

bugs and countermeasures

EXTRACTS FROM EYE SPY INTELLIGENCE MAGAZINE

* images are presented in low-res screen shots for quicker loading

T O O L B O X

Tradecraft: Surveillance expert Peter Jenkins provides a fascinating and authoritative overview of the world of bugs, video and camera techniques, telephone taps and much more

PAGE 02 ROOM BUGS AND MICROPHONE ISSUE 11

PAGE 02 COVERT COMPUTER MONITORING - ISSUE 12

PAGE 03 CAN YOU TRUST THE TELEPHONE? - ISSUE 13

PAGE 03 ARE YOU BEING BUGGED? - ISSUE 14

PAGE 04 VEHICLE TRACKING - ISSUE 15

PAGE 05 VIDEO PHOTOGRAPHY - 16



TITLE: TOOL BOX 1

SUB TITLE: ROOM BUGS AND RADIO MICROPHONES
ISSUE 11

INTRODUCTION:

...Not all is as hi-tech and sophisticated as you would expect, and occasionally the most simple of devices are the most effective. Bugging is **NOT** the sole domain of the intelligence services, and is very prevalent in the commercial intelligence sector. Investigative journalists, undercover reporters and amateur sleuths all use covert recording and listening devices to gather information.

When people think of spying or espionage, they automatically conjure up images of hidden bugs, microphones, and secret cameras. This overview provides a brief insight into some of the different types of eavesdropping devices....

Radio microphones or '**BUGS**' are small devices that can be left concealed in a specific *target* area. They can pick-up conversations via a microphone and then transmit the signal to a receiving unit which is located nearby. This receiver can be monitored with headphones or be connected to a recording device. Together, these devices can prove to be an important tool for gathering intelligence.

Transmitters can be manufactured and supplied as 'stand alone' units or disguised as everyday objects such as calculators, pens, mains power sockets, or built into briefcases. Some of the images featured here show their diversity in appearance. The majority of these units require an electricity supply in order for them to operate; this power can be drawn from the mains supply and be run almost indefinitely or be powered internally by battery. Commercially, battery operated devices will only last for a few days. Therefore, they would only be used for short term operations as the *Buggist* may risk compromise every time he changes the batteries....



A typical room bug



TITLE: TOOL BOX 2

SUB TITLE: COVERT COMPUTER MONITORING
ISSUE 12

Eye Spy takes a look at the increasing use of covert devices to monitor the activities of a computer user. From easily installed software to small devices that are attached to the actual machine, no personal or office computer is 100% safe.

EXTRACT:

GHOSTS IN THE MACHINE

Another simple and very effective method of viewing the activity on a computer monitor is with a nifty software programme called '*Spector*' produced in the USA by Sectorssoft. If you can imagine a camera inside your computer taking snapshots of the screen every 5 seconds, and then stores the pictures in a hidden file for you to look at later on, then this is what '*Spector*' is capable of doing.

The software, on floppy disc or CD, takes about three minutes to install and is immediately in use with no fuss. By accessing the hidden file with a password, the screen shots can then be reviewed using the on screen buttons similar to a video recorder which has Play, Rewind, and Fast Forward which help you scan through the snapshots.

It is an amazing piece of software and anything that appears on the screen will be recorded

- All applications
- Typed letters
- All web sites visited
- Email activity
- All keystrokes typed
- Screen snapshots

If you need to know what someone is looking at on a computer, this programme is first class.



Keycatcher 'bug' records every key stroke made on a computer and is virtually undetectable



TITLE: TOOL BOX 3

SUB TITLE: CAN YOU TRUST THE TELEPHONE?
ISSUE 13

Intercepting and listening to a telephone conversation is probably the best way of technically gathering information. People speak on the telephone and trust that it will not happen to them, but telephones can be bugged or monitored for as little as £25.00 (\$50.00), and by a person without any technical experience whatsoever.

A corporate spy or private investigator can easily lay their hands on a telephone transmitter or recorder from most spy shops or even obtain them over the internet.

At a government or police level in the UK, authority must be obtained from the Home Secretary in order for any telephone monitoring to be carried out. If approved, it is unlikely that a telephone bugging device would be planted inside the telephone or attached to the line (up the pole for example). Telephone numbers can be targeted via a central exchange.

Telephone conversations can be monitored in basically three ways:

- Hard Wired Telephone Tap
- Transmitted Signals (Transmitter/Bug)
- Induction Telephone Tap

Telephone systems can be divided into two categories: **ANALOGUE** or **DIGITAL**. Analogue systems are normally what you would expect to find in domestic (home) systems and small businesses. With the analogue system, signals carried through the system cabling have not been processed. Whereas in digital systems, the signals are converted into digital code before they are sent through the system...



