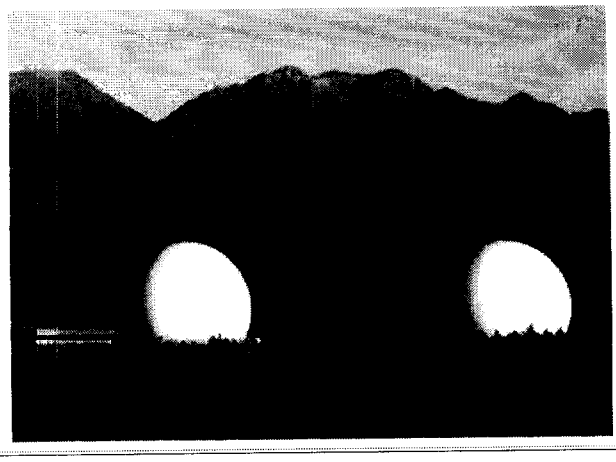
the Bulletin of the Atomic Scientists

March/April 2000
Vol. 56, No. 2, pp. 47-51



DESPERATELY SEEKING SIGNALS

by Jeffrey Richelson

Departments
Home
Back Issues
Spanish Edition
Nuclear Notebook
Bulletin Newswire
Book Reviews
Special Topics
Site Map
Search

The fear that "big brother" might be monitoring our private communications is not new. It's no wonder that when a January 1998 report to the European Parliament, *An Appraisal of Technologies of Political Control,* claimed that "within Europe, all e-mail, telephone, and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland . . . to Fort Meade in Maryland," it triggered a political controversy that continues to this day.

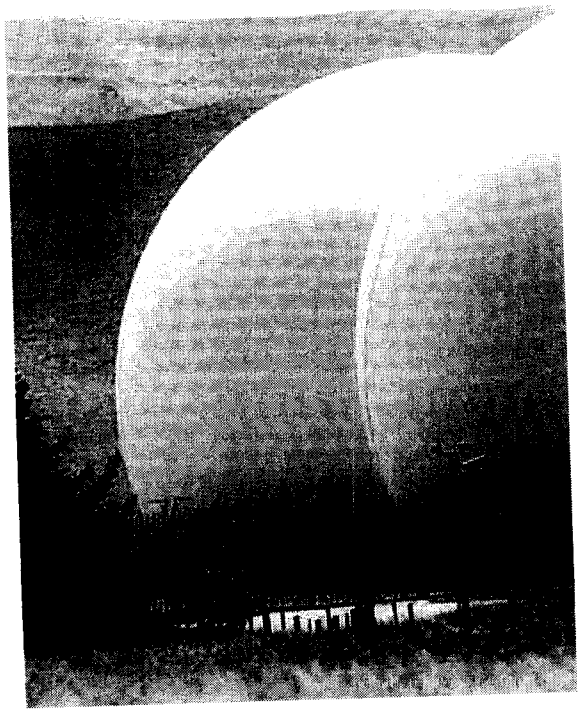
The study also asserted that the key to the eavesdropping operation was a system code-named "Echelon," designed to indiscriminately intercept the non-military communications of governments, private organizations, and businesses on behalf of the United States and its primary partners in the decades-old UKUSA signals intelligence alliance--Britain, Australia, Canada, and New Zealand. Items of intelligence value are selected by computer identification of keywords provided by the UKUSA nations.

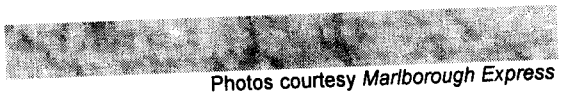
In response to extensive press coverage across Europe, the European Parliament commissioned a second report that focused exclusively on

Echelon and communications intelligence. Sweden's foreign minister promised to investigate whether Swedish companies were harmed by U.S. spying. Last October, activists on both sides of the Atlantic participated in "Jam Echelon Day" by sending a high volume of communications containing words, such as "terrorism," which they expected to be on the keyword list, in hopes of overloading the system.

