

British key in 'Echelon' controversy

A decades-long global electronic spy scandal is being put in the spotlight, both in Europe and the United States. Edward Spannaus reports.

In mid-April, the European Parliament is expected to create a special committee of inquiry into the global surveillance system operated by the United States and Great Britain which has become known as "Echelon."

The push for the investigation came after a period of weeks during which the news media in Europe, and to a lesser extent in the United States, had featured coverage of the Echelon project, which involves global signals intelligence (SIGINT) and communications intelligence (COMINT) collection by a consortium led by the United States and Britain, and which also includes Canada, Australia, and New Zealand, called "UKUSA."

Two reports commissioned by the European Parliament have warned that the Echelon system routinely intercepts all telephone, e-mail, and fax communications within Europe, and that information of value is then provided primarily to U.S. intelligence agencies.

Within the European Union (EU) and the European Parliament (EP), there is particular anger toward Britain, for its alleged "divided loyalties" and its betrayal of its European allies. EP members contend that Britain is in violation of Article 11 of the Amsterdam Treaty, which obligates member-states to "refrain from any action which is contrary to the interests of the Union."

Speaking on behalf of EU governments and the EU Council of Ministers on March 30, Portuguese Interior Minister Fernando Gomez said, "The Council cannot accept the existence of this kind of system, which does not respect the legal requirements of the member-states."

And during the debate, a French EP member declared: "We're told that the European Union is threatened by Jörg Haider's Austria, but it's the Great Britain of Tony Blair that is the real threat."

There is no doubt that the Echelon issue is being used for political and intelligence warfare—between France, on the one side, and Britain and the "Anglo-American powers," on the other; between the United States and Britain; and also within the U.S. intelligence community itself. One important context is the pattern of deterioration of relations between the United States and Europe—in which the British play both the role of instigator, and the intended beneficiary.

Before discussing the specifics of the current Echelon controversy in Europe and the United States, we will first review the background of British-U.S. cooperation on communications intelligence—which shows the danger of the British role for the United States as well for as continental Europe.

The 'special relationship'

The most important feature of the Echelon controversy, from the standpoint of U.S. patriots, is the treacherous "special relationship" between U.S. and British intelligence, which is reflected in the 1947 "UKUSA" agreement.

That agreement was an extension and formalization of the SIGINT cooperation between the United States and Britain and the the British Commonwealth countries, during World War II. The first formal agreement had been made in 1943, and was called BRUSA (Britain-U.S.A.).

In 1946, a leading American cryptographer, William Friedman, visited what he called his British "cousins" in London to work out postwar collaboration and cooperation, and a joint Liaison Office was established; this involved the exchange of both information and personnel.

For Franklin Delano Roosevelt, the war-time alliance with the United Kingdom and Winston Churchill was a necessary expedient; Roosevelt was emphatic that the war was not being fought to preserve the British Empire or to perpetuate colonial policies. But with FDR's untimely death in 1945, his successor, Harry Truman, abandoned FDR's postwar vision, and willingly accepted Churchill's call for an Anglo-American "special relationship" against the rest of the world, which Churchill delivered in Fulton, Missouri in March 1946.

Thus, in 1947 Britain and the United States signed the U.K.-U.S.A. Security Agreement, also known as "UKUSA," or the "Secret Treaty." With a year, the other signatories—Canada, Australia, and New Zealand—had joined, and the world was divided up into areas of responsibility for SIGINT collection. Subsequent agreements provided for standardized codewords, security agreements, and procedures for dissemination of information. The two principal agencies involved are the U.S. National Security Agency and Britain's Govern-

ment Communications Headquarters (GCHQ) at Cheltenham.

In the definitive work on the subject, *The Ties That Bind*, by Jeffrey Richelson and Desmond Ball, it is reported that within the UKUSA intelligence community, there have developed extremely close personal ties among senior officials of the relevant SIGNIT agencies (e.g., the U.S. National Security Agency [NSA], GCHQ), and also informal arrangements for information-sharing and joint action, in addition to the formal arrangements.

