

GBPPR 'Zine



Issue #16 / The Monthly Journal of the American Hacker / July 2005

Special *Watergate Surveillance Issue*. Remember, if there's a place worth breaking into, it's a Democratic National Committee office.

Table of Contents

- ◆ **Page 2 / Electronic Eavesdropping Techniques and Equipment**
 - ◆ Copy of DoJ electronic surveillance manual for law enforcement organizations.
- ◆ **Page 43 / Nortel DMS-100 Office Parameters Overview**
 - ◆ Quick overview of the default office settings on a DMS-100.
- ◆ **Page 53 / Nortel DMS-100 CDN SERVORD Command**
 - ◆ How to change someones telephone number under a DMS-100.
- ◆ **Page 57 / Spread Spectrum Surveillance Bug**
 - ◆ Overview of turning a cordless phone into a surveillance bug.
- ◆ **Page 66 / "Shotgun" Directional Microphone**
 - ◆ Construction overview of a multitube directional microphone.
- ◆ **Page 85 / Rugged J-Pole Antenna Design**
 - ◆ Design info for an easy to build, rugged, and portable antenna.
- ◆ **Page 92 / Bonus**
 - ◆ CIA Career Ad: Communications and Radio Operators
- ◆ **Page 93 / The End**
 - ◆ Editorial and rants.

LAW ENFORCEMENT STANDARDS PROGRAM

**ELECTRONIC EAVESDROPPING
TECHNIQUES AND EQUIPMENT**

prepared for the
National Institute of Law Enforcement and Criminal Justice
Law Enforcement Assistance Administration
U.S. Department of Justice

by

Raymond N. Jones

ELECTRONIC EAVESDROPPING TECHNIQUES AND EQUIPMENT

CONTENTS

	<i>Page</i>
Foreword	v
1. Introduction.....	1
2. Radiating Devices and Receivers	2
2.1. General.....	2
2.2. Operating Frequencies.....	2
2.3. Power Output, Operating Time and Operating Distance	5
2.4. Crystal Control vs. Free Running Oscillators	9
2.5. Automatic Volume Control.....	9
2.6. Modulation and Audiofrequency Response	9
2.7. Frequency Deviation.....	9
2.8. Packaging	10
2.9. Ease of Detection	10
2.10. Antennas.....	11
2.11. Propagation Conditions	11
2.12. Body-Mounted Transmitters	12
2.13. Telephone Tapping Transmitters	13
2.14. Receivers.....	14
2.15. Advantages and Disadvantages of Body-Worn Transmitters and Receivers.....	16
3. Tests of Radiating Devices.....	16
3.1. Laboratory Tests of Body-Worn Transmitters	16
3.2. Field Tests of Body-Worn Transmitters	23
4. Nonradiating Devices.....	30
4.1. General.....	30
4.2. Telephone Taps.....	30
4.3. Concealed Microphones.....	32
4.4. Advantages and Disadvantages of Wired Surveillance Systems	34
5. Tape Recorders	34
5.1. Open-Reel Tape Recorders.....	34
5.2. Cassette Tape Recorders	34
5.3. Telephone Recording Actuator.....	34
6. Conclusions and Recommendations	34
Appendix Annotated Bibliography	35

Electronic Eavesdropping Techniques and Equipment

FOREWORD

Following a Congressional mandate¹ to develop new and improved techniques, systems, and equipment to strengthen law enforcement and criminal justice, the National Institute of Law Enforcement and Criminal Justice (NILECJ) has established the Law Enforcement Standards Laboratory (LESL) at the National Bureau of Standards. LESL's function is to conduct research that will assist law enforcement and criminal justice agencies in the selection and procurement of quality equipment.

In response to priorities established by NILECJ, LESL is (1) subjecting existing equipment to laboratory testing and evaluation and (2) conducting research leading to the development of several series of documents, including national voluntary equipment standards, user guidelines, state-of-the-art surveys, and other reports.

This document, LESP-RPT-0207.00, *Electronic Eavesdropping Techniques and Equipment*, is a law enforcement equipment report.

¹ Section 402(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended.

ELECTRONIC EAVESDROPPING TECHNIQUES AND EQUIPMENT

1. INTRODUCTION

Voice surveillance using electronic techniques has become an essential activity of law enforcement organizations at almost all levels of government. Often the lives and safety of law enforcement officers, and others as well, depend upon the reliability of miniaturized and concealed communications devices. Furthermore, the apprehension of criminals and the successful prosecution of criminal cases can depend upon evidence obtained by these techniques. These considerations clearly indicate the importance of this type of equipment.

The advertising, manufacture, and distribution of equipment intended for use in surreptitious information-gathering is controlled by title III of the "Omnibus Crime Control and Safe Streets Act of 1968" (Public Law 90-351) as amended. One of the objectives of this law is the prohibition of surreptitious information-gathering by all except law enforcement agencies. In addition to protecting the public against the undesirable use of such devices, the law has made it more difficult for law enforcement agencies to procure and use them legitimately. Nevertheless, this type of equipment is being manufactured, purchased, and used. One discouraging aspect of the situation is that some of the devices being manufactured and sold are of very poor quality and are immensely overpriced.

All transmitting equipment must comply with the licensing and operating requirements of Part 89 of the Federal Communications Commission (FCC) Rules and Regulations, including Section 89.117(b) which requires type acceptance. Such equipment may not be marketed prior to a grant of type acceptance by the FCC. Proscriptions concerning the marketing of radiofrequency devices are contained in Volume II, Part 2, Subpart I of the FCC Rules and Regulations. (See Title 47, Code of Federal Regulations, Part 89, Subpart A and Part 2, Subpart I.) Court-ordered eavesdropping requiring radiofrequency devices may be accomplished either by the use of type accepted transmitters operating on specific frequencies authorized to the licensee, or by use of low power transmitters which conform to the requirements of Part 15, Subpart E of the FCC Rules and Regulations.

This report has a two-fold purpose: first, to help inform law enforcement personnel concerning the application and functioning of undercover *communications equipment* and, second, to be the forerunner of a voluntary standard to be used in the selection, evaluation, and procurement of such equipment.

The information contained in this report has been derived from a number of sources, including law enforcement personnel, manufacturers, publications, and laboratory measurements. This report is concerned with the types of devices available and their application, capabilities, advantages, and disadvantages. An attempt has been made to bring together a body of information which will assist the police officer in performing his duties safely and effectively. Although the variety of circumstances under which such equipment may be used is seemingly unlimited, there are some basic technical rules, facts, and techniques which are generally applicable in most situations. Understanding and utilizing scientific techniques can go a long way toward the realization of success in an undercover surveillance situation.

While the topic of immediate interest is surveillance or offensive activity, counter-surveillance or defensive activity cannot be ignored completely because of the strong influence these activities have on each other. Being involved with either of these

Electronic Eavesdropping Techniques and Equipment

activities requires a sound knowledge of the other. While a detailed treatment of countersurveillance is not within the scope of this report, it will be mentioned where it is of importance in the understanding of surveillance equipment and its use.

The equipment and techniques discussed herein are concerned only with the interception of voice or audio communication, and, therefore, no information is included on video or optical techniques. An annotated bibliography is provided as a guide to further reading.

2. RADIATING DEVICES AND RECEIVERS

2.1. General

In this category is the miniaturized transmitter which may be worn on the body, concealed in some stationary location, or concealed in a vehicle or portable container of almost any type. Because of this versatility, the miniature transmitter is used in a wide variety of situations. These transmitters are particularly useful in circumstances where unrestricted mobility is required. In contrast to hard-wire devices (see section 4.0), the miniature transmitter is most often used when operation is required for only a relatively short period of time, such as a few minutes or hours rather than days or weeks. This time limitation is imposed primarily by the lifetime of the power supply.

The use of miniature transmitters brings into play a great many factors which can cause performance to vary widely in seemingly similar circumstances. In this context, it is useful to look at a complete communications system involving the transmitter, the propagation medium and the receiver. Figure 1 is highly oversimplified; relaying information successfully from one location to another is an involved procedure. It has been estimated by users of typical equipment that the causes of failure are approximately as follows:

	Percent
Power supply failure (batteries)	50
Operator error.....	45
Equipment failure (circuitry).....	5

Because surveillance needs often arise on short notice and adverse conditions are frequently encountered, it is imperative that persons using surveillance equipment become familiar with all aspects of its use. The importance of well-trained personnel can hardly be overemphasized.

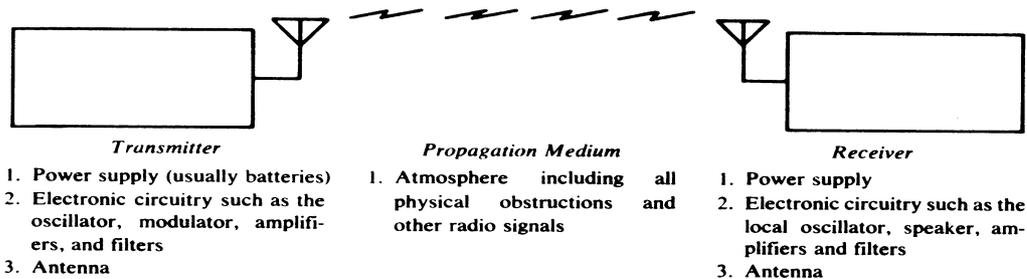


FIGURE 1. Model communication system.

2.2. Operating Frequencies

With few exceptions, miniature transmitters used in police work operate in the following four frequency ranges:

- 25-50 MHz
- 88-120 MHz
- 150-174 MHz
- 400-512 MHz

Electronic Eavesdropping Techniques and Equipment

Some experimental work has been conducted over the past few decades to determine which frequencies are best from a propagation standpoint, but the investigators have not produced conclusive evidence indicating that one frequency is better than another in a majority of circumstances. One such investigation was conducted by Rice [17], who compared propagation into buildings at 35 MHz with that at 150 MHz. In this study, 150 MHz was found to be slightly better on a statistical basis, but the difference was so small that the issue must still remain in doubt as far as any specific situation is concerned. Other work was reported by Huber [7] regarding the propagation behavior of frequencies from 0.1 to 1.0 GHz as related to communication from the inside of automobiles. This study clearly showed some frequencies to be superior to others, but factors other than frequency influenced the measurements so that definite conclusions concerning frequency selection could not be drawn.

For a number of reasons, the trend has been toward the higher frequencies. The use of higher frequencies is advantageous because shorter antennas are easier to conceal. Figure 2 shows the length of quarter-wavelength antennas in air for frequencies in the range from 25 to 600 MHz, with the specific frequency bands mentioned above shown as the solid portions of the curve. Note that at 25 MHz a quarter-wavelength antenna would be 300 centimeters (approximately 10 feet) long, while at 500 MHz it is only 15 centimeters (approximately ½ foot) long. The use of antennas shorter than a quarter-wavelength reduces radiation efficiency, thus reducing the effective communication range.

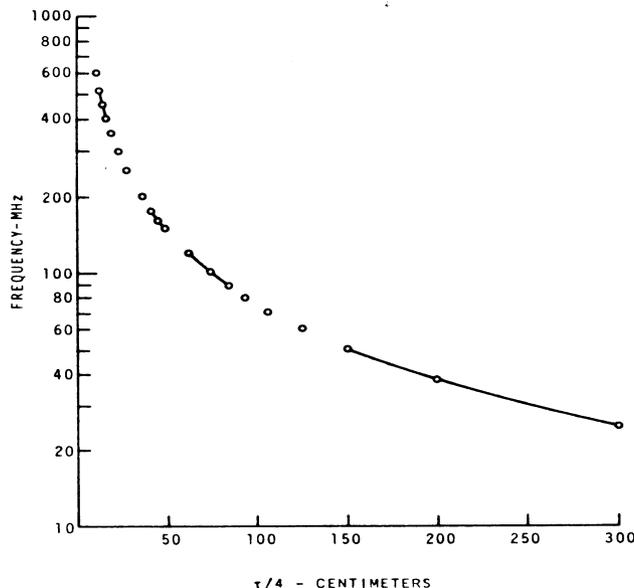


FIGURE 2. Length (in air) of quarter-wavelength antennas for the frequency range from 25 to 600 MHz.

Interference must also be taken into consideration in frequency selection. Both man-made and natural interference decrease significantly with increasing frequency, which further strengthens the tendency toward the use of higher frequencies. As more use has been made of radios for communication purposes, the lower frequency bands have become more crowded, constantly increasing the chances for interference or interception. As a precaution, an FM receiver can be used to monitor the frequency

Electronic Eavesdropping Techniques and Equipment

spectrum in the location where the undercover operation is to take place, and an unused frequency can be selected.

The use of higher frequencies improves the signal-to-noise ratio. As solid state technology improves and better devices and techniques are developed, the use of frequencies above the UHF region will almost certainly become common practice for surveillance work.

2.2.1. 25-50 MHz Band

The use of frequencies in this band for surveillance purposes is decreasing. There are several reasons for this. Principally, this band offers poor security compared to higher frequency bands. The 25 to 50 MHz band is very heavily used, and this has greatly increased the possibility of either undesired detection or interference from other signal sources. In addition, these frequencies are reflected by the night-time ionosphere, further increasing the problems of interference and security. These disadvantages, coupled with the requirement for fairly long antennas which are difficult to conceal, have caused surveillance personnel to abandon these frequencies for higher ones.

