electronics TODAY INTERNATIONAL

HI-FI

MARCH 1973 20p

PHONE PHREAKING

BEATING THE LASER BUG

INVERTER FOR FLUORESCENT LIGHTING

BEATING THE LASER BUG

The laser bug is no myth — it exists right now. Here's how it works — and how to beat it.

LASER eavesdropping equipments, it is alleged, are being used by Security and Intelligence organisations in quite a few countries, to monitor conversations in rooms up to two miles away.

There is much controversy and some secrecy about this but there is no question that such devices do exist.

In fact, Mr Laisk, a physicist in the Macquarie University (NSW, Australia) and his third-year students have built a laser snooping device and monitored conversations in a room 30 yards away — far short of two miles but it does show the feasibility of such devices.

WHY ARE THEY USED?

The laser bug has many advantages over more traditional techniques.

Possibly the greatest advantage is that no equipment whatever needs to be installed in the premises to be bugged — nor, in fact, does access have to be gained to the premises at any time.

A second advantage — and, to many people, one that is more important than the first — is that the device to some extent obviates the need for telephone tapping.

HOW LASER BUGS WORK

The basic principle is very simple. Any sound generated within a room will cause the windows — and, to a lesser extent, the walls — to vibrate very slightly in sympathy with the generated sound. This effect can readily be demonstrated by applying one's ear to the end of a stick, the other end of which is pressing against the glass. Any sounds within the room will be heard quite clearly.

An even more dramatic demonstration is to turn up the volume of a record player in a small room — when the window glass can often be seen and felt to be moving.

The laser bug exploits this effect. Sound within the room being monitored causes minute vibrations in the window glass (and in the walls). The laser beam is directed against this window. It is therefore now impinging on a surface that is moving at a velocity which is changing in sympathy with the sound inside the room. The changing velocity of the glass surface causes a doppler shift in the laser beam frequency. The reflected beam is therefore frequency modulated by the speech within the room.

The buggers (for want of a more couth phrase) receive the reflected — and now frequency modulated — beam, and mix this beam, together with a sample of the transmitted (and hence unmodulated) laser beam, in a PIN photodiode. The output of the diode is therefore the varying difference frequency between the outgoing and incoming signals.

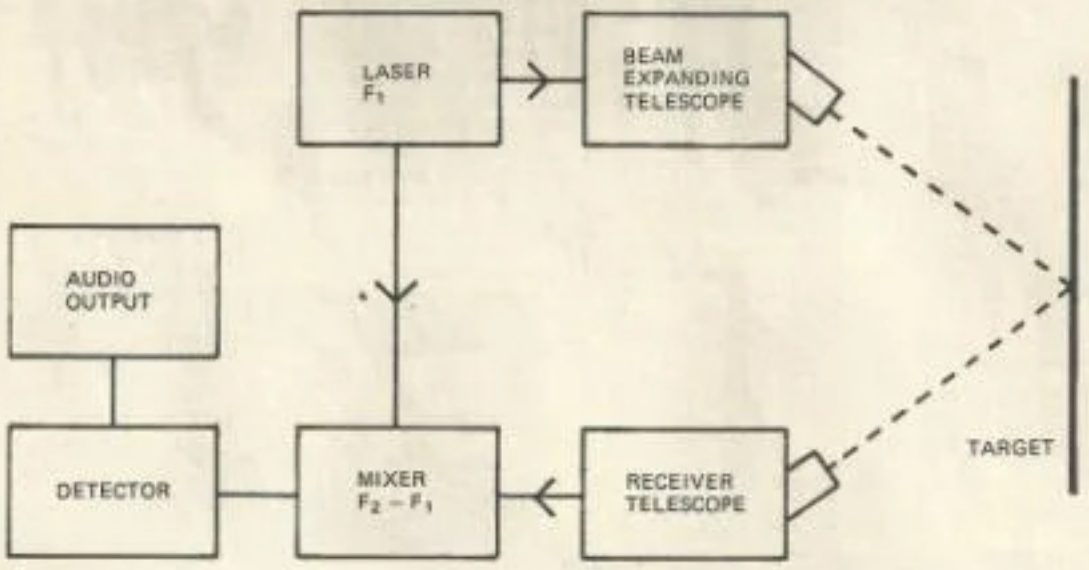
This signal is then further amplified and then detected. In Mr Laisk's equipment the final detector is a special high speed diode from Monsanto. In more elaborate systems, a double heterodyne principle may be used to provide extra gain before detection.

At first sight it would seem essential — in order to receive the reflected beam — to have the receiving and transmitting devices set up so that the beam is normal (at right angles in two planes) to the window glass.

In practice, when the incident ray strikes the glass, diffuse reflection takes place (as well as normal reflection) — i.e., some of the energy is reflected in all directions. Therefore the laser may strike the window from practically any angle, and sufficient energy will be diffusely reflected to provide a usable signal.

And this technique is feasible with relatively unsophisticated detectors such as PIN diodes at distances of 50 metres or more. Where greater range is involved, more sensitive detectors are required — probably operating at very low temperatures in order to provide an increased signal/noise ratio. As reported by Dr Sydenham in his transducer series, one commercially available IR detector system is capable of sensing the detail of a TV tower through 70km of thick fog.

Instruments are available commercially which with slight modifications can be used for snooping. These are known as Laser Velocimeters and are being bought in large numbers for use in industrial control applications. There is no doubt that modified versions of such instruments are being used for surveillance purposes.



Basic laser bug principle.

WIDE BANDWIDTH

Bandwidth of the modulated signal is very wide. For a laser operating at say 1000mm (i.e. 300 Terahertz), a glass movement of only a few microns at a few kilohertz will necessitate a bandwidth in the receiver of nearly 1GHz! Again, this is readily achievable with modern technology.

The sensitivity of these instruments is extraordinarily high.

Conventional laser interferometers can now detect movements of one angstrom (10^{-10} metres) and it is reported that detection of 1/100th angstrom movements has been achieved.

Thus there is no doubt at all that laser snooping is technically feasible and that equipment is commercially available with the required capability.

BEATING THE LASER BUG

As we have shown, the laser bug is a relatively simple device. It is practically certain to be used by many organisations – especially by those engaged in 'aggressive market research' – or industrial spying as it should really be called.

The easiest way to defeat it is merely to ensure that no confidential discussions ever take place in a room with an outside wall, but such is the sensitivity of the device that even then the conversations should be conducted at a very quiet level.

A more sophisticated approach is to install heavy double glazed windows – with the air space open to atmosphere, the outer pane should then be mechanically excited by a white noise generator (it would also be desirable to install a 'one way' mirror material on the outer pane to prevent optical coupling across the cavity). White noise should also be introduced into the air space of cavity walls.

In a less serious vein – a very effective approach would be to paint the entire outside of the premises matt black. This would totally absorb the energy of the laser beam thus preventing reflection!

Quite simple equipment can be used to detect the beam – but bear in mind that whilst most commercial interferometers use visible light, the laser snooping devices operate in the infra red part of the spectrum and hence cannot be seen. Nevertheless the heat energy can be detected quite readily.

So if you feel yourself getting hot under the collar, who knows? Maybe ASIO, SMERSH, or some other interested parties are after you.

Electronics Today International would like to thank the many academics, scientists and industrial organizations who supplied us with background material for this article.

They are not named – at their unanimous request! ●