The Australian and New Zealand public have also taken an interest. And in the United States, the conservative Free Congress Foundation issued a report on the topic titled *Echelon: America's Secret Global Surveillance Network.* The American Civil Liberties Union maintains an "Echelon Watch" section on its web site, at www.aclu.org/ echelonwatch. The controversy has even reached into the halls of Congress, where Cong. Porter Goss of Florida, the Republican chair of the House Permanent Select Committee on Intelligence, requested that the National Security Agency (NSA provide internal documents that would help reassure the committee that U.S. signals intelligence activities are not violating the privacy rights of Americans. Meanwhile, at the instigation of Republican Cong. Bob Barr of Georgia, hearings are scheduled for the current session of Congress to explore that issue.

The fear, press coverage, and rhetoric surrounding Echelon begs the question: could this be a case where life is imitating art? A number of recent films (*Sneakers, Enemy of the State, Mercury Rising, The Shadow Conspiracy*) depict the NSA as an organization that ignores legal restraints in pursuit of its vision of national security (and career advancement for key personnel). It is possible that some of the reporting and oratory concerning Echelon may be as over-the-top as these films, in which NSA officials also casually authorize murder, even of small children.





Photos courtesy *Marlborough Express*

The Waihopai intercept facility (above and at top) in New Zealand.

The Echelon network

That the UKUSA alliance, particularly as a result of U.S. efforts, operates an electronic eavesdropping network with global reach should come as no surprise. The National Reconnaissance Office maintains a constellation of geosynchronous, elliptically orbiting, and low-earth orbiting satellites that intercept communications, missile telemetry, and radar emanations. Civilian and military personnel run satellite ground stations in Britain, Germany, Australia, and Colorado which control the satellites and receive the intercepted signals. The Air Combat Command and the navy fly a variety of planes equipped to scoop up communications and other electronic signals. Nor has the end of the Cold War led to the termination of ship-based signals intelligence collection or submarine reconnaissance operations--including operations to tap undersea cables.

Ground intercept sites also continue to be part of the eavesdropping network. While the United States closed down a number of stations in the aftermath of the Cold War--particularly those that intercepted high-frequency military communications--ground sites still form an important part of the UKUSA network. One particular set of ground stations is devoted to the interception of satellite communications--or the "COMSAT intercept mission."

According to much of the press coverage, Echelon is the code word for the UKUSA "global surveillance network." But it is not, nor is there any code word for the overall U.S. or UKUSA "SIGINT (Signals Intelligence) apparatus. Rather, the U.S. system is known as the United States Sigint System (USSS).

Echelon is, however, very real. Its existence was first revealed by British investigative reporter Duncan Campbell in an August 12, 1988 *New Statesman* article. In 1996, New Zealand peace activist Nicky Hager provided a detailed description of the program in his book, *Secret Power: New Zealand's Role in the International Spy Network*, an extraordinary examination of New Zealand's SIGINT agency and its place in the UKUSA alliance. Virtually all reporting, including the original report to the European Parliament, is derived from these works. Unfortunately, much of the reporting does not accurately reflect what Campbell and Hager wrote.

The Echelon system that Hager describes links together computers, known as "dictionaries," at UKUSA ground stations. Those computers contain, for each of the cooperating agencies, a list of keywords whose appearance in any intercepted message makes the message an item of interest to the agency. The computers automatically search through millions of intercepted messages for the ones containing the pre-programmed keywords and then ship the selected messages off to the

computers of the requesting agency.

Before Echelon appeared in the 1970s, the agencies shared intelligence, but they usually processed and analyzed the intercepted communications. As a result, most exchanges involved finished reports rather than raw intercepts. Echelon, on the other hand, is an integrated network that allows the agencies to specify which intercepts are of interest and to receive them automatically via computer. A key question, then, is which UKUSA ground stations are part of the Echelon network?

COMSAT intercept sites are clearly part of that network. Almost 20 years ago, author James Bamford revealed in *The Puzzle Palace* that NSA-operated antennas at Sugar Grove, West Virginia, and Yakima, Washington, targeted the signals to and from INTELSAT communications satellites. Just 60 miles from Sugar Grove, at Etam, West Virginia, telephone calls, telegrams, and telexes arriving from or destined for 134 countries passed through an array of satellite dishes. The NSA operation at the obscure Yakima Firing Range, Bamford reported, was conveniently located 100 miles south of a similar station in north-central Washington.