Harmonic radiation is an additional disadvantage of operation in the 25-50 MHz band. Transistor oscillators are characteristically rich in odd-number harmonics, and unless the output is filtered, their use can lead to difficulties for other users. The third harmonics of frequencies between 29.3 and 40 MHz fall within the 88 to 120 MHz band. Unfiltered transmissions can thus result in detection by receivers operating in the 88 to 108 MHz commercial FM band or interference with aircraft communication.

2.2.2. 88-120 MHz Band

This frequency range includes the commercial broadcast FM band extending from 88 to 108 MHz. Receivers of good quality are mass produced and may be purchased at prices far below those of receivers of comparable quality on other frequency bands. Also, some of these receivers can be tuned to operate above the commercial FM band, at frequencies as high as 120 MHz. For these reasons, the 88 to 120 MHz frequency range is attractive, and has been widely used for surveillance purposes.

There are, several reasons however, why such use is undesirable. With millions of receivers in this band in constant use, it is evident that this frequency range affords less security than almost any frequency band that could be chosen. Also of importance is the fact that the commonly available commercial receiver is not crystal controlled and, therefore, more subject to drift with the attendant loss of signal strength. A second reason for avoiding this frequency band is that the portion from 108 to 120 MHz is used for aircraft landing systems, and any interference, especially in the vicinity of airports, can be very dangerous. Some electronic eavesdropping equipment manufacturers produce and sell equipment which operates at these frequencies, and articles have been written which openly advocate use of the aircraft band [3]. While there may be no intention to create a hazard, it is evident that once a device is sold, the manufacturer loses all control over its use. The best policy is not to use equipment operating in this range. It is not only a potential hazard, but is also in violation of FCC and FAA regulations.

2.2.3. 150-174 MHz Band

Surveillance equipment utilizing these frequencies is usually more sophisticated in design than that designed to operate at lower frequencies. Most of the higher quality body-mounted transmitters and receivers manufactured during the past few years operate within this band. When comparing this frequency range with the lower ones already discussed, several advantages appear. First, better security exists because there are fewer receivers in existence. Next, interference is lower because of lighter

Electronic Eavesdropping Techniques and Equipment

communication traffic, lower incidence of ionosphere reflection, and lower levels of natural and man-made noise. Finally, higher radiation efficiencies can be achieved using shorter antennas.

2.2.4. 400-512 MHz Band

Even lower interference is likely in this band and detectors which might lead to discovery are relatively rare. However, some reception difficulties can be expected in areas where physical obstructions are numerous. The shorter antennas required may be an overriding consideration because, at these frequencies, a quarter-wavelength antenna can be easily concealed.

2.2.5. Summary

Following is a summary of the significant points regarding the four frequency ranges:

25 to 50 MHz	
Advantages	Disadvantages
<ul style="list-style-type: none"> a. For same power, possibly better coverage in crowded areas. 	<ul style="list-style-type: none"> a. Requires longer antennas. b. A much-used frequency band, with consequently poor security. c. Skywave propagation at night may result in undesired signal transmission or reception. d. Third harmonic radiation.
88 to 120 MHz	
<ul style="list-style-type: none"> a. Low cost receivers available. 	<ul style="list-style-type: none"> a. Violates FCC regulation. b. Minimum security; easily monitored because of availability of receivers. c. 108 to 120 MHz may interfere with aircraft navigation and communication.
150 to 174 MHz	
<ul style="list-style-type: none"> a. Quarter-wavelength antennas short enough for concealment on body. b. Good equipment available. c. Good security compared to lower frequencies. 	<ul style="list-style-type: none"> a. Equipment is expensive. b. Band heavily used in many areas of the country.
400 to 512 MHz	
<ul style="list-style-type: none"> a. Rarely monitored; best from security standpoint. b. Requires very short antennas. c. Low level of interference. 	<ul style="list-style-type: none"> a. Equipment is expensive. b. Few sources of equipment.

2.3. Power Output, Operating Time and Operating Distance

The maximum practical distance between transmitter and receiver for satisfactory communication can be very important in surveillance applications. This distance is dependent upon a number of things, including transmitter power output, gains of transmitting and receiving antennas, and receiver sensitivity. Still other factors are the local conditions, such as the terrain, the conductivity and dielectric constant of the earth, the building density, and the heights of the antennas. The fact that any or all of these factors may vary with time and location makes accurate prediction of operating distance nearly impossible. General statements are often made about

Electronic Eavesdropping Techniques and Equipment

the operating distance or coverage area of a transmitter, but it is unwise to rely heavily upon information of this type. Such statements are likely to be based on a few specific experiences in a given locality, and performance may be found to differ widely in different situations. Claims about operating distance are not dependable criteria for determining the effectiveness of a transmitter under a given set of conditions and should not be used to determine the superiority of one transmitter over another.

There are two approaches to objective measurement of transmitter output. One is to make comparative field strength measurements under carefully standardized conditions, and the other is to measure the transmitter power into a 50-ohm termination. Either approach may present difficulties. The field strength approach requires a measurement site free of obstruction and a receiver or field strength meter. The intensity of the field radiated by each transmitter must be measured and plotted over a period of time. This method presents several problems, including the determination of the proper type antenna to use to achieve accurate data, the necessity for receiver calibration in the case where the transmitters to be compared operate on different frequencies, and the possibility of other radio signals on the same frequency leading to erroneous field strength measurements. Clearly, this is not an ideal approach unless field test facilities and highly skilled personnel are available.

Using the power output measurement approach is much simpler, but not without possible complications. The procedure is to connect a good quality power meter to the antenna output terminal of the transmitter and record the power over a specified time interval. However, power meters do not yield accurate results unless the output impedance of the transmitter matches the input impedance of the power meter. The input impedance of most power meters is 50 ohms. Providing the output impedance of the transmitter is also 50 ohms, an adapter from the transmitter output connector to the power meter input connector is usually all that is needed to make the measurement. If the output impedance of the transmitter is not 50 ohms, some sort of a matching or tuning network is necessary. The tuning network is inserted between the transmitter and power meter and is varied until the power meter reading is maximized, after which the measurement can proceed.

It is common to encounter miniature surveillance transmitters which are neither 50 ohms at the antenna output connector nor equipped with a coaxial connector. Some do not have a ground connection but instead have only a screw terminal for the attachment of an antenna wire. With such a combination of output connectors and terminal conditions, the task of making meaningful measurements becomes extremely difficult.

There is a need for standardization if there is to be meaningful and objective comparison of equipment performance. Ideally, there should be a convenient and straightforward means of measuring transmitter power output without ambiguity, and specifications should spell out not only maximum transmitter power output but also some indication of how this power decreases with transmission time.

One final, important point regarding the measurement of transmitter power output using a power meter is the manner in which the power is distributed over the frequency spectrum. Because most power meters utilize a broadband resistive element, such as a bolometer, as the sensing device, the power measurement alone will not provide sufficient information. If a particular transmitter has an output spectrum rich in harmonics, it will not be distinguishable from a second transmitter which shows the same power output but has had the harmonic frequencies drastically suppressed. It is possible to have a situation where as much as one-half of the power radiated is at the harmonic and other spurious frequencies. Such spurious radiation is detrimental in that it substantially increases the risk of detection.

Figure 3 [9] is a plot of operating range versus signal loss in decibels (dB), with the point 1.0 on the x-axis of the graph representing a maximum range, whatever

Electronic Eavesdropping Techniques and Equipment

this may be in actual distance. It can be seen that a decrease of 6 dB in the received signal strength corresponds to an effective reduction of this range by one-half. A loss of 20 dB reduces the range by a factor of 10. This illustrates how drastically the operating range can vary from one situation to another, especially when it is realized that many things, such as building density, antenna types and orientations, and antenna position with respect to the body of the wearer, can all contribute losses of several dB. Thus, claims about operating range do not offer a reliable basis on which to compare equipment. The best procedure is to make comparative measurements under identical conditions. Only then can superior performance be recognized.

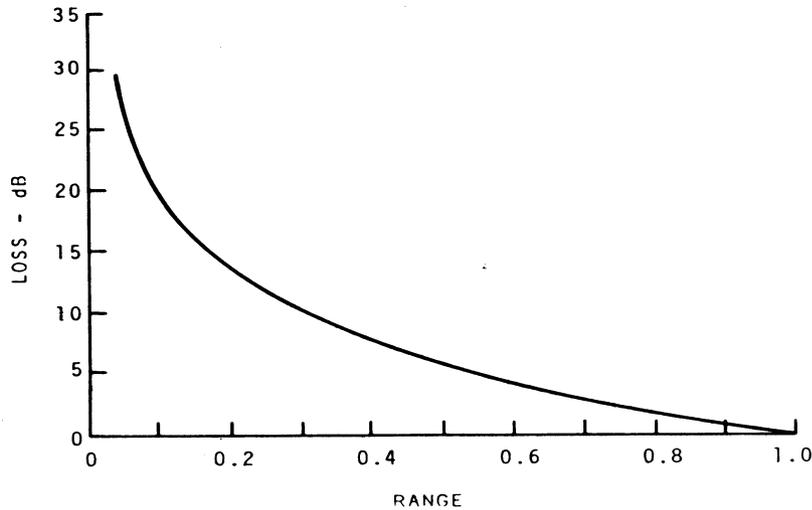


FIGURE 3. Normalized range as a function of signal loss in decibels.

2.3.1. Batteries

Most body-worn transmitters and receivers can be equipped with a number of different types of batteries. Even though there are wide differences in their chemical composition, these batteries are near enough to the same physical shape and size that they may be interchanged or adapted to fit. This permits the user to select the best type for a particular application. Manufacturers of the equipment usually recommend the most advisable type to use. The importance of battery quality is paramount, and the user should insure that the use of poor batteries is avoided. Detailed information on batteries is available [8]. Even recently purchased batteries may have already suffered sufficient shelf-life deterioration to cause significant degradation in the performance of a transmitter or receiver.

With undercover surveillance equipment, such as body-worn transmitters and receivers, the two most frequently used types of batteries are the alkaline and the mercury primary batteries. Nickel-cadmium batteries, which are rechargeable, have not as yet found wide acceptance in undercover work. The carbon-zinc or common flashlight battery is generally not suitable because of its low capability for meeting high-current drain requirements. Alkaline and mercury batteries are desirable mainly because they are able to supply relatively large amounts of energy for their size. Alkaline batteries are less expensive and more readily available than mercury batteries. However, body transmitters using mercury batteries usually have a less rapid decay in power output (see figs. 11 and 17).

Electronic Eavesdropping Techniques and Equipment

A good measure of the condition of a battery is its ability to sustain a moderate current drain. One test that may be used on a 9-volt alkaline battery is to determine whether it will supply 75-80 milliamperes of current for a period of 45 seconds. This can easily be done using the circuit shown in figure 4. If the battery is at an acceptable state of charge, the voltmeter indication should not drop below 9 volts for a period of 45 seconds.

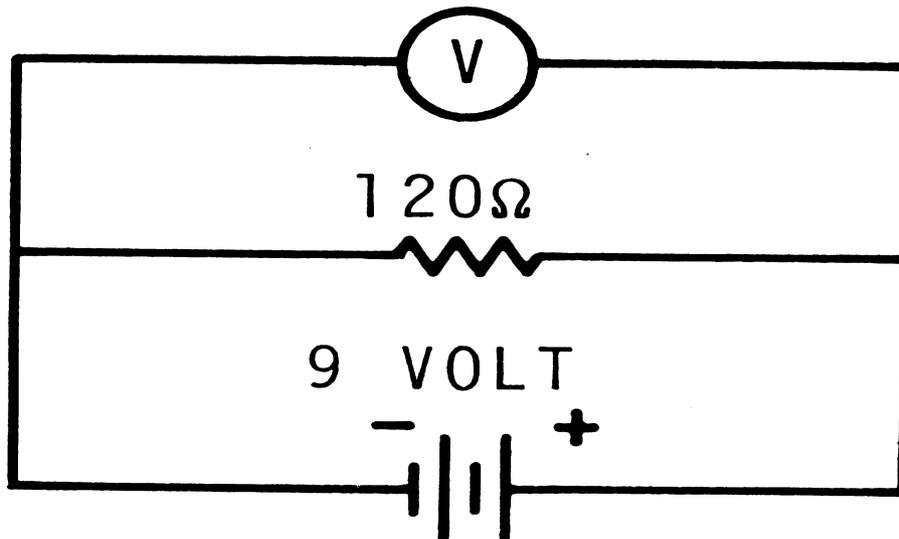


FIGURE 4. Battery test circuit.

