# Surveillance Systems in Use

## Surveillance Systems

There are basically three types of Surveillance Systems:

- Optical And Sound Surveillance Systems
- Hardwired Systems
- Radio Based Systems

## Optical or Sound Surveillance Systems

### Directional or Shotgun Microphones

These microphones pick out conversation from a target pair ignoring noise from other speakers. Distances of up to 500 metres in ideal conditions can be achieved.

### Optical Fibre Microphones

comprises a length of optical fibre terminated in the target room with a small mirrored cavity that can vibrate in sympathy with room sounds. At the other end an optical transmitter emits light pulses that are reflected back to the receiver by mirror. Movement of the mirror at the end modulates the reflected light pulses which are decoded at the listening post to provide an audio output. It is claimed that the performance is as good as conventional room-placed microphones. The fibre has a very small diameter and can not be detected with countermeasure equipment. There are however sweep techniques used by professional countermeasures specialist which makes detection of such devices possible.

### Laser Microphone

The most well known type of optical microphone is the Laser Microphone. The window or any reflective object in the target room vibrates in sympathy with room sounds. The Laser beam reflected of this object is consequently modulated, that is, its characteristics are altered in sympathy with the vibration. The return signal is demodulated to recover the vibration and hence the sounds from the target room. The Laser Microphone can give fair results under good conditions. (Good siting for best return signal, little atmospheric interference's from rain, mist, snow, low outside noise if reflecting from a window and the curtains open if reflecting from an object inside the room.). Manufacturer claims distances of 500 meters, up to 100 meters is more realistic.

AUDIOTEL INTERNATIONAL

# Surveillance Systems in Use

## Microwave Flooding Microphone

An often quoted example of such device is that claimed to have been used by the USSR against the USA Embassy in Moscow in the early fifties. Radio energy beamed in from the outside is reflected by a “passive” transmitter built into a carved American Eagle presented to the US Embassy. Sound waves from the room strike the diaphragm causing the cavity dimensions to change so modulating the radio energy reflected by the cavity and antenna in sympathy with room audio. This type of surveillance device would be readily detectable and is unlikely to give predictable results and is strictly short range.

## Infrared Optical Transmitter

The infrared Transmitter is placed in such way in the room that it can transmit an invisible infrared light beam out of the window to the receiver that is in line- of-sight. Range will be affected by the level of interference’s from the sun and artificial light sources. Manufacturers claim distances around 20 - 150 metres. These devices can be detected using the correct countermeasure equipment.

## Other Optical Devices

Other equipment as Video Cameras with zoom lenses can be used to record conversation between two people and to then make use of someone that can lip-read to translate the conversation. Documents can be photographed the same way from long distances.

AUDIOTEL INTERNATIONAL

# Surveillance Systems in Use

## Hardwired Systems

Hardwired Systems can be devised into four categories,

### *Simple Audio System*

is one in which conversation is picked up by a microphone connected to a tape recorder. The most basic type is a tape-recorder with internal microphone placed in the target area, concealed behind furniture or left behind in an attaché-case. Microphone cables of 200 metres or longer can be used if a line-driver or amplifier is used. The buggist may use his or her own cable or make use of cables already existing as spare telephone wires, old alarm or computer cables.

### Audio Modifications

A microphone or speaker already in the target room as that of a telephone, intercom or television may be modified and used without the bugging system interfering with the normal function of the equipment. The Infinity Tap is a good example.

### Speech or Machine Intercepts

An example of a Hardwired Speech intercept is a telephone tap. The telephone tap consists of a telephone interface and normally a tape-recorder. Switching is done by VOX or measuring the voltage or current from the telephone line. These systems may also be powered by the telephone line.

### Carrier Hardwired Systems

describe a bugging system in which room conversation is picked up by a microphone and relayed to the listening site by means of a higher-than-audio-frequency transmission along a cable. The most common type uses the mains power cables as both transmission medium and power source. The same principle is used in many “baby-alarm” or intercom systems.

AUDIOTEL INTERNATIONAL

# Surveillance Systems in Use

## Radio Based Systems

Radio based systems can be divided into three different areas:

### Radio Frequency Transmitters

for covert gathering, a small radio transmitter is used to relay conversation or telephone, facsimile, computer or other communications. The Transmitter characteristics such as operating frequency, power output and modulation method can be chosen to make accidental detection of the transmitter difficult or impossible without the aid of special equipment.

Modern transmitters are small and provide excellent signal and audio quality. Those for audio application can pick voice up at distances of 20 metres or more and then transmit it over kilometres. Various options of remote or time controlled switching are available.