(This is reminiscent of former U.S. Secretary of State Henry Kissinger's famous confession in his speech at London's Chatham House on May 10, 1982, that during his tenure in the Nixon and Ford administrations, "I kept the British Foreign Office better informed and more closely engaged than I did the American State Department." The treasonous Kissinger also remarked, "Our postwar diplomatic history is littered with Anglo-American 'arrangements' and 'understandings,' sometimes on crucial issues, never put into formal documents.")

The authors of *The Ties That Bind* also report that what they call "the UKUSA security and intelligence community," because of its multinational character, its personal relationships, and its "extraordinary network of written and unwritten agreements," is able "to shroud itself in secrecy and to invoke the mantle of 'national security' to an extent unmatched by even the national defence establishments." The UKUSA community is also able, they wrote, to carry out extreme and violent covert operations which are generally prohibited by national and international law.

Loopholes

This "special relationship" between the United States and Britain and its junior partners, embodied in the UKUSA agreement, is understood by many investigators and observers to provide a legal loophole, through which surveillance of U.S. citizens can be routed through the British, and through which surveillance of British subjects (Britain doesn't have "citizens") can be conducted by the Canadians, and so forth—thus providing a level of "deniability" to the respective governments and their intelligence agencies.

The loophole, according to *Puzzle Palace* author James Bamford and others, works as follows.

The Foreign Intelligence Surveillance Act (FISA), passed in 1978, speaks of "acquisition," which is undefined in the statute. To fill this gap, the NSA has defined it as "interception by the National Security Agency through electronic means of a communication." Thus, information acquired by Britain's GCHQ, or one of the other UKUSA parties, and then passed to U.S. agencies, is *not* covered under the act.

The use of the term "through electronic means," would also make it legal for the NSA to receive, for example, hand-delivered tapes or computer disks of transmissions provided by private communications carriers. This was in fact the way

that the SHAMROCK and MINARET programs worked, when copies of transmissions, and, later on, tapes, were delivered to NSA or GCHQ.

It was known before the passage of FISA in 1978, that the NSA obtained data by both these methods—non-NSA, and non-electronic. A secret Justice Department report in 1976 stated that MINARET intelligence was obtained through "the receipt of GCHQ-acquired telex and ILC cable traffic"—where ILC referred to International Licensed Carrier, such as Radio Corp. of America (RCA), International Telephone and Telegraph (ITT), etc.

That, by the way, was an official acknowledgement—by the U.S. Justice Department—that the British were part of the program of interception of communications from U.S. citizens and organizations.

SHAMROCK and MINARET

SHAMROCK was the name of a program begun in 1945, under which the three major U.S. cable companies—Western Union, ITT World Communications, and RCA Global—provided to the NSA and its predecessor, copies of all cable traffic entering and leaving the United States. Western Union and ITT gave the NSA microfilms of cable messages; RCA provided NSA with the most thorough cooperation, handing over complete copies of all cables, and later, magnetic tapes, when its operations were computerized.

The NSA product was provided at first only to agencies involved in foreign intelligence. But, in the early 1960s, the Justice Department and FBI provided names to the NSA so that NSA could expand its "watchlist" to include Americans believed to be involved in certain domestic criminal and political activities. In 1967, Maj. Gen. William Yarborough, the Army's Assistant Chief of Staff for Intelligence, requested information pertaining to civil disturbances, and during the late 1960s until the Congressional investigations of the mid-1970s, the Army, CIA, FBI, and DIA all were sending requests for intercept intelligence to the NSA, the subjects of which included domestic anti-war and civil rights activists, including Rev. Martin Luther King.

The domestic surveillance program was formalized under the code name MINARET in 1969, pertaining to, *inter alia*, "individuals who may foment civil disturbance or otherwise undermine the national security of the United States." As noted above, not only the NSA but also the British GCHQ provided intercepts which were then passed on to other U.S. intelligence agencies.

Congressional investigations

The role of the NSA in illegal domestic surveillance only became public in the mid-1970s; it was the post-Watergate Congressional hearings which put it in the public spotlight. A few months before that, the Rockefeller Commission (the "Commission on CIA Activities Within the United States") had issued a weak-kneed report which made vague reference

to the monitoring of telegrams handled by U.S. cable companies.