It is not appropriate to test mercury batteries in the same manner because mercury batteries sustain a nearly constant voltage under load until they are almost completely discharged. Therefore, even though a mercury battery has undergone considerable use and is near the end of its lifetime, the current drain test might not indicate it. At present there appears to be no simple and reliable method for determining the state-of-charge of a mercury battery. Mercury batteries, fortunately, have a shelf-life of approximately 2½ years. The best way to be confident of the freshness of a mercury battery is to make sure that its open terminal voltage is what it should be and to use batteries with fairly recent dates of manufacture. To avoid the possibility of battery failure during an operation requires vigilance. Points to remember about batteries include the following:

- a. Know the milliampere hours the battery can supply and the transmitter current drain.
- b. Make sure the batteries are fresh. If possible, use a fresh battery for each mission.
- c. Keep a log of battery life expended.
- d. For improved shelf-life, batteries should be stored at temperatures well below normal room temperature.

Neither the alkaline nor the mercury batteries are rechargeable and, once discharged, must be discarded. Care must be taken with mercury batteries to assure that they are not burned because toxic vapors are emitted which can endanger life. One further point regarding batteries is that their contents are corrosive and they should not be stored in an instrument for longer periods of time than necessary. Corrosion can cause serious damage to an expensive item of equipment.

Electronic Eavesdropping Techniques and Equipment

Another important consideration is the effect of ambient temperature on battery operation and life. Some types of batteries suffer severe reductions in performance when subjected to either extreme heat or extreme cold. One example is the carbon-zinc (flashlight) battery, which suffers in its ability to perform when temperatures are below 0°C (32°F) or above 50°C (122°F). Also, the mercury battery is a poor performer at temperatures below 5°C (41°F), but is an excellent performer at high temperatures. See reference [8].

2.4. Crystal Control vs. Free-Running Oscillators

Undercover transmitters and receivers should be crystal-controlled because free running oscillators drift in frequency and can be changed by modulation, making it difficult to sustain optimum performance over long periods of time without retuning. Crystal-controlled equipment should operate with a frequency tolerance of a few parts per million. This tolerance varies with frequency; however, tolerances of 10 parts per million are typical in the 150 MHz range.

In some instances, the requirement for miniaturization may be so critical that the extra size incurred by the addition of crystal-control circuitry cannot be tolerated. In these situations, extremely small and very low-powered transmitters of a size comparable to a 1-inch section of a common lead pencil can be used. In equipment this small, hearing aid batteries are used, and transmitter output power is typically in the vicinity of 10 mW. Frequency drift in devices not having crystal control will typically be of the order of 10 kHz per hour under normal operating conditions.

2.5. Automatic Volume Control

It is evident that voice modulations reaching the transmitter will be at different intensities, depending on the proximity of each speaker to the microphone. The wearer of the transmitter will of course be much closer than the other speakers. Consequently, it is probable that the wearer's voice will be too loud while others may barely be heard. This brings about the critical need for automatic volume control circuitry in the transmitter so that all those talking may be heard distinctly.

2.6. Modulation and Audiofrequency Response

Because of circuit simplicity, good fidelity and the relatively low power drain, frequency modulation is used almost exclusively in undercover transmitters, although there appears to be no reason why other types of modulation could not be used in order to provide better security.

Most of the frequency components of the human voice are in the range from 300 Hz to 3000 Hz. This is the audiofrequency response for which the equipment should be designed. Broader responses are not only unnecessary but may even be detrimental, because sounds could be transmitted which may interfere with the intelligibility of the conversation being monitored.

2.7. Frequency Deviation

Federal Communications Commission (FCC) regulations pertaining to public safety communications equipment authorize a maximum frequency deviation of ± 5 kHz for FM systems. It is important that surveillance transmitters be designed to satisfy this requirement, not solely because of the FCC regulations, but because the transmitters must be compatible with the receiving equipment commonly used in law enforcement communications. Clarity of reproduction is another reason for using equipment with the proper frequency deviation and modulation bandwidth. Using bandwidths narrower than those specified may create difficulty in identifying the speakers, while the use of broader bandwidths does not improve voice reproduction and may introduce unwanted sounds. It is particularly important that surveillance recordings be clear and intelligible because of their possible use as court evidence. In general, ± 5 kHz frequency deviation and 3 kHz audiofrequency response provide adequate voice

Electronic Eavesdropping Techniques and Equipment

reproduction. In surveillance work, problems can arise related to the loudness of the modulating voices and the action of the automatic volume control (AVC) circuits, which may, in some cases, produce recordings unsuitable as court evidence.

2.8. Packaging

Miniature transmitters have been packaged or concealed in almost every way imaginable, as dictated by specialized needs. Lamps, plugs, chair legs and flower pots have all been used to conceal a transmitter. Some have achieved fame and attracted international attention, such as the one concealed in the shoe of a diplomat and the one in the seal above an embassy desk. These are all custom-made devices, which for the most part would be unavailable to a police department unless it had direct contact with a facility which could produce them. Some of these devices are available, but information regarding specific suppliers is not easily obtained.

Good quality transmitters and receivers can be packaged in small ruggedized containers with dimensions on the order of 7.5 cm × 5 cm × 2 cm (3'' × 2'' × ¾''), and can be either body worn or concealed in some unlikely location. The particular situation dictates the necessary concealment precautions and in this the agent must use his own judgment. If he cannot wear heavy clothing or outer garments, concealment may be a severe problem.

Electronic packaging has to be considered, especially in the sense that the devices used should be repairable and the circuitry should be accessible for trouble-shooting purposes. Devices which are potted in an epoxy envelope, although weatherproof, are not repairable in the event of circuit failure. It is characteristically the very low-priced and lower quality devices that are manufactured in this way. Epoxy-potted transmitters usually operate in the 100 to 120 MHz range

2.9. Ease of Detection

Detection may occur by visual observation, physical search (frisking), or by the use of electronic defensive (countermeasures) equipment. Little can be said of the likelihood of detection by visual or physical means except that the smaller the device is the less apt it is to be discovered. Obviously, discovery is dependent upon how cleverly it is concealed.

Detection by electronic methods deserves more thorough attention. Consider the following three factors for the bearing they have on detection:

Operating Frequency.—As has already been mentioned, transmitters operating in the 88- to 108-MHz band are more apt to be detected due to the fact that receivers covering this band are extremely common. It does not require a very vivid imagination to picture an undercover agent in a situation where someone is tuning through this frequency band and picks up the broadcast of voices and sounds from within the room, or hears the oscillatory squeal of energy fed back to the receiver by a concealed transmitter. These frequencies should be avoided.

Power Output.—High power output increases operating range. But the greater the power radiated, the wider the area of coverage, with the consequence that detection is more probable. Therefore, it is advisable to avoid using a 1-watt transmitter, for example, where a one-quarter-watt unit would do. Where there is a reasonable choice, it is much wiser to improve receiver sensitivity or antenna efficiency than to increase transmitter power.

Harmonics.—Good equipment radiates energy primarily at the fundamental frequency, and filters out and suppresses the harmonics. This makes it less likely that the energy being radiated will affect other equipment, such as television receivers, which may draw suspicion and lead to discovery. It is not unreasonable to expect the level of radiated harmonic and other spurious energy to be at least 35 dB below that of the fundamental output of the transmitter. Devices may be discovered by detection of the energy radiated at their harmonic frequencies because antenna efficiency may be better at the harmonic frequencies than it

Electronic Eavesdropping Techniques and Equipment

is at the fundamental frequency. Searching by electronic methods is often done by starting at the high-frequency region and working downward.

2.10 Antennas

Overall system performance can be greatly affected by the type of antenna used, the type of installation, and the conditions of operation. Monopole antennas are used exclusively with body-worn transmitters, because they are omnidirectional and of very simple construction. For many reasons, other antenna configurations are impractical.

One important fact to consider is that best communication usually occurs between two monopole antennas when they are oriented parallel to one another; i.e., polarization should be the same in both antennas. Either they both should be vertical or both horizontal. Although this is generally true, local distortions in field configuration caused by conducting objects such as steel in a building can cause significant variations.

Normally, the optimum length for an omnidirectional monopole antenna is approximately one-quarter wavelength at the operating frequency. However, this is modified somewhat in the case of antennas placed next to the body. Because of the added capacitance between the antenna and the body of the wearer, resonance occurs when the length of the antenna is 4 or 5 percent shorter than one-quarter wavelength.

The requirements that the antenna be both small and located next to the body constitute very severe handicaps to efficient communication. Antennas that are short compared to a quarter wavelength are not efficient. In addition, the human body is a good absorber of radio energy. These constraints combine to place very severe limitations on the distances over which satisfactory communication can be achieved. Given ideal antenna conditions, it is entirely possible to maintain good communication with transmitters of 1-watt or less at distances of several miles. However, when antennas are shortened and placed next to the body, the range may drop to a few hundred feet or less, depending upon local propagation conditions.

The subject of body-worn antennas is a complex one. One study of this topic has been prepared for the Law Enforcement Assistance Administration by the Aerospace Corporation of El Segundo, California [9].

2.11. Propagation Conditions

The propagation medium is an important component of the communications system. This is the part of the system over which the operator has almost no control. An accurate prediction of how well a system will work in a given situation is not possible to any high degree of accuracy without actually making field strength measurements. This is usually impractical, so the next best thing is to examine some of the variables and do those things which will enhance the probability of success.

Two factors which affect the performance of an antenna are the conductivity and the dielectric constant of the ground. These vary widely around the country, and can make a difference in field strength of as much as several dB. The moisture content of the soil is also a factor, as higher amounts of moisture enhance propagation. While these factors are not controllable, they are mentioned for general interest.

Some factors are controllable by the operators. One way to improve the received signal from a vertical monopole is to elevate the receiving antenna. Improvements of several decibels in received signal strength can be realized by choosing listening post locations so that the angle between transmitter and receiver is 30 to 45 degrees from the horizontal.

A transmitter or receiver does not perform well when placed inside an automobile. The metal enclosure acts as a shield which attenuates high-frequency electromagnetic energy. If there were no windows in the car, or an outside antenna, there would be essentially no transmission or reception at all. The metal used as building reinforcement also reduces the strength of a transmitted signal. Even the average home may

Electronic Eavesdropping Techniques and Equipment

seriously hamper inside-to-outside communication because of the use of foil-backed insulation in the walls. A transmitter enclosed in a metal container is completely ineffective. This fact was once used in an extortion case involving a money drop. The criminal, suspecting that a transmitter was concealed in the package, placed it in a metal suitcase and thereby escaped because the transmitter was useless. The wearer of a transmitter may position himself near openings such as nonmetallic doors or windows, thereby avoiding the shielding effects of unseen metal barriers. The use of such tactics comes with experience and a general understanding of the behavior of radio energy.

2.12. Body-Mounted Transmitters

There are a number of other features which may be important in the field use of body-mounted transmitters and these are discussed below.

2.12.1 Polarity Protection

When installing batteries in a body-mounted transmitter, it is very important that the batteries be oriented for correct polarity. Most units employ alkaline batteries equipped with snap-on connectors. These batteries cannot be installed with the incorrect polarity because the connectors at the positive and negative terminals are different from each other and the battery will not fit the receptacle unless it is correctly oriented.

Occasionally a body-worn transmitter may be encountered which utilizes mercury batteries. A group of four or five individual cells are usually held in place by a cardboard or plastic sleeve, and two such groups are required to power the transmitter. Because the mercury cells are usually not equipped with snap-on connectors like the alkaline batteries, it is possible to install them with reversed polarity.

There are at least two possible consequences of imposing the incorrect voltage polarity. First, the transmitter will not operate and the operator may not know why. Next, the transmitter may be permanently damaged. This can happen with either mercury or alkaline batteries because even a very brief, momentary exposure to reversed polarity can result in irreversible damage. Whether or not such damage will result depends upon the circuit, and better quality units have built-in polarity protection.

2.12.2. Antenna Connector

A common trouble spot in body-worn transmitters is the connector between the antenna lead and the transmitter. A wide variety of connectors are used by various manufacturers and most have both advantages and disadvantages. There are the simple plug-in microphone jack types, the screw-on types, and the twist-lock types. Two considerations are important. First is the possibility that the lead will be pulled out of the socket during use, will work loose, or will otherwise break the connection. Second is the ease of making repairs if the antenna lead is broken. Some units combine the microphone wire and the antenna wire into one lead.

2.12.3. Microphone

Although microphones will be discussed in detail in a later section, it is worthy to note here that two different mounting schemes are used. Some miniature transmitters have the microphone built into the case of the transmitter, while others use a microphone connected by a cable. If the microphone is mounted in the case, there should be a dirt seal to protect it against clogging and subsequent damage or loss of sensitivity. A piece of foam-like material is a satisfactory protector for this purpose.

Most of the better transmitters use the electrodynamic type of microphone, which has excellent sensitivity and adequate frequency response for voice communication. Electret microphones (paragraph 4.3.4) of adequate quality are a relatively recent development.

Electronic Eavesdropping Techniques and Equipment

They provide better frequency response and may be expected to find increased use in undercover equipment. Both types are rugged, but electret microphones have a limited lifetime of about three years of operation at maximum sensitivity. Should this be overcome and costs made competitive with the electrodynamic types, electret microphones could come into common use.

2.12.4. Location of On-Off Switch

Because miniature transmitters are often located where they are subject to being jolted, or where other materials may rub against them, it is important that the on-off switch be of a positive type requiring a fairly strong force to operate and that it be in a location where it is not apt to be moved accidentally. In some situations it may be desirable to make it either difficult or impossible for the wearer to turn the switch off while the surveillance operation is under way. Some manufacturers make special provisions for this but may not indicate it in their specifications.

