COUNTER-EAVESDROPPING DEFENSE

by Glenn H. Whidden, CPP

A description of how a sub-carrier transmitter differs from more conventional "bugs" and how their signals can be identified

There are eavesdropping signals on the air from "bugs" that cannot be heard with ordinary radio receivers. That is not to say that it is impossible to detect them. It simply is not possible to properly demodulate them with the common types of AM or FM radios. Therefore, they pose somewhat more of a threat than the less sophisticated and more common types of eavesdropping transmitters. It is quite important that the operator conducting an examination of the r.f. spectrum in a counter-eavesdropping effort be aware of the characteristics of the signals from such devices.

The purpose of this paper is to describe how a sub-carrier transmitter differs from more conventional "bugs" and to outline how signals from them can be identified.

Characteristics of Radio Waves

A radio wave is also called a carrier when it carries information. It can carry information if it is interrupted according to a code such as the Morse code. It can also be varied in strength (amplitude) according to a code or voice sounds. This results in AM (amplitude modulated) signals. Or, it can be varied in frequency according to code or voice signals. In that case, FM (frequency modulated) signals are produced.

A radio receiver has circuits to select or tune in the carrier wave. The tuning circuits allow the operator to select one signal and to reject others. There is also a circuit in the receiver called a demodulator that removes the modulation from the carrier and converts it back to the electrical equivalent of the original modulating signal — a code or voice sound, for example. A loudspeaker or earphone can then change the electrical signal into energy that can be heard. If the type of demodulator chosen corresponds to the type of modulation on the carrier wave, the original information on the carrier will be reproduced by the loudspeaker or earphone.

Suppose now that a carrier signal is modulated by a signal that is not audible. Such a signal could simply be above the audible range of frequencies. I.e., so high in pitch that only a dog could hear it. Or, possibly higher than even a dog could hear. If a receiver picks up and demodulates a carrier with that type of modulation, nothing will be heard from the loudspeaker.

If this inaudible modulating signal is used as a carrier and is itself modulated with audible sounds it becomes useful for eavesdropping purposes. Then it is called a sub-carrier. When the eavesdropper uses a sub-carrier to modulate his main carrier and modulates the sub-carrier with room sounds, he does so with the expectation that his radio signal will not be identified as being from a bug because there will be no apparent sound modulating it. The eavesdropper of course, will use a special radio receiver that will first demodulate the main carrier and produce the sub-carrier, and then demodulate the sub-carrier to produce the room sounds.

The important point to remember is that the signal produced by an ordinary radio receiver when listened to

---

This material has been reviewed by the Central Intelligence Agency to assist the author in eliminating classified information; however, that review neither constitutes CIA authentication of factual material nor implies CIA endorsement of the author's view.

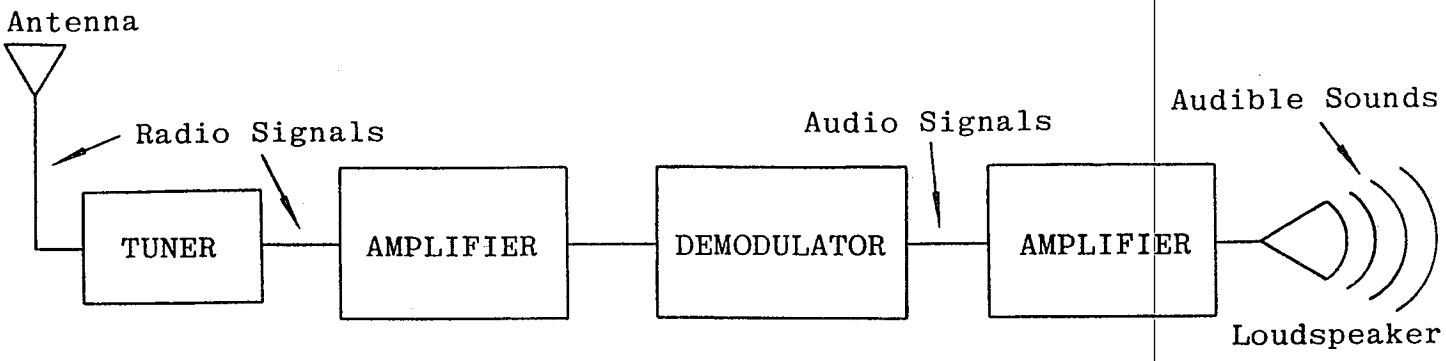

Figure 1

Block diagram of a basic radio receiver. The carrier signal desired is selected by the tuning circuit, is amplified by the amplifier and then demodulated before being converted to audible sound in the loudspeaker.

