

This extract was taken from Personal Computer World and written by Duncan Campbell.

Comms Surveillance

Data comms and electronic mail do pose special problems in relation to comms interception, since such messages (in contrast to telephone calls) are intrinsically 'machine readable'. Although British domestic communications (whether data or voice) are only supposed to be intercepted if a specific warrant is issued, few people comprehend the scale on which Western intelligence agencies are already routinely intercepting all civil international communications. As long ago as 1960, defectors from the United States NSA (National Security Agency also known as No Such Agency) revealed at a Moscow press conference that 'both enciphered and plain text communications are monitored from almost every nation in the world, including the nations on whose soil the intercept bases are located'.

Soon US, British and Allied intelligence agencies will embark on a massive, billion-dollar expansion of their global electronic surveillance system, which will enable them to monitor and analyse civilian and commercial communications into the 21st century. According to information recently given secretly to the US Congress, a new surveillance system, currently identified as Project P415, is being set up by NSA. Many other countries' intelligence agencies will be closely involved with the new network, including those from Britain, Australia, Germany and Japan, and even the People's Republic Of China.

New satellite stations and monitoring centres are to be built around the world, and a chain of new satellites launched, so that NSA and GCHQ Cheltenham, its British counterpart, may keep abreast of the burgeoning international telecommunications traffic. The largest existing station in this network is the US communications base at Menwith Hill, near Harrogate, Yorkshire, which has taps into Britain's main national and international networks. Although high-technology stations such as Menwith Hill are primarily intended to monitor international communications and control ultra-secret eavesdropping satellites, their capability can be and has been turned inwards on domestic traffic, according to US experts. This vast international global eavesdropping network has existed since shortly after the Second World War, when the US, Britain, Canada, Australia and New Zealand signed a secret agreement on signals intelligence, or 'SIGINT'.

COMMSURV.TXT

Although it is impossible for transcribers to listen to all but a small fraction of the billions of telephone calls and other signals which might contain interesting information, computer data signals can easily be processed in any way that NSA or GCHQ analysts require. The agencies' computers automatically analyse every telex message or data signal, and can also identify calls to, say, a target telephone number in London, no matter from which country they originate. At present, Operations Building 36M at the NSA's Menwith Hill station contains a network of eighteen powerful DEC VAX-11 processors supporting this and related tasks. Menwith Hill's nest of computers is part of a global system called Echelon, which will eventually be superseded by Project P415.

Both the new and existing surveillance systems are highly computerised, and rely on virtually total interception of international commercial and satellite communications in order to locate data of interest. Early last summer a US newspaper, the Cleveland Plain Dealer, revealed that the system had been used to target the telephone calls of a US senator. British and American domestic communications are also being targeted and intercepted by the Echelon network, the US investigators have been told, despite legal provisions that should make such intentional interception illegal. Special teams from GCHQ have been secretly flown in the last few years to a computer centre in Silicon Valley for training on the computer systems that perform both domestic and international interception.

Recently published US Department of Defense 1989 budget information has confirmed that the Menwith Hill base would be the subject of a major, \$26million expansion programme. Information given to the US Congress in February listed details of plans for a four-year expansion of facilities at Menwith Hill. Among other important stations being developed in the new P415 network, US intelligence sources say, are a GCHQ base in Cornwall, which intercepts links to and from many western commercial satellites. This spy base, at Morwenstow near Bude, has been continuously expanded throughout the 1980s.

When Britain's new interception of Communications Act was passed in 1985, however, it was obviously designed to make special provision for operations like Echelon to trawl all international communications to and from Britain. A special section of the Act, Section 3(2), allows warrants to be issued to intercept any general type of international messages to or from Britain, if this is 'in the interests of national security' or 'for the purpose of safeguarding the economic well-being of the United Kingdom'. Such warrants also allow GCHQ to tap all other communications on the same cables or satellites that may have to be picked up in order

COMMSURV.TXT

to select the messages they want. In practice, everything is intercepted.

There is no doubt that British law, along with British bases, has been designed to encourage rather than inhibit this booming industry in international data surveillance. This is quite a new development. In the 1960s, British government and Treasury officials took a lot of convincing (by the Americans) that the interception of ordinary commercial data communications was worthwhile.

Downloaded From P-80 International Information Systems 304-744-2253