2.12.5. Ruggedness

Body-worn equipment should be constructed to withstand severe physical shocks. Construction should be such that dropping from chest height to a concrete floor will not permanently affect operation. This requires either an all-metal case of heavy gauge or very high performance plastic. If plastic materials are used, they should not soften when warm or shatter in severe cold.

2.12.6. Size

The primary factor limiting the smallness of a transmitter is the size of the batteries required to supply the power. In general, a crystal-controlled transmitter with batteries, having an output in the 0.2 to 1 watt range, can be contained in a volume slightly smaller than a cigarette package. In such a transmitter, the batteries occupy approximately 75 percent of the total volume, and the crystal control feature adds additional bulk. Transmitters no larger than the eraser portion of a common lead pencil are available, but these devices are not crystal controlled, have a power output of only a milliwatt or so, and their greater frequency instability restricts their application and dependability. Such low-power transmitters are not suitable for applications where they must be placed next to a large power absorber such as the human body. They may be used as room bugs where long distances to a listening post are not involved.

2.13. Telephone Tapping Transmitters [15]

There are several types of telephone tapping transmitters usable for monitoring both sides of a telephone conversation. In general, they are not crystal controlled and have a power output ranging from a few milliwatts to perhaps one-quarter watt; many of them utilize the telephone line as an antenna. All types may be located either by their radiated signal or by visual inspection. The poorer ones may be found by the current they draw from the telephone lines. If the current drain is sufficient, it can give an indication of trouble on the line and draw the attention of the telephone company repair facilities. Some difficult problems are encountered in evaluating the output power of telephone tapping transmitters. Because of the antenna arrangements they utilize, it is not feasible to make output power measurements into a 50 ohm load, and it becomes necessary to rely on field strength measurements to determine the radiated power.

2.13.1. The Drop-In Telephone Transmitter

This device looks very much like the mouthpiece unit of a telephone. The carbon microphone mouthpiece drops out easily if the retaining ring over the mouthpiece is unscrewed. The drop-in transmitter may be substituted in its place very quickly and the telephone returned to apparently normal operation. The telephone transmitter

Electronic Eavesdropping Techniques and Equipment

draws its power from the telephone line and operates only when the receiver is lifted from the cradle. Both sides of the telephone conversation modulate the rf carrier frequency of the telephone transmitter which may be received and recorded at a remote location. One of the main advantages of the device is that it takes only a few seconds to install, and the better ones are so cleverly constructed that they may be difficult to recognize by anyone who is not extremely familiar with the telephone equipment. The drop-in transmitter does not require a separate antenna but instead utilizes the telephone line for this purpose. However, it is possible to detect the use of this type of transmitter by means of impedance measurements or by measuring the current drain while the telephone is in use.

2.13.2. The Series-Connected Telephone Transmitter

Any accessible location on the telephone line to be tapped, such as a terminal block, may be used as an installation point for a series-connected transmitter. Therefore, direct access to the telephone instrument is not required. The circuit in figure 5 illustrates the method of connection. The polarity is not important, so the transmitter may be installed in either side of the line. Because series-connected transmitters draw current from the telephone line, they can be detected in the same manner as drop-in transmitters.

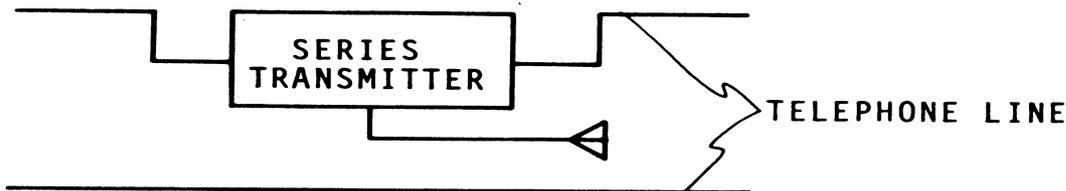


FIGURE 5. Series-connected telephone transmitter.

2.13.3. The Parallel-Connected Telephone Transmitter

Figure 6 illustrates the method used to connect a parallel transmitter to a telephone line. Again, the polarity is usually not important, but there are several differences between this installation and the series transmitter. Because the parallel transmitter is powered by a separate battery, it draws no current from the phone line and is essentially undetectable by impedance or current measurement techniques. As with any battery-powered device, it has a limited operating time. The transmitter is activated when the receiver is lifted.

2.14. Receivers

Receivers used in undercover work are not always packaged in miniaturized form because in many instances concealment is not required. The sensitivity of a receiver has almost nothing to do with its physical size. Receiver components and measurable characteristics which distinguish good quality equipment from poor quality equipment are discussed below.

2.14.1 Sensitivity

Sensitivity is probably the most important characteristic of receiver quality. It is a measure of how weak a signal can be detected, and therefore is of first-order importance in determining the operating range of an undercover receiver. There are two common methods of specifying this information. The first is in terms of microvolts for 20 dB quieting [13]. The second is in terms of microvolts for 12 dB SINAD [8]. Either is an acceptable method, although the 12 dB SINAD provides a better

Electronic Eavesdropping Techniques and Equipment

measure of true receiver performance because it is made under modulated conditions. As a general rule of thumb, one may add 0.1 microvolt to the 12 dB SINAD sensitivity figure to obtain a comparable sensitivity for a receiver rated on the basis of 20 dB quieting. Although this is not exact, it does provide a quick means of comparing two receivers which are specified in these different ways. For example, a good receiver should be capable of at least 0.4 microvolt sensitivity at 12 dB SINAD or 0.5 microvolt for 20 dB quieting.

2.14.2. Frequency Control

The receiver should be equipped with a crystal-controlled local oscillator for automatic frequency control. Otherwise, it will tend to drift or detune, causing fading of the received signal. This is especially important if the receiver is to be unattended for extended periods of time.

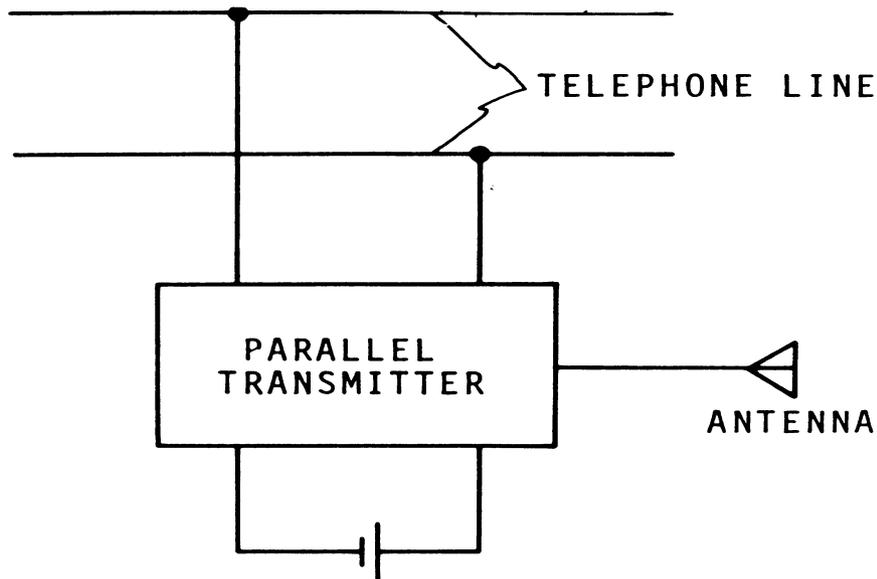


FIGURE 6. Parallel-connected telephone transmitter.

2.14.3. Adjacent Channel Rejection

Adjacent channel rejection, also termed selectivity, is achieved through the use of good filter networks which reject signals at nearby frequencies, preventing unwanted interference.

2.14.4. Antenna

Much the same considerations apply to receiving antennas as to transmitting antennas, particularly if they are worn on the body (section 2.10) Where the receiver is not body-worn, one would normally use antennas which have higher gains and/or directivities.

Electronic Eavesdropping Techniques and Equipment

2.15. Advantages and Disadvantages of Body-Worn Transmitters and Receivers

Advantages	Disadvantages
<ol style="list-style-type: none"> 1. Completely portable (small and lightweight). 2. Quickly installed. 3. Highly versatile. 	<ol style="list-style-type: none"> 1. Limited period of operation. 2. Limited and uncertain range of operation. 3. Can be located by electromagnetic sensors. 4. Will not relay information when surrounded by a conducting shield such as a car body, airplane, or metal suitcase. 5. Quality (intelligibility) of transmitted information may vary. 6. Subject to locally generated interference and atmospheric noise. 7. Personal contact with subject often necessary.

3. TESTS OF RADIATING DEVICES

3.1. Laboratory Tests of Body-Worn Transmitters

A limited number of measurements were performed to evaluate some of the equipment which is now commercially available to law enforcement agencies for electronic surveillance work. Five transmitters were tested to determine some of their operating characteristics. All units were of the FM crystal-controlled type, operating on either mercury or alkaline batteries and capable of output powers of 1 watt or less.

The units were tested for frequency stability, output power as a function of time, spurious emissions, AM hum and noise, and dc current drain and efficiency.

TABLE 1. *Laboratory Test Results*

Parameter	Transmitter				
	#1	#2	#3	#4	#5
Frequency stability parts per million.	3 ppm over period of 4 hr. 45 min.	5 ppm over period of 2 hr. 45 min.	5 ppm over period of 3 hr. 45 min.	6 ppm over period of 3 hr. 45 min.	1 ppm over period of 45 min.
Harmonic suppression.	33 dB	33 dB	31 dB	6 dB	30 dB
AM hum and noise...	57.7 dB	52.8 dB	50.1 dB	24.9 dB	25.1 dB
D.C. current.....	230 ma at 10.0 volts	97.8 ma at 9.3 volts	56 ma at 11.0 volts	34 ma at 9.3 volts	74 ma at 9.3 volts
Efficiency into 50 Ω load	65.9%	32.4%	34.1%	2.6%	6.2%

The testing was performed under laboratory conditions of approximately 23 °C (73 °F) and 40 percent relative humidity, with each transmitter radiating into a 50 ohm load. Table 1 shows some of the test results. Others are described below. The following units were tested.

- #1—Nominal rf output 1 watt, carrier frequency 165.188 MHz, frequency modulated, powered by three 4.2 volt mercury batteries.
- #2—Nominal rf output 250 milliwatts, carrier frequency 165.188 MHz, frequency modulated, powered by three 4.2-volt mercury batteries.
- #3—Nominal rf output 250 milliwatts, carrier frequency 151.625 MHz, frequency modulated, powered by two 7-volt mercury batteries.
- #4—Nominal rf output 10 milliwatts, carrier frequency 159.300 MHz, frequency modulated, powered by one 9-volt alkaline battery.

Electronic Eavesdropping Techniques and Equipment

#5 — Nominal rf output 25 milliwatts, carrier frequency 154.890 MHz, phase modulated, powered by one 9-volt alkaline battery.

#6 — Nominal rf output 100 milliwatts, carrier frequency 154.890 MHz, frequency modulated, powered by one 9-volt alkaline battery.

Units #1, #2 and #3 were designed for body-worn use, while units #4 and #5 were designed for stationary application in a building to provide security against holdups. Therefore, a direct comparison of the first three units with units #4 and #5 is not appropriate. All units were comparable in size to a cigarette package and therefore could be concealed on a person. With regard to table 1, the harmonic suppression is the difference in signal strength between the fundamental output frequency of the transmitter and the next most powerful component of the radiated spectrum. It is desirable that this difference be as large as possible; thus, the larger numbers indicate the better performance. Spectrum-pictures of the output of the five transmitters are shown in figures 8, 10, 12, 14, and 16. AM hum and noise is a measure of the undesired amplitude modulation produced within the transmitter, and again the larger numbers indicate the better performance. The efficiency values given in the last row were calculated from the relationship,

$$E = \frac{P_{rf}}{P_{dc}} \times 100,$$

where P_{rf} is the rf power of the transmitter and P_{dc} is the product of the dc current and dc voltage supplied by the transmitter batteries. The dc voltage and rf power data are shown graphically in figures 7, 9, 11, 13 and 15.

Transmitter #1

Figure 7 shows the decay in rf output power due to the expenditure of battery energy over the operating period. Also shown on the same graph is the battery voltage variation over the same time period. The output power was nearly constant for the first hour and did not fall below the half-power point until approximately 2½ hours of operation. Three 4.2-volt mercury batteries were used to power the transmitter, and it appears that a cell failure may have occurred in one of the batteries near the end of the first hour. This would explain the rather significant drop in output power over the next 30 minutes of operation. This performance is apparently not typical, as is indicated by the data from the other transmitters. However, it does illustrate what can happen and shows how critical battery performance is to reliable operation. The output spectrum of this transmitter, shown in figure 8, remained essentially the same over a 3-hour period.