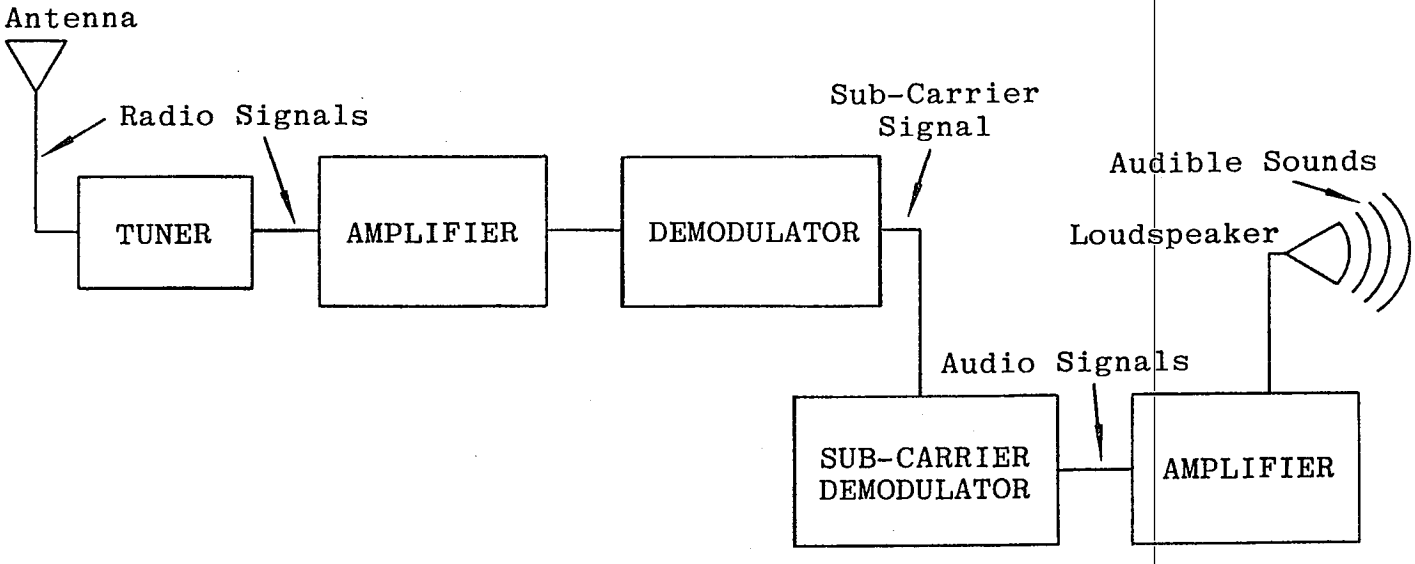

Figure 2

A receiver for use with sub-carrier signals. The signal is tuned in and amplified and demodulated as in an ordinary receiver but the demodulated signal is then demodulated a second time to produce audible signals.

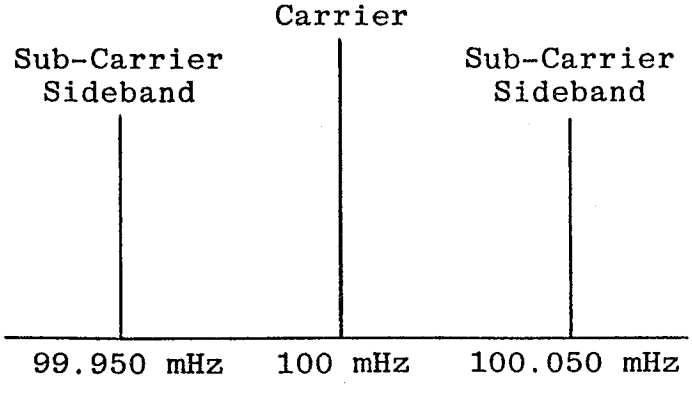

Figure 3

When a carrier at 100 mHz is modulated by a signal at 50 kHz (.050 mHz), sidebands appear on each side of the main carrier and are spaced 50 kHz on either side of it.

