
According to Frost, Canadian embassy collection began in 1971 following pressure from the NSA. The NSA provided the equipment (on indefinite loan), trained the staff, told them what types of transmissions to look for on particular frequencies and at particular times of day and gave them a search list of NSA keywords. All the intelligence collected was sent to the NSA for analysis. The Canadian embassy collection was requested by the NSA to fill gaps in the United States 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. Leaks in the 1980s described installation of 'extraordinar-

ily sophisticated intercept equipment, known as Reprieve' in Australia's High Commission in Port Moresby, Papua New Guinea and in the embassies in Indonesia and Thailand. The operations are said to take a whole room of the embassy buildings and to be able to listen to local telephone calls at will.[14] There is good reason to assume that these operations, too, were prompted by and supported with equipment and technical advice from the NSA and GCHQ.

Of course, when the microwave route is across one of the UKUSA countries' territory it is much easier to arrange interception. For example, it is likely that there is a GCHQ operation intercepting, and feeding through Dictionary computers, all the trans-Atlantic undersea cable communications that come ashore in Cornwall.

There are also definitely United States and possibly Canadian facilities for this type of interception. By far the most important of these is the NSA-directed Menwith Hill station in Britain. With its 22 satellite terminals and over 2 hectares of buildings, Menwith Hill is undoubtedly the largest station in the UKUSA network. In 1992 some 1200 United States personnel were based there.[15] British researcher Duncan Campbell has described how Menwith Hill 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.[16] The station



Bill Robinson

Canada's Leitrim station, just south of Ottawa, appears to be used to intercept Latin American satellites.

also intercepts satellite and radio communications and is a ground station for the electronic eavesdropping satellites. Each of Menwith Hill's powerful interception and processing systems presumably has its own Dictionary computers connected into the ECHELON system.

Menwith Hill, sitting in northern England, several thousand kilometres from the Persian Gulf, was awarded the NSA's Station of the Year prize for 1991 following its role in the Gulf War. It is a station which affects people throughout the world.

In the early 1980s James Bamford uncovered some information about a worldwide NSA computer system codenamed Platform which, he wrote, 'will tie together fifty-two 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 organisation, GCHQ.'[17]

There is little doubt that Platform is the system that links all the major UKUSA station computers in the ECHELON system. Because it involves computer-to-computer communications, the GCSB and perhaps DSD were only able to be integrated into the system in the 1990s when the intelligence and military organisations in the two countries changed over to new computer-based communications systems.

The worldwide developments, of which construction of the Waihopai station was part, were co-ordinated by the NSA as Project P415. Although most of the details remained hidden, the existence of this highly secret project targeting civilian communications was publicised in August 1988 in an article by Duncan Campbell. He described how the UKUSA countries were 'soon to embark on a massive, billion-dollar expansion of their global electronic surveillance system', with 'new stations and monitoring centres ... to be built around the world and a chain of new satellites launched'.

The satellite interception stations reported to be involved in P415 included the NSA's Menwith Hill station, the GCHQ's Morwenstow and Hong Kong stations and the Waihopai and Geraldton stations in the South Pacific. Other countries involved, presumably via the NSA, were said to be Japan, West Germany and, surprisingly, the People's Republic of China.

'Both new and existing surveillance systems are highly computerised,' Campbell explained. 'They rely on near total interception of international commercial and satellite communications in order to locate the telephone and other target messages of target individuals....'[18]

There were two components to the P415 development, the first being

the new stations required to maintain worldwide interception. More striking, though, was the expansion of the NSA's ECHELON system, which now links all the Dictionary computers of all the participating countries.

The ECHELON system has created an awesome spying capacity for the United States, allowing it to monitor continuously most of the world's communications. It is an important component of its power and influence in the post-Cold War world order, and advances in computer processing technology continue to increase this capacity.

The NSA pushed for the creation of the system and has the supreme position within it. It has subsidised the allies by providing the sophisticated computer programmes used in the system, it undertakes the bulk of the interception operations and, in return, it can be assumed to have full access to all the allies' capabilities.

Since the ECHELON system was extended to cover New Zealand in the late 1980s, the GCSB's Waihopai and Tangimoana stations—and indeed all the British, Canadian and Australian stations too—can be seen as elements of a United States system and as serving that system. The GCSB stations provide some information for New Zealand government agencies, but the primary logic of these stations is as parts of the global network.

On 2 December 1987, when Prime Minister David Lange announced plans to build the Waihopai station, he issued a press statement explaining that the station would provide greater independence in intelligence matters: 'For years there has been concern about our dependence on others for intelligence—being hooked up to the network of others and all that implies. This government is committed to standing on its own two feet.'

Lange believed the statement. Even as Prime Minister, no one had told him about the ECHELON Dictionary system and the way that the Waihopai station would fit into it. The government was not being told the truth by officials about New Zealand's most important intelligence facility and was not being told at all about ECHELON, New Zealand's most important tie into the United States intelligence system. The Waihopai station could hardly have been more 'hooked up to the network of others', and to all that is implied by that connection.