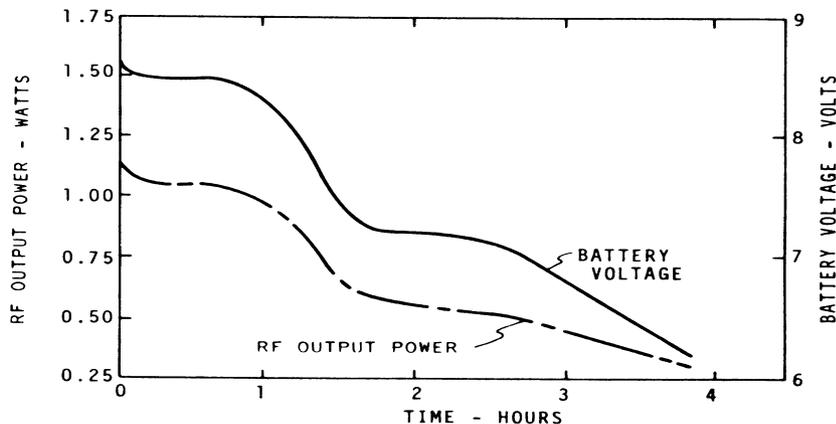


FIGURE 7. Decay of output power and battery voltage for transmitter #1.

Electronic Eavesdropping Techniques and Equipment

TRANSMITTER #1:

POWER APPROXIMATELY 1 WATT
 FREQUENCY (f_0) = 165.188 MHz

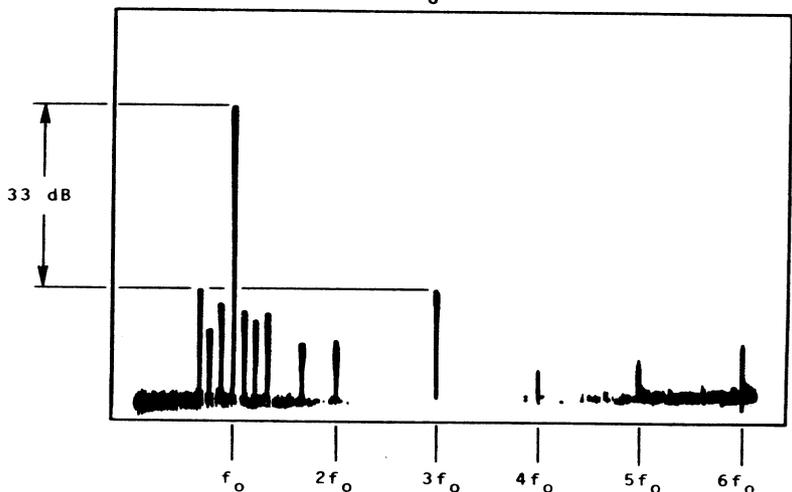


FIGURE 8. Output spectrum of transmitter #1.

Transmitter #2

As shown in figure 9, the decay in transmitter output was approximately linear after the first few minutes of operation, and the half-power output level was not reached until after 8 hours of operation. A cell failure appears to have occurred at approximately 7 hours and 45 minutes into the test. The batteries were three 4.2-volt mercury batteries of the same type and manufacturer as those used in the test of transmitter #1. This would appear to be typical of the expected performance. Figure 10 shows the output spectrum with the strongest spurious radiation being the fourth harmonic (660 MHz), which is approximately 33 dB lower than the fundamental carrier frequency output, f_0 .

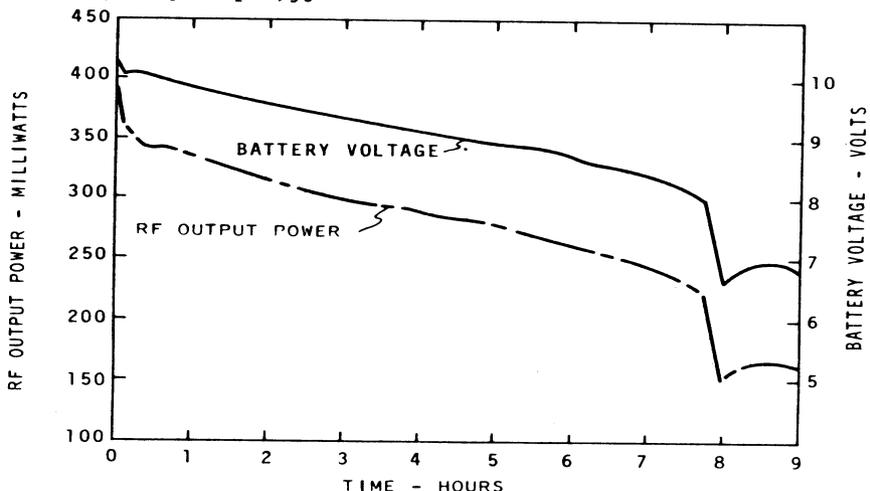


FIGURE 9. Decay of output power and battery voltage for transmitter #2.

Electronic Eavesdropping Techniques and Equipment

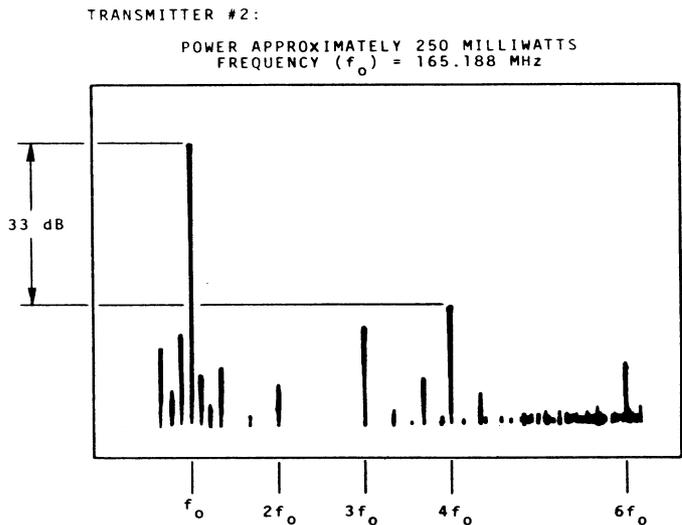


FIGURE 10. Output spectrum of transmitter #2.

Transmitter #3.

Referring to figure 11, it is apparent that the behavior of transmitter #3 was much the same as that of transmitter #2. Operation time to half-power output level was nearly the same. In this instance, the dc power supply was two 7-volt mercury batteries, and a cell failure occurred after approximately 6 hours and 15 minutes. The output spectrum (fig. 12) shows the spurious radiation to be down approximately 31 dB below the fundamental. In contrast to transmitters #1 and #2, the most intense spurious radiation was evidently not a harmonic of the fundamental frequency.

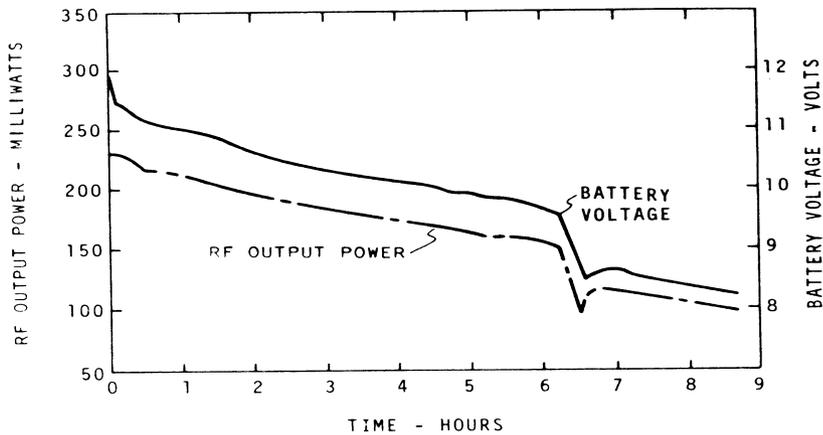


FIGURE 11. Decay of output power and battery voltage for transmitter #3.

Electronic Eavesdropping Techniques and Equipment

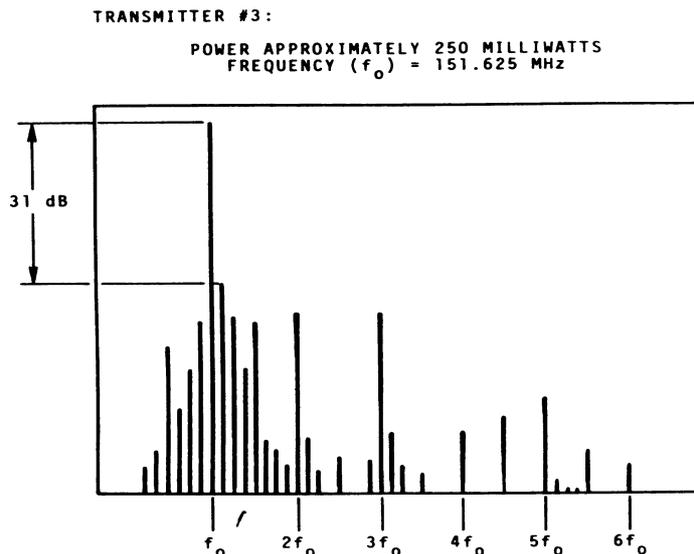


FIGURE 12. Output spectrum of transmitter #3.

Transmitter #4

One 9-volt carbon-zinc battery served as the dc supply for this transmitter, and its performance was noticeably different from those of transmitters #1, 2, and 3, which used mercury batteries. Transmitter #4 was received in a poorly adjusted condition, as can be seen from figures 13 and 14. For this reason, the spurious radiation level was only 6 dB below the fundamental carrier frequency output (fig. 14). In this condition, this transmitter would be unacceptable for undercover work because of the ease with which it could be detected by its excessive spurious radiation. Elimination of unwanted spurious radiation wastes power; when a bandpass filter was inserted between the transmitter and power meter to eliminate the spurious energy, the output power showed a very significant drop. This is shown by the curves labeled case 1 and case 2 in figure 13. Compared to other transmitters using mercury batteries, it is apparent that a rather large initial drop in output power occurs soon after turn-on when using carbon-zinc batteries, although the decay rate after the first hour or so appears to be comparable. Also, the mercury batteries do not appear to suffer the radical voltage drops under load evidenced by the carbon-zinc batteries. It should be noted that the efficiencies of this transmitter and transmitter #5 are quite low, which means that the radiated output energies are very low for the battery powers being expended.

Electronic Eavesdropping Techniques and Equipment

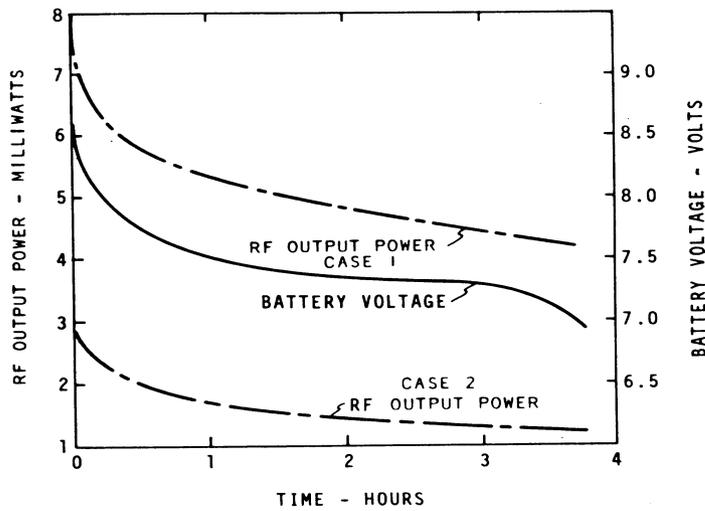


FIGURE 13. Decay of output power and battery voltage for transmitter #4.

TRANSMITTER #4:

POWER APPROXIMATELY 7 MILLIWATTS
 FREQUENCY (f_0) = 159.300 MHz

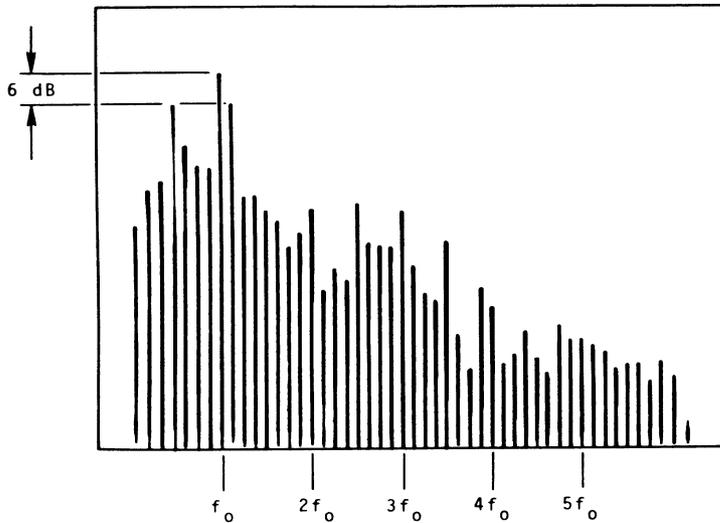


FIGURE 14. Output spectrum of transmitter #4.