through headphones or a loudspeaker is silence even when voice sounds are modulating the sub-carrier. Therefore, if one is tuning through the spectrum looking for the signal from a "bug" and encounters a signal that is obviously there but apparently unmodulated, he should suspect that he has encountered a signal from a sub-carrier device.

Identification of Sub-Carrier Signals

There are at least four ways that the presence of a sub-carrier can be detected on a carrier signal. The most obvious way is to demodulate the sub-carrier so that voice frequencies or room sounds, if any, can be heard. That requires a radio receiver that tunes to the carrier wave and that has sufficient bandwidth to pass the side-bands produced by the sub-carrier. For example, suppose that the carrier wave has a frequency of 100 mHz and the sub-carrier frequency is at 50 mHz. The complete signal will consist of a sideband at 99.050 mHz, the carrier at 100 mHz, and another sideband at

" . . . eavesdropping transmitters with sub-carrier modulation pose a significant threat because they are not difficult to construct and use and their signals are not identifiable with conventional receivers."

100.050 mHz. (Other modulation products may be present in the signal but this describes the significant points sufficiently for a basic understanding of the subject). Thus, the receiver in this case must have a bandwidth of at least 100 kHz (100.050 − 99.950 = .100 mHz or 100 kHz).

To listen for room sounds on the sub-carrier, the receiver must first demodulate the 100 mHz carrier. This will produce a signal of 50 kHz at the output of the first demodulator. Then, the 50 kHz signal must be demodulated in a second demodulator. If the output of the second demodulator is amplified and fed to a loudspeaker, room sounds, if any, will be heard.

A variation on this would be a receiver with a relatively narrow bandwidth that can tune in only one sideband while ignoring the main carrier and the other sideband. If such a receiver has the right type of demodulator, the room sounds modulating the sideband produced by the subcarrier (at 100.050 mHz for example) can be heard.

It is important to note that the aforementioned examples are rather simplified versions of what practical situations are like. An examination of the r.f. spectrum for "bugs" calls for a radio receiving system that can cover much more than the region around 100 mHz. In addition, the sub-carrier signal may not be exactly at 50 kHz. In this case, it is fortunate for the equipment designer and user that the range of frequencies that might be used for sub-carriers is rather limited. The sub-carrier cannot be so low in frequency that it becomes audible at all when the main carrier is demodulated. At the same time, if the sub-carrier frequency is very high, the bandwidth of the eavesdropper's receiver will have to be high and that will tend to reduce the effective sensitivity of his system because with greater bandwidth he will collect more extraneous noise and be more likely to be interfered with. In addition, if his sidebands are spaced far out from his main carrier, they will be more vulnerable to detection and inspection.

Therefore, a lower limit of 10 kHz is likely with 20 kHz a more practical figure. An upper frequency limit of 100 kHz is also likely but this figure may be debatable because substantially higher sub-carrier frequencies are feasible particularly as the frequency of the carrier is increased. Nevertheless, as mentioned before, the higher the sub-carrier frequency, the more visible and vulnerable the sidebands that they produce become. Therefore, the upper limit of sub-carrier frequencies will depend to a considerable extent on the eavesdropper's perception of his target's technical defense capability and on his own understanding of the problem.

