



Echelon: How it works

29 Jun 2000 11:09

How does the covert arm of the intelligence services work? How does Echelon listen to and see what its targets are doing?

Espionage is a dark art, and the truth behind who's doing what to whom and for why rarely becomes apparent -- even to those involved. With Echelon, attempts to find out the essence or extent of the system is doubly dogged by the inherently complex nature of the technology.

However, in the absence of an operator's manual, press briefing or white paper, it is still possible to build up a reasonable picture of the nuts and bolts of the operation. Whether it is true or not is impossible to ascertain, and what follows is informed guesswork seasoned with some possibly relevant facts.

Echelon's function is to covertly intercept information and pass it to those who need to know. This breaks down into three stages: the collection of all possible intelligence, its analysis and contextualisation, and its redistribution. At each stage, there is little public information about what is actually even possible, let alone how much is used and where, but the basic systems must follow certain lines in order to work.

Echelon's main source of raw information is electronic signals. These can be carried on radio or on copper or fibre cables: with few exceptions, wireless signals can be best intercepted remotely while cables need a physical tap.

Wireless signals used by commercial and governmental concerns extend from very long wave transmissions through to microwaves, each waveband having its own characteristics. Most areas of interest are at VHF and higher frequencies, although shortwave has traditionally been heavily used and monitored by the military and intelligence agencies, its unreliability, low bandwidth and ease of monitoring has led to it falling out of fashion.

Echelon used to have many stations around the world capable of listening in to shortwave transmissions and precisely locating their position -- high frequency direction finding, HFDF or huffduff -- but these numbers have fallen. Most characteristic of these stations is the antenna, which looks not unlike an empty gasometer and is around the same size.

At VHF and above, radio signals rarely carry more than a couple of hundred miles at the most before being shielded by the curvature of the earth from ground-based monitoring stations. They are, however, detectable from space, and Echelon makes use of a wide variety of monitoring satellites -- you'll see references to such names as Ferret, Trumpet, Vortex and so on, but these aren't the names by which they're currently known. These can listen directly to mobile phones, or the microwave links that connect base stations to the central network, as well as to the microwave networks that many countries still maintain as part of their basic infrastructure. Although microwaves can be tightly focussed, using parabolic antenna in the same way that car headlights use a curved reflector, some signals always go past their destination and fire out into space and the waiting satellites -- this is thought to be a major source of information for Echelon.

A large part of Echelon is devoted to monitoring the Intelsat network of geostationary communications satellites, with ground stations in all of the UKUSA countries (and, rumour has it, work going on in Ireland pending that country's forthcoming

membership of the club this month). There are also ancillary stations near to the official Intelsat groundstations, monitoring spillage of microwave uplinks and downlinks. Inmarsat, the maritime satellite system, has links to the American government and contains its own monitoring system, and other satellites with nominally civilian purposes may also have components linked to Echelon, the NSA or other agencies -- a tradition extant since the very first US Discovery series of satellites. Signals collected by satellite aren't analysed to any great extent in situ, instead they are encrypted and beamed down to the UKUSA's network of monitoring stations for dissection. Each station has responsibility for a specific geographic region.

Some ground-based collection takes place, especially in cities where embassies, focal points of domestic microwave networks and other high concentrations of microwave links can be found. Here, for a change, some technical details are available -- companies such as [Applied Signal Technology](#) offer devices such as the Model 128B TDM Channel Analyser, a behemoth of a mobile phone monitoring device capable of processing 12,000 channels simultaneously. It is hard to think of many customers for this device outside security services operating indiscriminate signal capture regimes.

Cable tapping is harder to do covertly, although most countries have some history of installing listening devices to their own or conveniently unguarded enemy trunk lines. In the UK, all international phone, fax and data traffic is monitored along spur cables installed and maintained by BT -- whose Martlesham Heath labs have always had a major GCHQ involvement. Provisions in the [RIP Bill](#) extend that system to all domestic Internet traffic.

Once the information is gathered in raw form, it is sifted using various systems. Echelon is famous for having so-called dictionary computers that can perform massive keyword searches on intercepted text, with the word lists being shared among all the agencies. A dictionary at the [Waihopai station](#) station, New Zealand, would look for GCHQ words alongside its own list, while one at the UK's Morwenstow station would reciprocate.

Voice recognition remains a hotly-debated capability of Echelon. Systems capable of automatically triggering tape recordings on key words have existed for a while, but their reliability, scale and usability have never been established. Some automation is undoubtedly used, but it is unlikely to extend to full transcription of all calls.

We understand that a large proportion of Echelon's internal traffic uses much commercial off-the-shelf (COTS) equipment on its own global WAN -- a system that as recently as five years ago was bigger than the Internet at that time. It's known to use IP and very strong encryption, with dedicated fibre and satellite channels providing intercommunication between sites. Exactly what form of encryption is used depends on the nature of the data, with the most important information being encrypted through truly random one time pads (OTPs): a system still capable of offering unbreachable security if used correctly. High bandwidth, lower level information streams use algorithmic encryption developed by UKUSA cryptographers themselves -- and the system has some of the very best.

However, as with cryptography itself Echelon is fighting a losing battle. As more and more phones become low-power digital devices, the range over which they can be monitored and the effort needed to decode them increases, and a brand-new wireless technology called ultrawideband or pulse wireless -- already in use by the security services -- promises to make many transmission virtually undetectable. And that's before users really get into strong cryptography, a habit likely to spread as knowledge of Echelon's capabilities spreads. Its best years may be behind it, and it may be supplanted with global monitoring of public information such as security cameras and legal tapping of data networks.

Go to ZDNet's [Echelon Special](#)

The British are keeping a stiff upper lip, the US simply avoid mentioning it and the French believe *it* has been stealing secrets from France for years. Go to the [TalkBack](#) forum to tell us what you know and think about Echelon.

Story URL: <http://news.zdnet.co.uk/hardware/0,1000000091,2079849,00.htm>

Copyright © 1995-2006 CNET Networks, Inc. All rights reserved

ZDNET is a registered service mark of CNET Networks, Inc. ZDNET Logo is a service mark of CNET Networks, Inc.