In August 1975, the House Select Committee on Intelligence Activities, headed by Rep. Otis Pike (D-N.Y.), held hearings on NSA domestic surveillance, in the course of which CIA Director William Colby disclosed NSA's interception of international communications, and during which NSA Director Lt. Gen. Lew Allen testified in an open hearing for the first time.

In October 1975, when Allen was called to testify before the Senate Select Committee on Intelligence Activities—known as the “Church Committee” for its chairman, Sen. Frank Church (D-Id.)—the world learned for the first time of the SHAMROCK AND MINARET programs by name.

Church opened the hearing on Oct. 29, 1975 by announcing that the committee was beginning public hearings on the NSA, noting that even “the agency name is unknown to most Americans.”

“Just as the NSA is one of the largest and least known of the intelligence agencies, it is also the most reticent,” Church said. “While it sweeps in messages from around the world, it gives out precious little information about itself.” And, in a bit of understatement, Church commented, “Even the legal basis for the activities of the NSA is different from other intelligence agencies,” in that there is no statute, only Executive Orders, governing the activities of the agency. “Today, we will bring the agency from behind closed doors,” Church announced.

General Allen did not mention SHAMROCK or MINARET in his testimony. He did discuss the substance of MINARET, the “watch list” surveillance in which requests were made by other agencies, including the FBI and military intelligence agencies, beginning in the early 1960s, for foreign communications of designated U.S. citizens and organizations.

However, following Allen's testimony, the terms SHAMROCK and MINARET were cited by Senators, and SHAMROCK was discussed in general terms. Shortly thereafter, overriding objections from President Gerald Ford, and a plea from Attorney General Edward Levi, on Nov. 6, 1975, the Senate Committee made public its report on SHAMROCK.

In response to the Rockefeller Commission report, and in the wake of a brawl with a House Government Operations subcommittee chaired by Rep. Bella Abzug (D-N.Y.), Attorney General Levi established a top-secret task force to investigate questionable or illegal electronic surveillance, including SHAMROCK and MINARET.

The resulting Justice Department report was classified at the level of Top Secret Codeword, and only two copies were printed; it was delivered to George W. Calhoun, the chief of the Department of Justice Criminal Division's Special Litigation Section, from whence a shorter “prosecutive summary” was given to Criminal Division head Benjamin Civiletti. It recommended that no prosecutions be conducted, and that the DOJ's investigation of the legality of the pro-

grams be terminated.¹

The Justice Department's investigation was terminated, but it seems clear that the NSA's “watch list” program was not.

Echelon, specifically

Although the term “Echelon” is often used, especially in journalistic accounts, as interchangeable with the entire UKUSA surveillance network, it actually refers to a specific component of the overall program.

The specific Echelon program has reportedly existed since the early 1970s, and it is in fact a continuation of the “watch list” program. Echelon provides for automated processing, or “sifting,” of intercepted COMINT; extensive further automation of Echelon was carried out in the mid-1980s, under NSA Project P-415.

Jeffrey Richelson, an authority on U.S. intelligence capabilities, states that Echelon is *not* the same as the UKUSA “global surveillance network.” Rather, it is the system which links together the computers known as “dictionaries” at UKUSA ground stations, which contained pre-programmed keywords. They sift through millions of intercepted messages for those containing the pre-programmed keywords, and then forward those particular messages to the requesting agency.

Political and intelligence warfare

Currently, the Echelon controversy has been given much play in the French press, but also in Britain, Italy, and other countries in Europe. Inside the United States, it has been covered in some major news media, but with the most intensive coverage on Internet sites and other media outlets of both liberal and right-wing libertarian groups.

Sources in the United States indicate that there is a fight going on between elements of the CIA, and the NSA—an agency which overwhelms the CIA and the rest of the U.S. intelligence community in terms of its size and budget. It is suggested that certain groups within the U.S. intelligence community believe that the NSA's enormous capability to surveil and monitor U.S. citizens should not go unregulated and unsupervised.

An indication of this may be, that the two most prominent spokesmen exposing Echelon in Congress and demanding hearings are Reps. Bob Barr (R-Ga.), and Porter Goss (R-Fla.), both former CIA officers. And the most outspoken private groups that have published lengthy reports on Echelon over the past year or two, are organizations historically linked to intelligence-spook Richard Mellon Scaife—Paul Weyrich's Free Congress Foundation, and Joseph Farah's WorldNetDaily.

