

# Revelations about Echelon spy network intensify US-European tensions

By Steve James  
12 April 2000

The British government is losing its fight to suppress debate in the European Parliament on the role of US intelligence gathering, particularly a spy system known as Echelon in which the UK has long been a crucial partner.

Last week, 171 out of 626 European MPs signed a petition calling for two further debates and a public commission of inquiry into Echelon. This easily exceeded the 160-signature requirement to inaugurate an inquiry, and was supported by the regionalist UK parties—the Scottish National Party and the Welsh Plaid Cymru, along with the Green party. Labour, Conservatives and Liberal Democrats all fiercely opposed it.

The debate threatens to undermine the UK's efforts to integrate more fully into Europe while maintaining close economic and military connections with the United States. It would expose Britain's role as an American ear in Europe.

The call for an inquiry into Echelon was led by the Portuguese presidency of the European Union (EU)—each country holds the post for six months—after several years during which Echelon has emerged from complete obscurity to become a source of economic and political tensions between the United States and Europe.

Echelon is an information processing system that relies on a network of spy satellites and ground listening stations operated under the terms of a 1947 UK-USA treaty. Full details of the agreement remain secret, but it was intended to build on the transatlantic intelligence cooperation established during World War II. It was aimed primarily at spying on the Soviet Union and Warsaw Pact countries of Eastern Europe. The network also monitored parties, groups and individuals opposed to aspects of US and British foreign policy.

The UK-USA treaty allows the US National Security Agency (NSA) and the British Government Communication Headquarters (GCHQ) to share information and resources. A series of spy bases were established, the most important being Menwith Hill on the North Yorkshire moors in England, which is directly linked with the NSA headquarters in Fort Mead, Maryland. Other listening posts were set up around the globe, as other countries became involved in spying operations. Canada, Australia and New Zealand were significant participants in the scheme, along with Turkey, Germany, Denmark, Norway, South Korea and Japan.

Over the years, the system has acquired an extraordinary degree of sophistication and information gathering capacity. Ground-posts collect transmissions picked up from spy satellites, the first of which was launched in 1968. Menwith Hill alone has around 30 radio receivers pointing in different directions, indicating it is receiving data from many different satellites. The system can monitor telephone conversations, faxes, email and cell phones, and can decrypt secure communication and generally intercept most transmitted data.

Using "dictionary" programmes to sift through the billions of transmissions received every hour, the Echelon system attempts to identify information of interest to the spy services and their national governments.

Following the collapse of the Soviet Union and the end of the Cold War, Echelon has been increasingly reporting on so-called "economic" intelligence. It is this, and not the subversion of the democratic rights of the world's citizens, which has provoked opposition from some EU governments. They have become concerned that European companies are losing contracts to US companies because of information supplied by Echelon.

In 1998, the European Parliament received a report it had commissioned—"An Appraisal of the Technologies of Political Control"—by Steve Wright of the Omega Foundation, a UK-based human rights organisation. Wright comprehensively summarised developments in crowd control, sub-lethal weapons, torture, prison control, DNA databanks, and mass surveillance. Within the last category, he reviewed Echelon and noted the decades of effort by investigative journalists who had painstakingly collected and collated data on the system. Wright was highly critical of many aspects of European policy, including the export of torture and sub-lethal crowd control equipment, and the formation of an all-European spy organisation, Enfpopol.

In September 1998, when the European Parliament debated the matter, very little of Wright's report was mentioned. However, a resolution was passed which called for "surveillance technologies to be subject to proper open debate both at national and EU level, as well as procedures which ensure democratic accountability".

The resolution, a copy of which was forwarded to the US

Congress, went on to state, in point 14: "[The European Parliament] considers that the increasing importance of the Internet and worldwide telecommunications in general and in particular the Echelon System, and the risks of their being abused, require protective measures concerning economic information and effective encryption."

In February this year "Interception Capabilities 2000", another report prepared by the European Parliament's Justice Committee with assistance from investigative journalist Duncan Campbell, focussed more closely on Echelon and other communication interception systems. This report comprehensively charted the growth of the network of ground-bases and satellite surveillance (presently around 120 satellite systems are thought to be in operation). Submarine telephone cables have been subject to interception from 1971 onwards.

The Internet is particularly vulnerable to surveillance, because the majority of its traffic passes through the US at some point. Even data packets transmitted between addresses outside the US often pass through American-based routers. There are nine points at which this traffic is routinely picked up. From 1995, the NSA has employed "packet sniffer" software to identify traffic of interest to its sponsors. Leading US software companies are also implicated. Campbell stated that Netscape, Microsoft and Lotus reduced the encryption capacities of their exported versions of e-mail packages to facilitate NSA decryption.

Section 5 of the report deals with "economic intelligence" and cites a series of instances in which European-based companies have been undermined in favour of US outfits. In 1993, the "Panavia European Fighter Aircraft" was specifically targeted. In 1994, the French company Thomson CSF lost a \$1.3 billion contract to Raytheon of the US after the NSA intercepted their phone calls. In 1995, the European Airbus Company lost a \$6 billion contract to Boeing, after the NSA intercepted its fax transmissions. Campbell stated that there have been numerous other instances when the US has used information picked up by the NSA operations during trade negotiations.

The publication of this report has brought both transatlantic and inter-European disputes to a head. France, which operates its own advanced electronic spy system, has been particularly vociferous. Former Interior Minister Charles Pasqua, a member of the EU Justice Committee, said, "The rules of the game are rigged and they are rigged especially by the British. This is shocking." French Justice Minister Elisabeth Guigou warned European companies, "Communications must never carry vital information, especially when the link is made via a satellite." French lawyer Jean-Pierre Millet is launching a class-action court case against the British and US governments, pointing to Echelon's role in undermining French and European commercial and trade negotiations.

On March 30, Erkki Liikanen, EU Enterprise and Information

Commissioner, told the European parliament that efforts to establish the EU in the "knowledge economy" depended on electronic communication that could be trusted, and that encryption was the key to this. European encryption should challenge US technology. Liikanen alluded to the suspicions of there being built-in decryption facilities in US software: "Software whose source code is not open, leaves the user in uncertainty, the possibility of built-in circumvention of encryption cannot be excluded."

Liikanen reported that the US government had denied they were involved in any industrial espionage. But a more frank and bellicose assessment of US operations came from James Woolsey, CIA chief from 1993 to 1995. Writing in the *Wall Street Journal* the week before, Woolsey said, "That's right, my continental friends, we have spied on you because you bribe. When we have caught you at it, you might be interested, we haven't said a word to the US companies in the competition. Instead we go to the government you're bribing and tell its officials that we don't take kindly to such corruption."

Woolsey's astonishing outburst—justifying spying on the grounds of European corporate corruption—makes clear that the Echelon revelations, and the transatlantic encryption war now being joined, mark a new and noisy low in US/European relations. European corporate interests will not tolerate having all their internal and external discussions monitored, particularly when they are up against US rivals, as is the case in all strategic areas of economic life.

At the same time, the European governments' new emphasis on encryption poses them with a fresh dilemma. How can they defend corporate, financial and state security from US spying without prejudicing the interception and surveillance efforts directed against their own citizens by all European governments?

The British government seized on this quandary to declare its preference for a discussion that would "cover the issue in the round, rather than focusing on just one member state [Britain]. There is no incompatibility between our position as an EU member state and our duty to maintain national security. Others are in the same position."

To contact the WSW and the  
Socialist Equality Party visit:

<http://www.wsws.org>