Government telephone-taping is usually carried out via a central or local telephone exchange



A telephone call is also vulnerable to bugging via an international satellite communications system called ECHELON

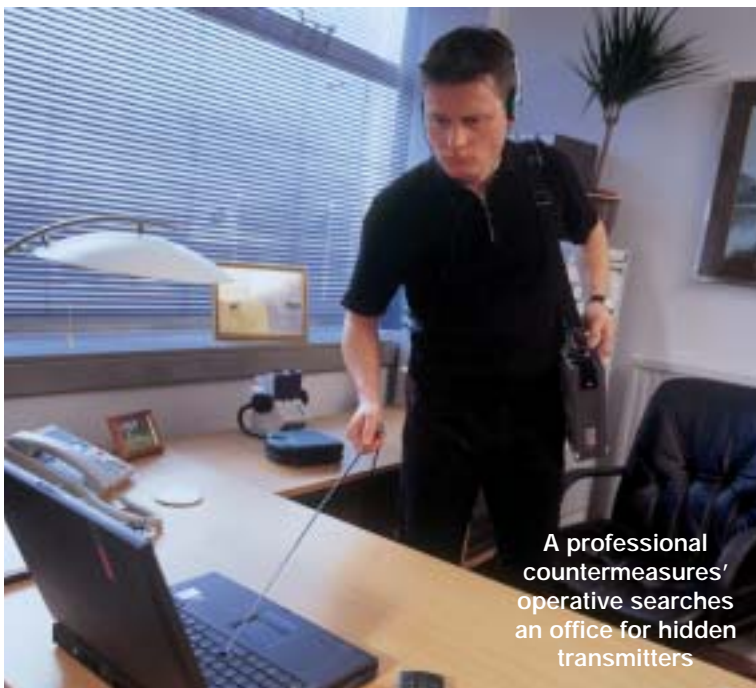
TITLE: TOOL BOX 4

SUB TITLE: ARE YOU BEING BUGGED?
ISSUE 14

What you do if you suspect that you are being bugged? And what type of equipment is available to a search team so that bugging devices can be identified and located?

ELECTRONIC SURVEILLANCE COUNTERMEASURES is a very technical complex subject which cannot be covered in a few pages. If you suspect that you are being bugged, it would be wise to call in a Technical Counter Surveillance Measures (TCSM) expert who knows what he is doing rather than attempting to locate any device yourself. It is strongly recommend using only search teams that perform this task for a living.

There are many people who advertise a 'search and sweep' service, especially private detectives.



A professional countermeasures' operative searches an office for hidden transmitters



However, the majority are just going through the motions without really knowing what they are doing. A private investigator may advertise a search and sweep service, but he may also carry out accident enquiries, tracing missing persons, process serving, and debt collection. The

phrase *'Jack of all trades but a master of none'* comes to mind. Ensure that your search team has the correct equipment and training.

Eye Spy provides an in-depth overview of what you should do if you believe you are being bugged...



TITLE: TOOL BOX 5

SUB TITLE: VEHICLE TRACKING
ISSUE 15

Eye Spy looks at specialist vehicle tracking equipment freely available to the general public.

In surveillance, there is nothing better than having actual 'eyes' on the target. A good surveillance team will be able to keep watch on a target by having him in view constantly. However, this is not always possible - especially with a very aware target. Therefore, technical means may have to be deployed in order to track the movements of the target.

Vehicle Tracking

Up until a few years ago, the only way to track a vehicle's journey was by using Direction Finding (DF) transmitters and receivers. These transmitters were concealed in or under a vehicle and emitted a 'bleep' signal every couple of seconds over a fairly wide distance.

The trackers have a special receiving unit in their vehicle, providing data and giving a "general direction" of where the transmitter is. In addition, the audio level of the 'beep' will let the tracker know how far away the target is.



A magnetic car tracker used in conjunction with GPS technology can provide accurate data on a map (inset)



A second vehicle fitted with the same equipment would also have to be deployed. This ensured a more accurate location of the target because both tracking vehicles would provide a compass bearing which can be plotted on a map, and therefore, pin point an accurate location of the target. This method has proven to be fairly accurate.

With advances in technology, tracking transmitter devices are available that require the use of only one tracking vehicle. The vehicle is equipped with an array of antennas on its roof. The antenna device will specify direction and a rough distance of the target location. However, in order for this to be an effective surveillance tool, you must be capable of understanding how to read this device's mapping coordinates.

Eye Spy provides a fascinating insight into the tradecraft of vehicle tracking...