Transmitter #5

As with transmitter #4, a 9-volt carbon-zinc battery was used as a dc power source for transmitter #5, and similar output characteristics were displayed, as shown in figure 15. However, the initial decay in output power was so severe that a half power level was reached after only a few minutes of operation. Such a transmitter might serve satisfactorily for short and intermittent use but would be unsatisfactory

Electronic Eavesdropping Techniques and Equipment

for most undercover missions. As with transmitter #4, a bandpass filter was inserted and the change in output power noted. Because the spurious radiation was an acceptable 30 dB below the carrier output (see fig. 16), there was a much less severe change in the output upon insertion of the filter, as is illustrated by the similarity between the curves of case 1 and case 2.

Carbon-zinc batteries are not recommended to power transmitters in undercover surveillance use because of their inability to provide adequate power. Both mercury batteries and alkaline batteries are much more satisfactory.

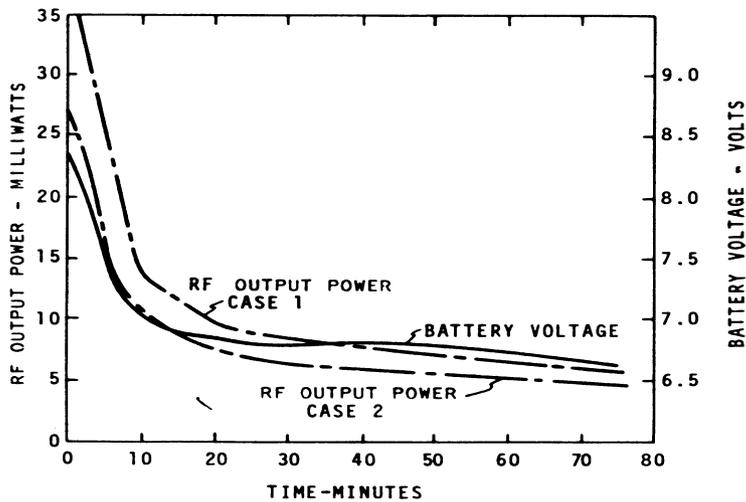


FIGURE 15. Decay of output power and battery voltage for transmitter #5.

TRANSMITTER #5:

POWER APPROXIMATELY 25 MILLIWATTS
 FREQUENCY (f_0) = 154.890 MHz

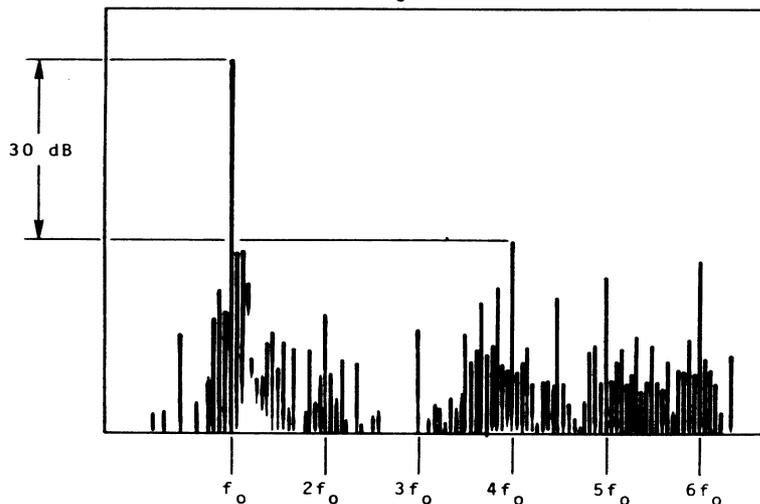


FIGURE 16. Output spectrum of transmitter #5.

Electronic Eavesdropping Techniques and Equipment

Transmitter #6

The sixth transmitter was tested to assess the difference in transmitter performance as a function of the type of battery used. It was operated until it reached its half-power output levels, first with a carbon-zinc battery and then with an alkaline battery. Figure 17 is a plot of the resulting data and shows a half-power lifetime of slightly more than 1½ hours using the alkaline battery compared to only 15 minutes with the carbon-zinc battery. The performance of mercury batteries is similar to that of the alkaline.

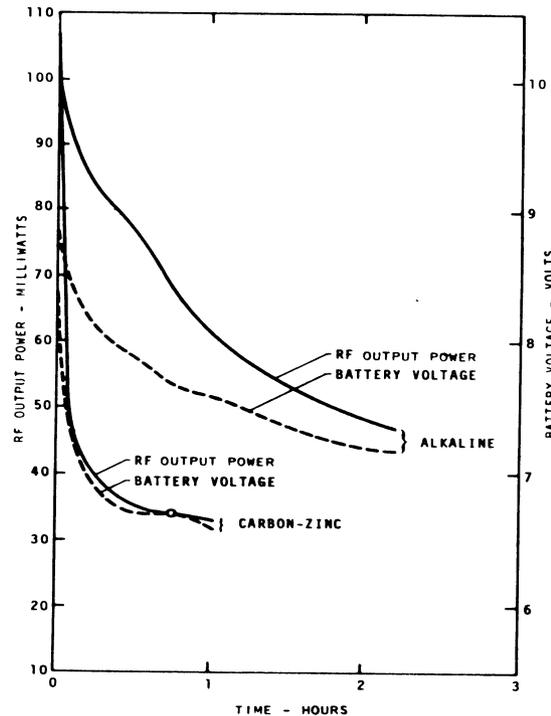


FIGURE 17. Decay of output power of transmitter #6 using alkaline and carbon-zinc batteries.

3.2. Field Tests of Body-Worn Transmitters

When the antenna of a transmitter is mounted on a human body, the effective radiated power of the transmitter is considerably reduced. To study this phenomenon, an outdoor test range was established and measurements were made under simulated field conditions. The data thus gathered are very interesting, and illustrate the amount of variation and the complexity of the problem of maintaining dependable communication using body-worn equipment.

The measurement setup, using a field strength meter at the receiver location, is illustrated in figure 18. Transmitter #1, described in section 3.1, was used. Measurements were made in the daytime under warm, dry conditions, and there were no buildings or other obstructions in the area. Initial measurements were made with the transmitter and its antenna mounted on a wooden post, with the transmitter and receiver antennas oriented vertically. A series of measurements were then made with the transmitter and its antenna mounted in various locations on a person with the person oriented at different angles to the receiving antenna. In all cases, the first position was with the subject facing the receiver with arms extended downward

Electronic Eavesdropping Techniques and Equipment

at the sides. Succeeding observations were made with the subject rotated clockwise to the successive 90 degree positions. To observe the changes in field strength due to arm movement, the arms were moved through a variety of positions including extending them directly overhead, to the front, and to the sides. The arm movements followed a consistent pattern of continuous motion during which the field strength fluctuations were observed on the meter. These fluctuations are shown for measurements two through six; the approximate variation of the field strength reading is indicated for each of the four facing positions. In some instances, arm movement appeared to increase signal strength perceptibly. The measurement conditions and data observed were as follows (observed field strengths at the receiver are given in dB above one microvolt per meter):

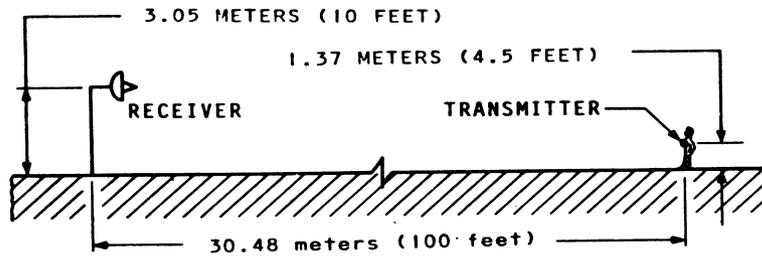
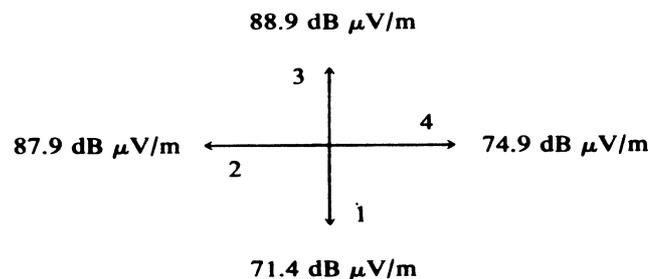


FIGURE 18. Test setup for field performance studies of body-worn transmitters.

Measurement #1.—Transmitter mounted on a vertical wooden post with transmitting and receiving antennas vertical. The observed field strength was 91.4 dB $\mu\text{V}/\text{m}$.

Measurement #2.—The transmitter was mounted on the under belt at approximately waist level (see figure 19). The antenna extended up the left side of the chest to the shoulder. The subject was wearing a cotton "T-shirt." The subject was then oriented at the four quadrant angles to the transmitter, and the variations due to arm movements were noted at each position. The transmitting and receiving antennas were oriented vertically.



Facing receiver—arms down in all positions

Changes in field strength, E, with arm movement

Position	Variation (dB)
1	-12 to +8
2	-4 to +1
3	-4 to +1
4	-4 to +1

Electronic Eavesdropping Techniques and Equipment

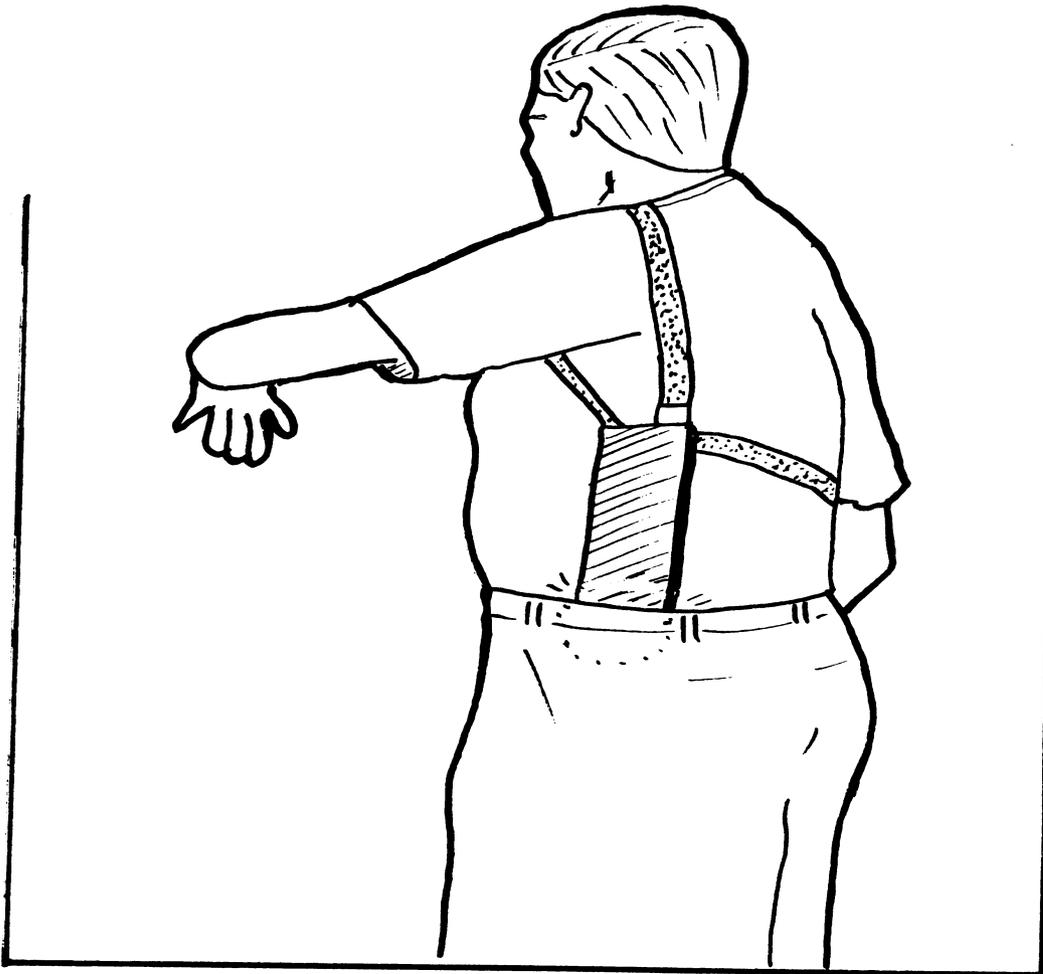


FIGURE 19. Transmitter position for measurement #2.