A third way to detect the presence of a sub-carrier on a main carrier is to examine the output of the first de-

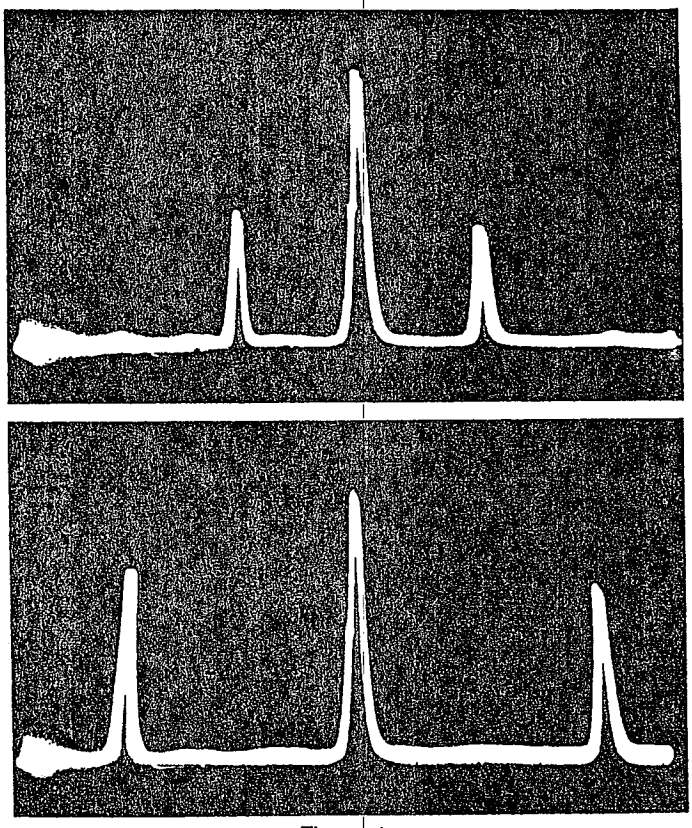

Figure 4

The appearance of a 40 mHz carrier signal when modulated with (A) a 20 kHz sub-carrier and (B) a 40 kHz sub-carrier. Photos from a visual display unit connected to a Scanlock Mark V B receiver. FM Sub-carrier.

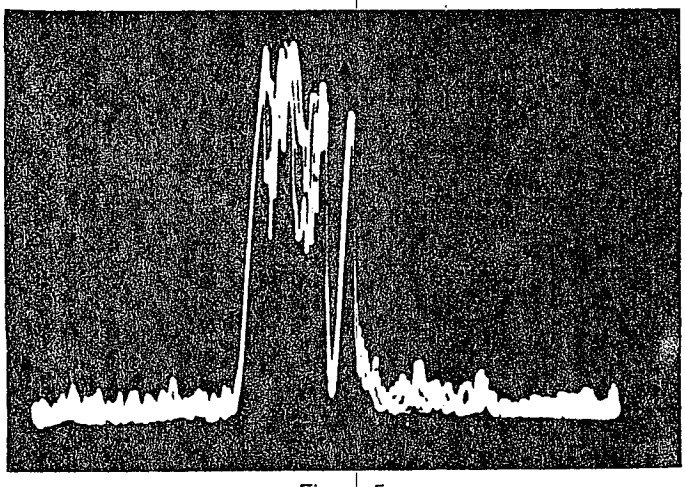

Figure 5

A photo of the audio portion of a TV signal (Ch 20) as seen on a visual display device. The frequency modulation caused by voice sounds can be seen as "squiggles" at the top of the carrier. The signal occupies about 20 kHz with the modulation shown. The "grass" along the base line is noise from the receiver (Scanlock Mark V B).

"The important point to remember is that the signal produced by an ordinary radio receiver when listened to through headphones or a loudspeaker is silence even when the voice sounds are modulating the sub-carrier."