In the U.S. Congress, hearings are planned for late spring

1. The Special Litigation Section was the predecessor of the General Litigation and Legal Advice Section (GLLAS). See Lyndon H. LaRouche, Jr., “He's a Bad Guy, But We Can't Say Why,” *EIR*, March 10, 2000, footnotes 29, 30, 41.

or early summer, to be held by the House Government Reform Committee.

Echelon product is shared

In France, the news media have highlighted allegations of industrial espionage by the United States, targeting European companies with the help of the British. However, it is curious that the actual EP report, on which these allegations are based, was written not by a Parliamentary committee or staff, but by a British journalist, Duncan Campbell. Moreover, the sole documentation for the reports of alleged commercial espionage (the use of intercepted communications to favor U.S. companies over European companies), derives from news media accounts.

There is also a degree of irony in the vociferousness of the allegations coming from France, because it is well known that the French are no strangers to the ways of surveillance in general, and to commercial espionage in particular.

A further paradoxical element of the cries of outrage coming from western Europe, and especially France, is that much of the Echelon product is shared with NATO members. But, France is in an even better position: According to a reliable U.S. intelligence source, France has access to everything Echelon gathers, through its “friends” in the UKUSA arrangement, most notably Canada.

Moreover, the EP report itself states that the French intel-

ligence service DGSE operates a number of communications intelligence collection sites—at locations within France, in New Caledonia in the South Pacific, and in the United Arab Emirates.

In addition, Germany and France collaborate in the operation of a COMSAT collection site at Kourou, Guyana (formerly French Guyana), targeting U.S. and South American satellite communications.

The French weekly *Le Point* has reported that information obtained from the French satellite surveillance goes directly to French corporations.

Industrial espionage

The EP report cites a number of specific incidents of industrial espionage by the United States; it is these allegations which have gotten the most coverage in the press—but, in fact, they all come from the press in the first place.

As background, the report says that in 1977, NSA and CIA officials met with the U.S. Commerce Department to create a liaison office to channel secret COMINT and SIGINT into the Commerce Department. The source cited in the EP report is—a British television program.

(A U.S. source who has long been involved with both telecommunications in the private sector, and with civilian oversight of intelligence activities, scoffed at this allegation, pointing out that in the 1970s, U.S. intelligence was singularly

EIR SPECIAL REPORT

The True Story Behind The Fall of the House of Windsor

Reprints of EIR's 1994-1997 groundbreaking exposés

What political battles lie behind the assassination of Princess Diana? Why do 22 out of 30 top terrorist groups have their headquarters in London? EIR's series on the House of Windsor is indispensable for understanding today's news.

- The Coming Fall of the House of Windsor** (Oct. 28, 1994)
- The Sun Never Sets on the New British Empire** (May 24, 1996)
- Britain's "Invisible" Empire Unleashes the Dogs of War,** (Aug. 22, 1997)
- Epilogue: Can the House of Windsor Survive Diana's Death?** (Sept. 12, 1997)

Order from:

EIR News Service

P.O. Box 17390 Washington, D.C. 20041-0390 Order number EIR 97-004 **\$75**



focussed on the Soviet Union, and he states unequivocally that no such thing as described in the EP report, ever happened.)

The EP report further quotes from a 1996 *Baltimore Sun* article citing former intelligence officials saying that tips based on spying flow regularly from the Commerce Department to U.S. companies, to help them win contracts overseas.

The examples given by the report are:

- Intelligence was gathered by the U.S. National Security Council concerning Middle East sales of the European Pannavia aircraft company; the source is former NSC official Howard Teicher, speaking on a BBC program.

- NSA is alleged to have intercepted phone calls between the French firm Thomson-CSF and Brazil, concerning a surveillance system for the Amazon rain forest and alleged bribes by Thomson-CSF officials paid to Brazilian officials. No source is given for this allegation—except that the U.S. competitor, Raytheon, put out a public press release acknowledging Commerce Department support for their efforts on this project.