Electronic Eavesdropping Techniques and Equipment

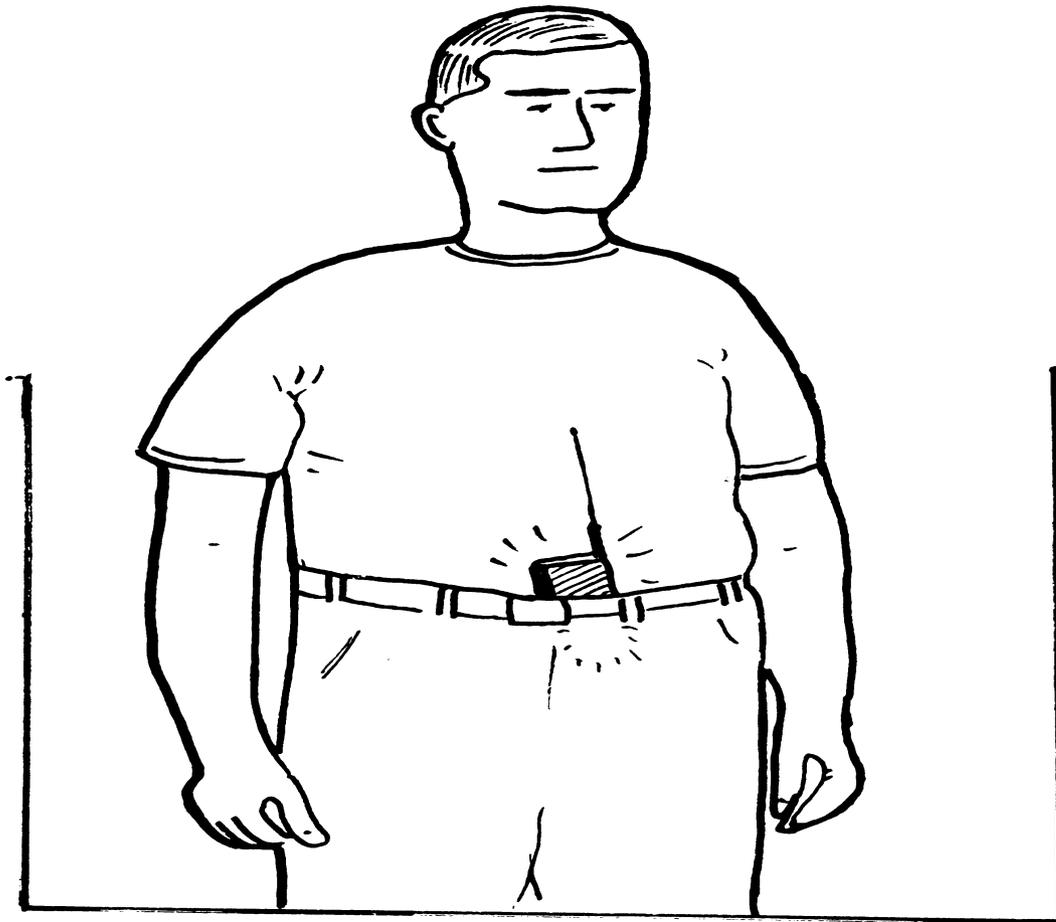
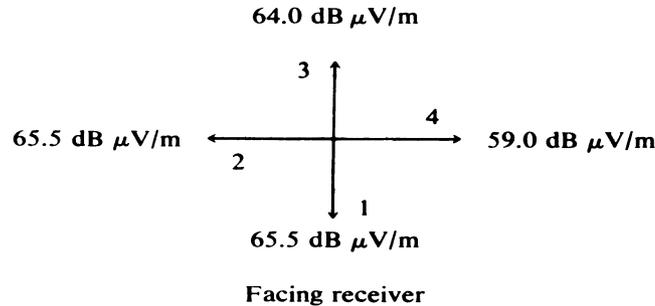


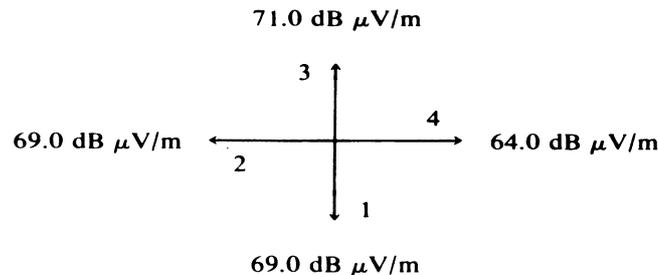
FIGURE 20. Transmitter position for measurement # 3.

Electronic Eavesdropping Techniques and Equipment

Measurement #7.—Both the transmitter and receiver antennas were oriented vertically, with the transmitter mounted on the left hip of the subject and the antenna extended down the thigh toward the knee.



Measurement #8.—The conditions were identical to those in #7 except that the transmitter was mounted at the knee of the subject and the antenna extended down the lower leg toward the ankle.



Note that measurements #1 through #6 were made on one day and measurements #7 and #8 were made on a second day. This allows the possibility that the radiated power from the transmitter might not have been equal on the two days. Therefore, it is not certain that upper-body mounting of the transmitter provides a larger signal, as the data would seem to indicate.

Although these data are by no means conclusive, several tentative conclusions can be drawn.

(1) When the body is between the transmitting and receiving antennas, there is a very significant reduction in the strength of the received signal. Therefore, the wearer should make every effort to keep himself oriented so that his transmitting antenna is on the same side of his body as the receiver.

(2) It is desirable to have the receiving antenna oriented parallel to the transmitting antenna. The data of measurement #6 show severe signal loss (approximately 25 dB) when the two antennas are perpendicular to each other.

(3) Arm movement is significant and can have a very important effect when communication is marginal. It is best to keep the arms as far away from the antenna as possible. Folding the arms across a chest-mounted antenna could attenuate a signal enough to make it unrecoverable.

4. NONRADIATING DEVICES

4.1. General

The distinguishing feature of nonradiating surveillance devices is the medium used to convey information from one location to another. The information is transmitted over wires, usually telephone wires, instead of being broadcast.

Wired surveillance systems have several distinct advantages over radiating systems. Most notable is the security from detection by an electronic sweep made by a radio receiver. Because virtually no electromagnetic energy is radiated from the wired network, this means of discovery is eliminated. A second very important consideration is the virtually unlimited range that is possible. Although the range of radiating devices is usually measured in feet, the range of wired systems can be measured in miles. In addition, wired communication systems include a source of dc voltage. Many wired surveillance devices utilize this built-in voltage source to eliminate the troublesome and limiting battery requirement. A final advantage which cannot be overlooked is the reliability of the communication medium. Wires are not affected by atmospheric conditions, and signals of consistent and dependable quality are almost certain, with the additional benefit that natural and man-made radiation interference are eliminated.

While wired systems have many advantages, they also have limitations. Restricted mobility is most often the reason a wired surveillance system is not used. In cases where the person under surveillance is on the move or located away from a fixed listening post, the use of wired equipment is obviously not feasible. A second drawback is that prior access to the premises is required to install listening devices or telephone taps. Also, in most instances, more advance preparation time is needed to set up wired equipment, so it is difficult to respond quickly to emergencies. Where these restrictions pose insurmountable problems, there is no choice but to use radiating devices.

In some states there are laws which prohibit telephone tapping. Therefore, portable and body-worn transmitters and receivers are essentially the only undercover communications devices available to law enforcement officers for electronic surveillance.

4.2. Telephone Taps

Surveillance must often be carried out by using remotely located tape recording equipment to record telephone conversations. The fact that telephone companies install extra wiring in anticipation of future demands for service provides a unique and convenient situation for wiretapping. Almost invariably, there will be one or more pairs of conductors in a cable which are not in use and which can be appropriated for surveillance purposes. These pairs are easily located at various access points in a given building or neighborhood by someone who is familiar with the telephone system and its equipment. Thus, not only the telephone itself but the whole wire communication network offers a limitless range of possibilities to the skillful technician. Even if a thorough examination were to determine that the telephone itself was not being tapped, there would still be no guarantee that a hidden microphone was not present which was carrying the conversation within a room to a remote listening post via telephone wiring. In the following paragraphs, some of the more frequently used telephone tapping methods and equipment are discussed along with the methods used to detect them.

4.2.1. "Infinity Transmitter" or "Harmonica Bug" [1]

Although the infinity transmitter is installed in the telephone, it does not monitor telephone conversations. Instead, it enables someone to listen in on a room conversation by means of another telephone. Once the device is installed in a telephone, a listener dials the number of the altered telephone in the customary manner. How-

Electronic Eavesdropping Techniques and Equipment

ever, just before the dialed telephone rings, an audible note or tone is transmitted over the phone line. This activates the bug, which opens the phone line without ringing, thereby enabling the caller to listen to any conversation taking place in the vicinity of the bugged telephone. The bug itself is an electronic switch which closes in response to the audio tone. It is wired in parallel with the hookswitch on the telephone so that, upon being activated, it prevents the telephone from ringing and opens the phone line at the same time. When this bug is in operation, the telephone will be busy to all other callers even though the receiver is in the cradle in the usual position. Thus, one symptom of the presence of such a bug is the receipt of a busy signal when the phone is known not to be in use. This device must be installed in the telephone and can be located by physical search. Defensive equipment is manufactured which will place a tone sweep on the phone line and detect the voltage drop from 48 volts to approximately 8 volts when such a bug is activated. A tone sweep is necessary because these bugs can be made to respond to a wide range of audio frequencies. The name "harmonica bug" is derived from the use of a common harmonica to actuate the device.

4.2.2. Inductive Coupling or "Pick-Up Coils"

A current in a conductor gives rise to a magnetic field around the conductor; when the current varies either in magnitude or direction, the magnetic field also changes. Conversely, if a conductor is immersed in a changing magnetic field, a current will be produced. This is the principle of the transformer and is used as a means of tapping a telephone. Various types of coils and pick-up loops can be employed to couple to an active telephone line and hence to monitor the conversation in progress. Many such devices are used in conjunction with an audio amplifier to actuate a tape recorder or to modulate a radio transmitter. Such devices do not produce any measurable loading or draw any detectable extra current from the line and therefore can not be located by voltage or current measurements. Physical search is practically the only means of detecting such a device.

4.2.3. Three-Wire Systems

A telephone may be used for both tapping and bugging simultaneously by the use of a third conductor for bypassing the hookswitch and thereby activating the mouthpiece for use as a room bug. Telephone hookswitch bypass is the term sometimes used to refer to this method of eavesdropping and some highly sophisticated electronic devices are employed to accomplish it and to make detection difficult.

4.2.4. Dialed Number Recorder

Although not a device for intercepting oral communication, the dialed number recorder is used to monitor telephone calls by providing a record of all numbers dialed from a particular telephone. These devices usually provide a paper tape printout of numbers dialed, and in addition may provide the date and time a call was made. Such devices were once called "pen registers" because a pen riding on a moving chart was used. The pen records the groups of pulses emitted by the telephone dial mechanism as it returns to the rest position. The dialed number is ascertained by counting the number of pulses in each group. In telephone systems using touch-tone dialing, a touch-tone decoder with a printed readout is used. These instruments are manufactured mainly for use by the telephone companies. Application is very simple, requiring only the connection of a lead to each side of the telephone line. No legal implications are involved, and connection can be made anywhere along the line between the telephone and the exchange. Detection of the presence of a dialed number recorder is extremely difficult by any means other than visual inspection, because these devices have a high input impedance and the line loading effect is negligible.

Electronic Eavesdropping Techniques and Equipment

4.3 Concealed Microphones

Microphones cannot be found by electromagnetic sensing devices. The only means of discovery is through physical search. Installation requires access to the premises, but the degree of concealment is limited only by the imagination of the installer, the cleverness of his methods, and the time he has to work. The basic equipment required consists of a microphone as small as possible, the necessary length of shielded wire, and a tape recorder. Shielded wire is used where possible to avoid unwanted pickup, such as power line hum or other noise coupled into the circuit. For short lead lengths, very fine wires can be run along baseboards, window sills, or under floor coverings. Conducting paint can be used to form a conducting path on a wall surface. This is done by simply painting thin conducting stripes on the surface as required, and making electrical connections at the ends of the painted stripes. These stripes can then be painted over with regular paint, making discovery difficult.

Excellent microphones as small as 10 mm × 7 mm × 5 mm ($\frac{3}{8}'' \times \frac{1}{4}'' \times \frac{3}{16}''$) are available, with sensitivities such that they can pick up a whisper at approximately 7.5 meters (25 feet). These can be combined with an amplifier of comparable size so that a listening post can be established several miles away, using a pair of unused telephone wires.

The small dynamic-type microphones commonly used for these purposes require a column of air (a leak) directly in front of the pick-up surface so that, in mounting them, a very small hole must be drilled in the object used for concealment. Sometimes, plastic tubing threaded through a crack serves this purpose and aids in concealment. Microphones equipped with a small section of metal tube directly over the microphone leak opening are available for attaching the tubing.

In the use of a microphone for eavesdropping, it is important that precautions be taken to avoid rubbing against the microphone because this introduces noise. This becomes a problem especially when a microphone is used with a body-worn transmitter which is hidden in clothing. Friction from cloth rubbing against the microphone is called "clothes noise" and poses a problem in obtaining good quality sound reproduction.

Miniature surveillance microphones, with their amplifiers, have characteristics similar to those of the human ear. The fact that the ear and the microphone can detect the same sound at the same distance provides a guide to the limits of a physical search for a hidden microphone. There are devices such as the highly directional shotgun or parabolic microphones which have greater ranges, but they are much more difficult to conceal. These instruments can detect normal conversation at ranges of 50 to 100 feet. Their increased range is derived from their directionality and, for some, their acoustic amplification. This directionality prevents interference from any direction other than that in which the device is pointed. One defense against such devices is to add background sounds, such as music. This, along with speaking in low voices, can render the recorded conversation unintelligible.

