BREAKING AND ENTERING

Gaining illicit access to mainframe machines using home computers and modems is known as 'hacking'. In recent years there have been a number of celebrated cases involving government departments and multinational corporations, and hacking has now become a topic of public concern.

The film *War Games* captured the imagination of many home computer owners. Using a micro and a modem, the hero illicitly dials up a succession of computers to change his college exam results, book airline tickets and download the latest games software. Things start to go wrong, however, when he unwittingly gains access to the NORAD computer responsible for North American air defence, and almost starts a global nuclear war. A fine piece of entertainment, but surely it's much too far-fetched?

Illegal Distribution

Athough the Pepsi-Cola Company of North America deny any knowledge of the incident, they were the victims of a celebrated case of hacking in recent years. Reports claim that someone in the United States illegally accessed a Pepsi-Cola company computer in Canada. The hackers sent large shipments of Pepsi to assorted destinations as a means of moving large sums of money into illicit accounts

IAN McKINNNELL

Many such computer 'break-ins' have actually happened, with the culprit often turning out to be a teenager using a home micro and modem. The 'victims' range from powerful mainframe computers belonging to universities and large corporations to the bulletin board services run by enthusiasts on microcomputers. Any computer that allows external access by telephone is vulnerable. In 1983, reality came close to imitating fiction when it was suspected that two 'hackers' had succeeded in accessing the NORAD computer system in Omaha, Nebraska.

The two teenagers involved came from Los Angeles and had managed to get into Arpanet — the secret computer network run by the Defense Department in the United States. Using a Commodore Vic-20 and a Tandy TRS-80, the pair managed to explore the contents of several of the computers connected to Arpanet, which typically belong to defence contractors, research organisations and universities. Although no classified information was obtained — the system is used mainly for sharing scientific data — the ease with which the two teenagers 'broke in' caused major embarrassment to the Defense Department.

The reason the boys found it so easy had more to do with human laziness than any computer fault. Registered Arpanet users all have passwords; unfortunately, these were not chosen very imaginatively. In this case, the two boys guessed that the University of California at Berkeley might be an Arpanet user. Sure enough, the password 'UCB' got them into the network and then they were free to access any of the computers connected to Arpanet — one of which is the NORAD underground headquarters in Omaha.

Although the NORAD headquarters is on Arpanet, the computers responsible for actual air defence are not. They sit under the Cheyenne Mountains in Colorado and are not connected to the public telephone lines.

NORAD computers might be immune to violation from hackers, but many others are not. In another incident, in July 1983, a group of Milwaukee teenagers broke into more than 60 computers belonging to colleges, corporations and the Los Alamos National Laboratory, which is engaged in weapons production. Again, according to the authorities, no classified information was obtained — just records, routine reports and messages. The FBI was called in to find out how the group, who called themselves the '414s', had pulled off such a feat. The 414s said that there were no security measures on any of the computers they phoned up.

These are just some of the cases that have been publicised. Many others are not made public, as few organisations want it known that their mainframe computer has been infiltrated by, say, a 17-year-old with a £100 home micro. Also, many organisations simply are not aware of infiltration: it is often very difficult to know if an unregistered user or impostor has been 'on-line' — though some of the more cheeky hackers leave 'can't catch me' messages and sign-off as 'System Crasher' or 'Captain Zap'.

How exactly is hacking done? All the potential hacker needs is a home computer, a modem and a bit of ingenuity. The first hurdle is finding a computer's telephone number. For public-access networks, such as Telecom Gold in Britain or The Source in the USA, this is not difficult as they are usually widely published. For private computers it's more difficult. But if you know roughly where