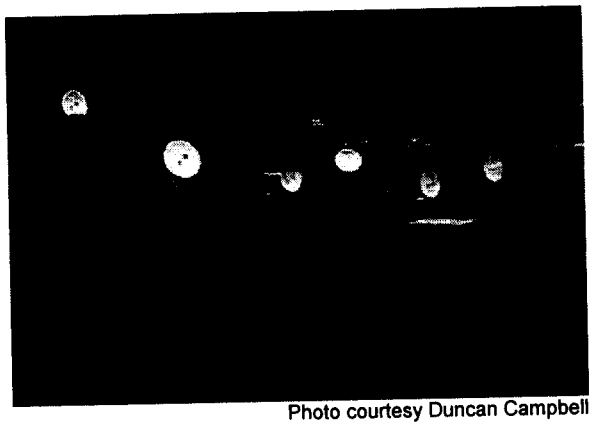


Photo courtesy Duncan Campbell

Antennas at Sugar Grove, West Virginia, monitor COMSAT and INTELSAT traffic.

Today, Sugar Grove hosts both navy and air force SIGINT units that operate four satellite antennas targeted on the communications flowing in and out of the Etam ground station. The mission of the air force unit was described in the 1998-99 *Air Intelligence Agency Almanac* as providing "enhanced intelligence support to air force operational commanders and other consumers of COMSAT information." That Sugar Grove is part of the Echelon program is clear from declassified Naval Security Group Command regulation C5450.48A, which notes that one of the duties of Sugar Grove's commander is to "maintain and operate an Echelon site."

The air force unit at Sugar Grove is a detachment of the Air Intelligence Agency's 544th Intelligence Group; Yakima and Sabana Seca, Puerto Rico (another COMSAT intercept site), host detachments from the 544th IG,evidence that they are also part of the Echelon network. More evidence is provided by the official *History of the Air Intelligence Agency* (AIA) for 1994, which contains a section titled "Activation of Echelon

Units." That section noted that, in 1994, the AIA, NSA, and the navy's SIGINT agency "drafted agreements to increase AIA participation in the growing [deleted, but apparently 'civilian communications'] mission" and that AIA was to establish detachments of the 544th Intelligence Group to accomplish that objective.

The other partners to the UKUSA agreement do not have the resources or incentive to maintain an array of SIGINT systems similar to those of the United States. But they can and do operate COMSAT intercept sites. Even tiny New Zealand has a modern intercept facility on its east coast at Waihopai. Hager reports that the station, operational since 1989, consists of a services building, two satellite dishes under large radomes, and an operations building. If there was any doubt about what was going on at the facility, it was dispelled when a television reporter entered the station and filmed close-ups of INTELSAT technical manuals held in the control center, as Duncan Campbell wrote in his 1999 report to the European Parliament, *Interception Capabilities 2000.*

Meanwhile, Australia operates a more extensive intercept facility at Geraldton in western Australia. When Geraldton opened in 1993 it had four intercept dishes targeted on INTELSATs orbiting above the Indian Ocean and Pacific. Among the keywords in the Geraldton dictionary are ones related to North Korea's economic, diplomatic, and military situation, Japanese trade ministry plans, and developments in Pakistani nuclear weapons technology. Another Australian intercept site, at Shoal Bay on the northern-central coast, began operating in late 1979, with two dishes targeted on Indonesian communications satellites. Shoal Bay is not, however, part of the Echelon network, as Australia refuses to share the raw intercepts with the United States and Britain.1

The other UKUSA partners also target communications satellites. A Canadian Communications Security Establishment site at Leitrim appears to intercept the signals from communications satellites over Latin America. Britain's Government Communications Headquarters operates a major COMSAT intercept site at Morwenstow, near Bude, Cornwall.2

While Echelon's dictionary computers are also present at the ground stations for U.S. SIGINT satellites, the stations do not appear to be tied into the Echelon network. According to Campbell, they sort through intercepted material in the same way that the Echelon dictionaries do, but their intercepts are not made available to U.S. partners. Nor do any cable tapping operations appear to feed into Echelon.