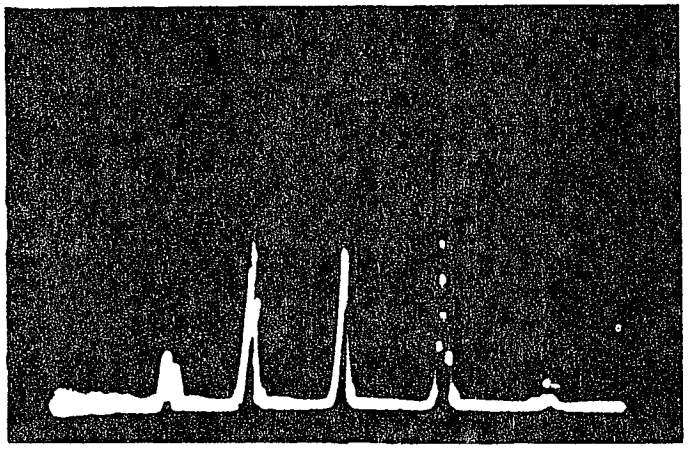

Figure 6

The signal from a sub-carrier transmitter. It can be seen that there is no modulation in evidence on the main carrier which is in the center. There is modulation present on the two sidebands. If room sounds cause the modulation effects to change, the signal can be identified as being from a "bug." In this instant the modulation was inaudible when AM and FM demodulators were used. It became audible when a sub-carrier demodulator was switched in. The sub-carrier frequency in this case is about 20 kHz with the main carrier at 40 mHz.

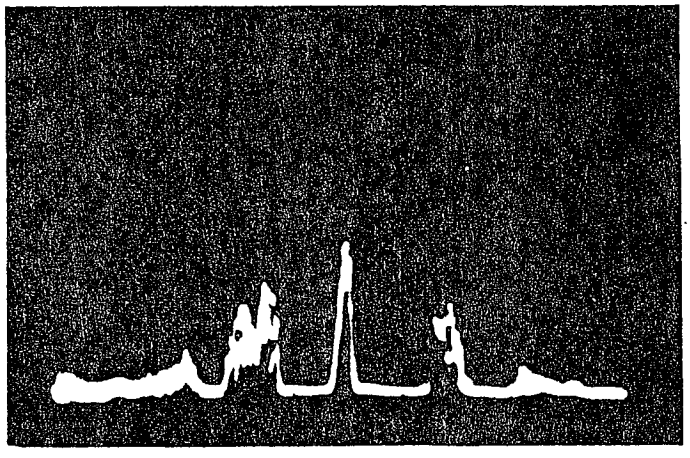

Figure 7

The signal from a heavily modulated sub-carrier transmitter. In this case, because of some circuit deficiences in the transmitter, some modulation from room sounds is beginning to appear on the main carrier in the center. The modulation on the two sidebands is quite obvious.

modulator of a wide bandwidth receiver (i.e., wide enough to accept the sub-carrier sidebands) using an oscilloscope or a frequency counter. If the oscilloscope has sufficient bandwidth in its vertical deflection amplifiers and the horizontal sweep rate is accurately calibrated, it is possible to calculate the frequency of the sub-carrier signal, if one exists, and to observe modulation on the sub-carrier. A frequency counter can be usd in place of the oscilloscope. If a sub-carrier is present at sufficient level to allow the counter to function, the frequency of the sub-carrier should be displayed on the counter.

The fourth way to identify sub-carrier signals is through the use of a visual display device. These devices use a cathode ray tube to display the characteristics of signals fed to them. They are actually radio receivers that tune themselves back and forth across parts of the spectrum. As they tune, a dot of light moves horizontally across the face of the screen. When a signal is encountered, the dot is deflected upward to an extent dependent upon the amount of energy in the signal. With a device of good resolution, the modulation on the signal will be visible.

Visual display devices are called by varius names. If they operate independently and cover a large part of the r.f. spectrum, they are called spectrum analyzers. If they are connected to a radio receiver and are used to examine the characteristics of signals acquired by the receiver, they are called spectrum monitors or panoramic adapters. The photo of Figure 5 was taken from a panoramic adapter connected to a receiver.

Usually, the visual display devices have provisions that allow different amounts of the spectrum to be inspected. It is quite important that they be used properly because improper settings may not allow the sidebands caused by sub-carriers to be seen and inspected for modulation.

In summary it is important to realize that eavesdropping transmitters with sub-carrier modulation pose a significant threat because they are not difficult to construct and use and their signals are not identifiable with conventional receivers. At the same time, equipment of several kinds is available for use by security officers and technicians that can reduce the threat from sub-carrier devices to that of more conventional transmitters. The use of those devices requires a certain amount of training and experience for effective use. ■