European Parliament concludes Echelon electronic spy network does exist

Mike Ingram
6 June 2001

A report issued by the European Parliament last week advises the use of encryption software to protect electronic communications against the Echelon spy network. Against continued US denials, the report concluded that the spy network does exist and that its primary purpose is to intercept private and commercial communications, not military intelligence.

During the Cold War, the Echelon information processing system, using a network of spy satellites and ground listening stations, was used primarily to spy on the Soviet Union and Warsaw Pact countries of Eastern Europe. But the European Parliament was pressed to investigate the network after numerous allegations were made that the US was using its spy system to obtain "economic" intelligence on behalf of US corporations following the collapse of the Stalinist states.

Reporting back on its investigation, the European Parliament's vice-president Gerhard Schmid said, “What we cannot deny or prove is that information is passed on to companies. The problem is there are no tracks or traces of interception.” But he added that the committee's inquiry had found evidence that Echelon existed and is run by the US in co-operation with Britain, Canada, Australia and New Zealand.

In contrast to an earlier parliamentary study last year, which found that Echelon listens in and intercepts “billions of messages per hour, the new report claims that “only a small portion” of global telephone, e-mail and fax transmissions are being tapped.

The seven-month investigation heard testimony by security experts from Britain, the US, Australia, Canada and New Zealand. It established that Echelon was set up in the 1950s by the intelligence services of the US and Britain, and was later joined by Canada, New Zealand and Australia. During the Cold War, a worldwide network of listening posts were established, which are still in operation.

Echelon is said to be capable of intercepting electronic messages sent across the world either by cable or by satellite. The latest report claims that interception is largely limited to satellite communications. But this makes no sense, as it would be too easy for targeted companies or individuals to avoid surveillance.

In an interview with *Radio Netherlands*, parliamentary committee member Jan Marinus Wiersma said, “By using keywords with a kind of search engine, they randomly intercept a lot of communications in order to find certain messages or certain e-mails, in which certain words are used.”

The report says that only a small number of these messages then land on the desks of intelligence officers, who analyse them before passing them on to other government services. The committee says that the system appears to be mainly used to intercept criminal or terrorist information, or messages from so-called "rogue states" such as Iraq or North Korea.

The European Parliament does not object to the use of Echelon for these purposes, and Wiersma points out that France is believed to operate a similar system. “You need to have the capability to intercept, to find out what the criminals are doing, or the terrorists, or the rogue states. So, I think in principle, there's nothing against having such a system in the framework of your security systems. But it should be organised in such a way that it's not used for industrial espionage or in a harmful way for private citizens.”

It is the allegation that the spy network is being used to gain commercial advantage for US corporations over their European rivals, rather than any concern for individual privacy, that lead to the publication of the present report.

Echelon's operations, based at Fort Meade in Maryland in America and at Britain's GCHQ spy centre in Cheltenham, were first made public by ex-CIA director James Woolsey in an interview with the French newspaper *Le Figaro*. Woolsey said that Echelon was being used to track electronic messages sent by European companies. While he insisted that the intelligence services were motivated by the need to check for corruption and sanctions busting, allegations of industrial espionage quickly followed.

European demands for an investigation into Echelon coincided with the emergence of increased trade rivalry between Europe and the US in the aftermath of the collapse of the Soviet Union and of Eastern Europe. Investigators met with open hostility when they went to Washington last month to meet with officials and the intelligence agencies. Both the CIA and the National Security Agency, believed to be responsible for Echelon, refused to meet them.

It is not only relations between the US and Europe that have been worsened by the investigation, but also those between the European Union (EU) and Britain. The report calls on EU member Britain to reconsider its link to Echelon, stating that it could be violating European human rights laws and its commitment to its 14 other EU partners.

“The Brits have a special relation with the US ... It could be a problem,” Wiersma said.

Echelon is only one of a number of such spy agencies internationally that routinely violate the privacy of millions of ordinary working people in the name of the “fight against terrorism”. In addition to its continued use of the Echelon network, Britain's Labour government under Prime Minister Tony Blair has established unprecedented surveillance over people's daily lives.

In April, Home Secretary Jack Straw announced the creation of a specialist police force supposedly to tackle computer-based crime. The new squad was established under the Regulation of Investigatory Powers Act (RIP), which came into force last year, and is based at a new £25 million National Technical Assistance Centre (NTAC). The job of the new force is to sift the information gathered through so-called “black-box” devices, which the law now requires Internet Service Providers (ISPs) to attach to their servers, allowing information to be filtered back to NTAC.

NTAC will thus have permanent links to ISPs based in Britain, making it easy to intercept email, chat sessions or any other data passing over the networks run by these companies. In an attempt to thwart the use of encryption software preventing monitoring, the RIP grants the police the power to demand the passwords and codes needed to read all encrypted messages. This also includes the codes used by business to protect credit card numbers in electronic commerce transactions. Failure to comply with a decryption notice will be a criminal office, unless the individual concerned can prove he or she did not have the ability to decrypt the message for any reason, such as losing the password.