Chinks in the armor

That "Echelon" is not synonymous with the entire UKUSA eavesdropping effort does not mean that the questions raised about it are not valid. An intercept operation that scoops up a good deal of the world's communications satellite traffic, automatically processes it in search of whatever intelligence any UKUSA nation wished, and then sends it on its way, would be unsettling.

At least for the immediate future the reality seems to be somewhat less frightening. The UKUSA SIGINT agencies certainly do not intercept every signal that passes through the airwaves. And, because of the volume of communications, the expense of collection systems, and the limits of their computer resources, NSA and its allies have always had to prioritize targets and selectively task collection systems. Campbell notes in *Interception Capabilities* that it is possible to identify certain satellite signals, whether television or communications, as of no intelligence interest, and that "these signals will not progress further within the system."

There is also a significant limit imposed on the ability to monitor voice communications, resulting from the failure of extensive U.S. Efforts to produce "word spotting" software that would allow computer transcription of intercepted conversations. In 1993, former NSA director Bobby Inman admitted that "I have wasted more U.S. taxpayer dollars trying to do that [word spotting in speech] than anything else in my intelligence career." Nor has the capability been developed in the intervening years, according to Campbell's report.

Thus, while faxes, telexes, e-mail, and computer traffic are subject to automatic processing and analysis, phone calls are not--although the phones of the parties involved in a call can be automatically identified and voice-prints can be used to identify who is speaking.

Congressional intelligence oversight committees have recently lambasted NSA for its failure to adequately modernize its operations. Last year, the House Permanent Select Committee on Intelligence (HPSCI) stated that as result of NSA's failure to address process and management problems, "The committee believes that NSA is in serious trouble." Later that year, Cong. Sanford Bishop Jr., a Democrat from Georgia, said that although NSA is facing "tremendous challenges coping with the explosive development of commercial communications and computer technology . . . [the agency] has not demonstrated much prowess in coping with the challenge."

A year earlier, on October 5, 1998, HPSCI Staff Director John Millis told the Central Intelligence Retirees Association, "Signals intelligence is in a crisis. . . . In the past four or five years technology has moved from being the friend to being the enemy of SIGINT." Millis went on to suggest that the United States "shouldn't be spending one more dollar than we do to try and intercept communications . . . from space."

That judgment is reinforced by a number of articles, the most prominent one by investigative journalist Seymour Hersh in the December 6, 1999 *New Yorker*, which have painted a picture of NSA as an organization facing serious challenges. At least three developments have reduced NSA's ability to collect and process communications.

One is the expanding use of fiber-optic cables. Any signal sent through the air can be snatched out of the air, but signals transmitted on fiber optic cannot. Tapping them has also apparently proven a major challenge

in ways that tapping conventional cables has not, according to Campbell's report.

A second problem is the quantum leap in the sophistication of encryption software. A September 16, 1999 cabinet-level report to President Clinton noted that "for the strongest form of encryption, only the intended recipient can unscramble the message and read the original plain text, unless someone else has gained access to the corresponding decoding software and decryption key."

The explosion in communications volume, because of the widespread use of cell phones, faxes, and the Internet, is also a problem. As communications increase, the percentage of messages containing valuable intelligence drops, and finding that information becomes more and more difficult. Hersh reports that daily satellite telephone calls in the Arab world, many of which are encrypted, number in the millions.

Checks and balances

Even if it becomes widely accepted that Echelon is not a technological Big Brother, individuals across the political spectrum are likely to remain concerned about violations of individual privacy. The NSA and its allies clearly do intercept an enormous volume of data. And a breakthrough in word-spotting or other technologies that would allow upgrades to Echelon certainly cannot be ruled out. In addition, many have not forgotten NSA's role in monitoring the activities of dissidents during the Vietnam War, which Bob Woodward disclosed in the October 13, 1975 *Washington Post.* And Hager revealed that in the past Britain's Government Communication Headquarters gathered communications intelligence on Amnesty International, apparently through the Echelon network.

The recent controversy over Echelon has led both Australian and Canadian authorities to issue unprecedented statements--acknowledging for the first time their participation in the UKUSA alliance and stating that precautions are being taken to safeguard the privacy of their own citizens as well as those of the other UKUSA nations.