The RF Transmitter offers several important advantages to the buggist over all other methods:

- Information is received directly in real time from the target, allowing immediate analysis and action.
- The device can be completely self-contained enabling the device to be installed and hidden quickly and easily with a consequent lessening of risk to the installer. The buggist has no need to visit the RF Transmitter on a regular basis in order to change tapes or batteries.
- The receiving site can be some distance from the target area allowing recording and processing of the information with little risk of discovery.

### Radio Frequency Intercepts

describe any bugging system that intercepts RF voice or RF machine communication as they enter or leave the target area. Typical applications are:

### Cordless Telephones

transmit on one of a few radio frequencies. To overhear conversation the buggist tunes a radio receiver into the frequency used. A tape recorder with VOX can be activated automatically for unattended operation.

AUDIOTEL INTERNATIONAL

# Surveillance Systems in Use

## General Cellular Radio or Telephone

in the past communications traffic has been intercepted using easily obtained radio receivers. Intercepting a particular subscriber was not straight forward but could be achieved by a technically competent buggist. Digital Cellular Telephones are much safer to use.

## Unintentional Signal Radiation

is when the signals from the target computer, printer, typewriter or scrambling or encrypt machine, are picked up by the buggist from a distance and then reconstructed. The signals produced by the target computer to write its screen display is rapidly changing voltages. Unless the computer and the screen are specially constructed various signals, modulated with screen display information, will radiate away from the computer. Radiation may be via mains power cables as well or directly from electrical paths within the computer. It is claimed that computer screens can be successfully reconstructed up to a kilometre.

## Switching Systems for bugging devices.

In order to have a small and "quick-plant" bugging device, much of the surveillance equipment is battery powered. To save battery power, minimise chances of detection and safe recording space on tapes, various switching methods are used in order to switch the bugging system on when needed as:

- Voice Activated Switch (VOX) or Sound Activated Switch
- Remote Control Switching by Coded Radio Frequency, Dual Tone Multi Frequency (DTMF), Infrared (IF), etc.
- Switching by Light Activation using a photocell.
- Relays, measuring voltage changes on telephone lines for example
- Various movement detectors could also be used for switching these systems.
- Timers
- Various mechanical switches as reed/magnetic switches, mercury tilt switches, etc.

The batteries of bugging equipment can also be charged making use of solar cells or by trickle charging from other power sources such as telephone lines.

AUDIOTEL INTERNATIONAL

# Surveillance Systems in Use

## The Buggist's choice of equipment

When assessing the threat, think like the Buggist. The Buggist will choose a bugging technique and associated device that:

- Yields the correct type and quality information. Information regarding site close-downs or redundancies will probably best found in boardroom meetings, whereas tapping a computer may yield detailed data about the design of a product or by intercepting fax communication the Buggist might get information on tenders or quotations.
- Has an acceptable degree of immunity to detection - a high power bugging transmitter broadcasting on a frequency that can be tuned to using a commercial FM radio is prone to accidental detection, whilst a low power transmitter operating at near microwave frequencies is not. RF Transmitters can normally be detected with Radio Frequency Detectors which are commonly available, but Mains Carrier Systems (sold as baby-alarms), cannot be detected with the same equipment and need specialised equipment.
- Exposes the buggist to minimal personal risk during installation of the device and its subsequent operation - daily access to the target area to collect tape recordings is risky, whereas listening and recording from some distance away is less so.
- Is easy to use and the degree of information processing required to yield tangible results is acceptable. - a tape recording of speech is easy to process, extraction of information from machine emissions is difficult and the results unpredictable.
- Is cost effective and the devices are easily obtained - the surveillance device cannot be too expensive or difficult to obtain. Very special devices may easily be traced back to the user if they are found.
- Is cost effective in terms of the whole surveillance operation. It is often the case that the cheapest methods yield the best quality intelligence. It is only necessary to employ expensive and exotic techniques if the target has some countermeasures in place and even then the chance of success is often very limited.

AUDIOTEL INTERNATIONAL

# Surveillance Systems in Use

## More Likely Threats

Analysis of bugging equipment and techniques used have determined that the following techniques pose the greater threat to industry and commerce.

- Radio Based Systems
- Use of radio transmitters for speech, telephone, fax, telex and computer.
- Radio Speech and Machine Intercepts for telephone and radio links.
- Hardwired Systems comprising;
- Telephone, Facsimile and Computer Taps
- Simple Audio Systems
- Mains Carrier Systems

Recognising the more likely threats enables priorities to be made with respect to the types of countermeasures implemented. Analysis of a particular site may alter the priorities

AUDIOTEL INTERNATIONAL