- The NSA is said to have intercepted faxes and phone calls between the European Airbus consortium and the Saudi national airline and government, learned that Airbus agents were offering bribes to Saudi officials, and passed the information to Boeing and McDonnell Douglas Corp. officials. The documentation is a 1995 *Baltimore Sun* article.

- Under the category of international trade negotiations, the EP report says that the U.S. government is said to have targeted data on emission standards of Japanese vehicles (source: a 1994 *Mother Jones* article by Robert Dreyfuss), and information about the imports of Japanese luxury cars (source: *Financial Post* of Canada, 1998), information about French participation in the General Agreement on Tariffs and Trade negotiations in 1993 (no source), and about the 1997 Asia-Pacific Economic Cooperation conference (no source).

Unofficial admission

Throwing fuel on the fire, was a March 16 *Wall Street Journal* commentary entitled “Why We Spy on Our Allies,” written by loudmouth Washington lawyer, Anglophile, and one-time CIA Director James Woolsey.

“Yes, my continental European friends, we have spied on you” Woolsey wrote—but not to obtain technology from European companies, which he claims “isn’t worth our stealing.” Citing the EP report on Echelon, Woolsey says, “We have spied on you because you bribe,” and he arrogantly explains: “Your companies’ products are often more costly, less technically advanced or both, than your American competitors’. As a result you bribe a lot.”

Woolsey then says that when we catch you at it, we don’t go to the U.S. companies that are competing for contracts, but instead, “we go to the government you’re bribing and tell its officials we don’t take kindly to such corruption.”

Woolsey then explains, clearly speaking on behalf of the British side of Echelon, and backing the British system of

economics over the American system:

“Why do you bribe? It’s not because your companies are inherently more corrupt. Nor is it because you are inherently less talented at technology. It is because your economic patron saint is still Jean-Baptiste Colbert, whereas ours is Adam Smith.” Despite some reforms, Woolsey continues his lecture, “your governments largely still dominate your economies. . . . You’d rather not go through the hassle of moving toward less *dirigisme*. It’s so much easier to keep paying bribes.”

Changing capabilities

Finally, one more irony of the current controversy over Echelon should be noted, which is that, according to many sources, government intelligence organizations are falling behind technologically in both encryption technology and the capacity to intercept and process large quantities of data. So, contrary to the “tin foil hat” crowd which believes the government is listening to their every conversation and reading every e-mail, it is in fact getting harder for the NSA and other agencies to keep up.

Telephone and voice communications present the biggest problems for COMINT agencies. Tapping a specific phone line is one thing; picking targeted individuals or conversations out of the air is something quite different. A great deal of resources have been devoted to the development of speech recognition systems, word-spotting, speaker-identification systems, and the like, but most accounts and sources agree that such systems still operate with a high degree of error.

Fiber-optic cable transmissions also present significant problems. Their signals cannot just be plucked out of the air, as can satellite transmissions, but they require a physical tap. Some sources say that tapping fiber-optic cables is impossible, but others say it can be done, but that the sheer volume of data transmitted per cable poses major problems of processing and handling, involving trillions of data-bits per second.

In other words, as technology advances, SIGINT and COMINT isn’t getting easier; it’s in fact getting much harder to carry out.

References:

- James Bamford, *The Puzzle Palace* (Boston: Houghton Mifflin Co., 1982).
Duncan Campbell, “Interception Capabilities 2000” (Luxembourg: European Parliament, 1999).
Jeffrey Richelson and Desmond Ball, *The Ties That Bind: Intelligence Cooperation between the UKUSA Countries—the United Kingdom, the United States of America, Canada, Australia, and New Zealand* (Boston: Allen & Unwin, 1985).
Jeffrey Richelson, *The U.S. Intelligence Community* (Cambridge, Mass.: Ballinger Publishing Co., 1985).
L. Britt Snider, “Unlucky Shamrock: Recollections from the Church Committee’s Investigation of NSA,” *Studies in Intelligence* (Washington, D.C.: Central Intelligence Agency, Winter 1999-2000).
U.S. Senate, Hearings before the Select Committee to Study Government Operations with Respect to Intelligence Activities, Vol. 5, “The National Security Agency and Fourth Amendment Rights,” 1975.