In a letter to the Australian news program *Sunday Nine*, Martin Brady, director of the Defense Signals Directorate, revealed the existence of a classified directive, "Rules on SIGINT and Australian Persons." The directive, with certain exceptions, prohibits the deliberate interception of communications between Australians in Australia, the dissemination of information on Australians gained accidentally during the course of routine collection on foreign communications, and the reporting or recording of the names of Australians mentioned in foreign communications.

In his 1997-98 report, the commissioner of the Canadian Communications Security Establishment reported that policies existed which required his employees "to conduct their operational activities in strict recognition of . . . the rights, privacy, and freedoms of Canadians." He also noted the existence of a reciprocal agreement whose purpose was

to ensure that UKUSA nations did not "circumvent their own legislation" by targeting the communications of each other's citizens by request. "They do not do indirectly what would be unlawful for them to do directly," the commissioner wrote.

The guidelines under which NSA operates require that if it incidentally obtains a communication from or to a U.S. citizen or organization in the United States for which there is no warrant or court order, the agency can retain the message but must remove the name of the citizen or company. There are several exceptions--for example, the name can be retained if NSA officials believe it is "necessary to understand foreign intelligence information or assess its importance" or if the intercept indicates that the individual "may be an agent of a foreign power."

Such guidance is the subject of U.S. Signals Intelligence Directive 18, "Limitations and Procedures in Signals Intelligence Operations of the USSS"--one of a number of classified directives issued by the Director of NSA that guide the operation of U.S. Signals intelligence activities. A redacted version from 1980 notes that the purpose of the 50-page directive is to "ensure that the SIGINT mission of the National Security Agency . . . is conducted in a manner that guarantees proper safeguards to the rights and privacy of U.S. persons." Four sections of the October 20, 1980 directive, portions of which were blacked out when the document was released in response to a Freedom of Information Act request, concern the guidelines on the collection, processing, storage, and dissemination of the communications of U.S. citizens.

Two challenges

Evidence that these guidelines do reach down to the collectors can be found in the 1991 navy regulation concerning Sugar Grove. The commander of the site, in addition to being instructed to operate an Echelon site and to "[gather], process, and report intelligence," is ordered to "ensure the privacy of U.S. Citizens are [sic] properly safeguarded pursuant to the provisions of USSID 18."

But many, including Congs. Goss and Barr, want more reassurance than is provided by these documents. Goss requested, on behalf of the HPSCI, all legal opinions and guidance provided by NSA's legal office to NSA's operations staff and others--which could demonstrate how the agency is applying the laws that restrict their collection of information about American citizens. NSA argued that some of the documents could not be provided due to "government attorney-client privilege." Discussions between the two parties are continuing.

Further, the November 5, 1999 conference report on the intelligence authorization act directed the director of NSA, the director of Central Intelligence, and the attorney general to prepare a report, in classified and unclassified forms, providing a detailed analysis of the legal standards employed by the intelligence community in signals intelligence operations. The report is to cover standards for the acquisition of SIGINT about Americans as a result of U.S. Signals intelligence operations as well as those of U.S. allies.

In recent years, NSA has reduced some of the secrecy surrounding the agency and U.S. SIGINT operations. But it faces two challenges--providing needed intelligence in the face of new technological challenges and convincing both critics and friends that it will do so without infringing on basic freedoms. To do the latter it may have to open up even more.

Jeffrey Richelson is a senior fellow with the National Security Archive, Washington, D.C. Some documents pertaining to Echelon can be found at www.gwu.edu/~nsarchiv.

1. Desmond Ball, *Australia's Secret Space Programs* (Canberra: The Australian National University, 1988), pp. 5, 18, 36; Nicky Hager, *Secret Power: New Zealand's Role in the International Spy Network* (Nelson, N.Z.: Craig Potton, 1996), pp. 34-35; Duncan Campbell, "Careful, They Might Hear You," *The Age,* May 23, 1998; communication from Duncan Campbell, January 4, 2000.

2. Nicky Hager, *Secret Power,* p.39; Duncan Campbell, *Interception Capabilities 2000* (Luxembourg: European Parliament, 1999), p. 7.