Microphone technology is an extensive field, and no attempt will be made to cover the subject in depth. However, several types of microphones which are of special interest in electronic surveillance, and which find fairly wide application, will be described briefly [2, 14, 16].

4.3.1. Carbon Microphones

The carbon microphone is the type used in the mouthpiece of the telephone transmitter. It operates on the principle that the resistance of a package of carbon granules varies as the external pressure on the package changes. When mounted behind a vibrating diaphragm and energized with a dc voltage, the carbon microphone will cause the current in the circuit to vary in accordance with the sound striking the diaphragm. This modulating effect enables the voice to be transmitted over the

Electronic Eavesdropping Techniques and Equipment

telephone circuit. Carbon microphones are very sensitive but have a rather high background noise of the hiss type. They do not lend themselves to miniaturization as well as other types of microphones.

4.3.2. Condenser Microphone

Also referred to as an electrostatic microphone, the condenser microphone utilizes a vibrating diaphragm as one plate of a parallel-plate, air-dielectric capacitor. Sound striking the diaphragm produces capacitance variations which, in turn, produce electrical impulses. Condenser microphones can be made very sensitive and reproduce sound with excellent fidelity, but they have the disadvantages of being fragile and sensitive to vibrations transmitted through solids. For these reasons, they are generally not suitable for eavesdropping applications.

4.3.3. Electrodynamic Microphone

Often called simply a dynamic microphone, this is the type most commonly used in electronic surveillance. These microphones have many desirable features. They can be very small, adequately sensitive, rugged, and require no external power source. The modulated current is generated by the motion of a coil of wire in the field of a permanent magnet.

4.3.4. Electret Microphone

Recent technology [5] has resulted in the development of miniature electret microphones which have many features useful in electronic surveillance work. An electret is the electrical analog to a permanent magnet. A permanently polarized dielectric material which is sensitive to pressure changes produced by acoustic energy is used as the sensing element. Operation is similar to that of the condenser microphone, but the electret microphone is much more resistant to shock and solid-borne vibration. Advantages of the electret are that no external bias is required, and it has a frequency response which is superior to those of other types. Superior frequency response, however, is not of first-order importance in electronic surveillance, where only voice frequencies are of interest. Electrets perform well under temperature extremes and may be slightly superior from the standpoint of ruggedness, but one precautionary note is worthy of mention. While it appears that better materials are being developed which will diminish the problem, periods of humidity in the range of 90 percent or more cause drastic loss of sensitivity. Should this problem be overcome and costs made competitive with those of the dynamic types, the electret may become the preferred type of microphone. At present, however, the electret appears to be little used, and it may be several years before this situation changes.

4.3.5. Induction Microphone

The induction microphone is very similar in principle of operation to the electrodynamic microphone in that both incorporate a moving conductor in the field of a permanent magnet. The induction microphone utilizes a fixed coil and a moving piece of magnetic material, whereas the electrodynamic type employs a moving coil and is often much smaller. A common example of the induction microphone is the ear piece of the telephone. These microphones are sometimes used as room bugs where concealment problems do not require a device as small as the electrodynamic type. Because they are used in telephones, they are inexpensive and readily available; this explains their common use.

Electronic Eavesdropping Techniques and Equipment

4.4. Advantages and Disadvantages of Wired Surveillance Systems

Advantages	Disadvantages
<ol style="list-style-type: none">1. Unlimited range.2. Operating time not limited by battery life.3. Not subject to radiated electromagnetic interference.4. Not detectable by electromagnetic sensors.5. Personal contact with subject not required.	<ol style="list-style-type: none">1. Prior access to premises required.2. Lack of mobility.3. Outlawed in some states, court order required in others to use telephone system.4. Installation requires highly skilled people.

5. TAPE RECORDERS

In gathering legal evidence through electronic surveillance, the tape recorder is an indispensable item. Whether the surveillance method is a radiating system involving transmitters and receivers or a wired system using a telephone tap or a concealed microphone, a tape recorder is invariably involved. Many very good tape recorders are available, but there are apparently none designed specifically for surveillance purposes. In general, most good tape recorders are adequate to perform the functions required by electronic surveillance, especially in regard to sensitivity and frequency response. Both open-reel and cassette-type recorders are used.

5.1. Open-Reel Tape Recorders

The main advantage of the open-reel recorder is its large tape capacity, which allows for very long periods of recording without the necessity of changing reels. It generally yields broader frequency response, but this is not required for good fidelity in voice reproduction since the voice frequency band is relatively narrow. Important options available on open-reel recorders include voice-actuation, and automatic shut-off at the end of a reel so that tape flap noise will not reveal the presence of a hidden recorder. Temperature extremes are to be avoided; the temperature inside the trunk of an automobile on a hot day, for example, can cause serious operational difficulties.

5.2. Cassette Tape Recorders

The cassette is being used increasingly in spite of its smaller recording capacity. This is due to the advantages of small size and ease of operation; it is much quicker and easier to change and handle the tape. Miniature versions of the cassette tape recorder are now making their appearance, and at least one model is available which is small enough for concealment within clothing, its dimensions being 5 cm × 7.5 cm × 2.5 cm (2'' × 3'' × 1''). This will have a significant bearing on the application of recorders and could conceivably displace radiating equipment in certain situations.

5.3. Telephone Recording Actuator

In order that a tape recorder not be required to run continuously, or be monitored continuously, a recorder actuator may be used. With the actuator, the tape recorder is turned on when the telephone receiver is lifted from the cradle and turned off when it is replaced. These actuator devices may be attached to a telephone line at any point between the telephone and the control switchboard. They are battery powered, so they create no detectable electrical effect on the telephone line. These devices utilize the fact that the voltage on the telephone line drops from 48 volts to approximately 8 volts when the receiver is lifted from the cradle.

6. CONCLUSIONS AND RECOMMENDATIONS

There are several standards available to gauge the quality and performance of personal/portable electronic equipment [3, 11, 12]. However, there is a degree of

Electronic Eavesdropping Techniques and Equipment

uniqueness about electronic surveillance equipment which would seem to require standards especially tailored for these devices. As an example, since battery life is so critically important in the case of body-worn transmitters, it follows that maximum use should be made of available power. This leads to the need for some standard for transmitter efficiency. This does not mean that a simple specification of efficiency based upon power delivered into a 50-ohm load would be appropriate, because few of these devices are designed to work into 50 ohms. It would be desirable to develop some criteria whereby a high level of efficiency could be assured, thereby providing the maximum signal strength and transmitting time consistent with the battery power available.

A second component of a standard should be a specification of operating frequencies. This would include a safeguard against the use of transmitters operating in the aircraft landing system bands, which could constitute a very serious hazard to air travel. A serious accident caused by an electronic surveillance system operating on instrument landing system frequencies is too high a price to pay for any evidence which might be thus obtained. The exclusion of these frequencies would eliminate the use of the detuned commercial FM receiver as a listening post, and require the purchase of receivers manufactured specifically for surveillance work. Although this is an economic penalty, it will likely pay off handsomely in terms of system performance because many commercial FM undercover receivers are of relatively poor quality.

Finally, the modulation bandwidths characteristic of high-fidelity equipment are not required for good quality voice communication. Therefore, the standard can afford to relax some of the requirements normally made of equipment used, for example, in the entertainment industry.

The need for high-quality training for those engaged in electronic surveillance work is most evident. This work encompasses a large body of knowledge, much of which is not found in textbooks and which can therefore be conveyed only by those with experience.

Much additional work is needed in the area of antenna design and evaluation, especially of body-mounted antennas where large variations in received signal strength are observable.

In the process of gathering information for the preparation of this report, one fact was outstandingly evident. This was that information regarding the manufacturers of electronic surveillance equipment and the places where such equipment could be purchased, was difficult to obtain. On the positive side, this would indicate that the present laws governing the advertising of such equipment are proving effective. From the side of law enforcement, however, this presents a serious problem. Where there is a legitimate need for electronic surveillance, law enforcement personnel need ready access to current information on the sources for the purchase of equipment and instruction in its use. Many law enforcement officials have expressed a desire for a users guide that could be consulted for information on a particular type of equipment, who manufactures it, and how the products of the various manufacturers compare, for the money invested. The development of objective performance standards is a step in this direction. In the meantime, however, it appears that law enforcement agencies would benefit greatly from some source of current information on manufacturers and suppliers. A listing of known manufacturers of electronic eavesdropping equipment is included as appendix B. This list is not complete for the reason given above, but it includes most of the companies which sell equipment for this purpose.

APPENDIX ANNOTATED BIBLIOGRAPHY

- [1] Brown, R. M., *The Electronic Invasion*, John F. Rider Publishing, Inc., New York, 1967.

This book deals with the many types and applications of devices usable for eavesdropping, as well as those used to detect the presence of such devices. For almost every device discussed, there is given the name of its manufacturer and often the prices as well. Because many manufacturers of such equipment are small firms, it may be found that many are no longer in business. The book is written in a popularized style and contains a great deal of general information along with some technical information, including circuit diagrams.
- [2] Dash, S., Schwartz, R. F., and Knowlton, R. E., *The Eavesdroppers*, Rutgers University Press, New Brunswick, N.J., 1959.

This is a lengthy book written in three parts, namely the practice, the tools, and the law as they pertain to eavesdropping. Probably because the book was written prior to the advent of miniaturized electronics, it does not deal with radiating equipment. However, it is quite comprehensive and informative on such subjects as video devices in use up to the date of publication. Also included is a good bibliography.
- [3] EIA Standard RS-316, *Minimum Standards for Portable/Personal Land Mobile Communications FM or PM Equipment 25-470 MHz*, Electronics Industries Association, 11 West 42nd Street, New York, N.Y., July 1965.
- [4] Farmer, R. A., "SINAD System Design," *IRE Transactions on Vehicular Communications*, Vol. VC-10, No. 1, Apr. 1961, pp. 103-108.

This paper describes the SINAD system for evaluating performance of a mobile communications system as well as explaining its use and advantages in evaluating system components and parameters, such as receiver sensitivity and selectivity. It also discusses the problems of site noise and propagation and terrain variations. Specific data are given for frequencies in the vicinity of 50, 150, and 450 MHz, which are the frequencies of major interest in undercover communications work.
- [5] Fraim, F., and Murphy, P., "Miniature Electret Microphones," *Journal of the Audio Engineering Society*, Vol. 18, No. 5, Oct. 1970, pp. 511-517.

This technical paper discusses the development of miniaturized electret microphones, tells how they are constructed and the requirements of the preamplifiers used with them. The significant performance characteristics of the electret are discussed along with their strengths and weaknesses, and comparisons are made to other types of miniature microphones.
- [6] Greene, R. M., Jr., editor, *Business Intelligence and Espionage*, Dow Jones-Irwin, Inc., Homewood, Illinois, Oct. 1966.

Chapter 11 of this book is entitled "Electronic Eavesdropping (Bugging): Its Use and Countermeasures." It is an essentially nontechnical discussion of both radiating and wired devices used in undercover information-gathering activities. No attempt is made to delve into the engineering and technical characteristics of the devices described; instead, it gives an overview of the types of devices in use, a brief description of what they do and how they are applied.
- [7] Huber, J. L., "Signal Attenuation for Passenger Vehicles Between 0.1 and 1.0 GHz," *Proceedings of the 1970 Carnahan Conference on Electronic Crime Countermeasures*, Bulletin 92, Apr. 1970.

Signal attenuation experienced when transmitted energy was radiated from the inside of various vehicles was observed to vary from 3 to 15 dB for

Electronic Eavesdropping Techniques and Equipment

a vertically polarized antenna and from 10 to 30 dB with a horizontally polarized antenna over the frequency range 0.1 to 1.0 GHz. Wide variations occurred in a cyclic pattern with the average attenuation over all frequencies being around 15 dB.

- [8] Jesch, R. L., and Berry, I. S., *Batteries Used with Law Enforcement Communications Equipment, Comparison and Performance Characteristics*, LESP-RPT-0201.00, National Institute of Law Enforcement and Criminal Justice, U.S. Department of Justice, GPO Stock Number 2700-0156, May 1972.

This report is the result of an extensive literature search conducted in the field of primary and secondary batteries. It lists terms and definitions pertaining to batteries and their characteristics, reviews basic battery principles, and types and assembles performance characteristics of battery systems into chart form for comparison purposes. Includes basic precautions and references to pertinent literature.

- [9] King, H. E., and Yowell, C. O., *Assessment of Technology Applicable to Body-Mounted Antennas*, prepared for the Law Enforcement Assistance Administration, U.S. Department of Justice, Contract No. F04701072-C-0073, Controlled Access, Mar. 1973.

This report was written in connection with a development effort on body-mounted antennas for police transceivers. Although these antennas are not necessarily designed for concealment, such as those used with surveillance equipment, there are many common problems and interests in the two applications. The report contains a great deal of analytical and measurement information pertinent to the manufacture and use of surveillance equipment. Subject headings include electrically small antennas, antenna types, antenna and the body, and propagation information.

- [10] Mason, J. F., "Designers Compete for that Snug Automatic Bug in a Rug," *Electronic Design*, Vol. 21, No. 20, Sept. 27, 1973, pp. 22-30.

This popularized article discusses many of the modern techniques of electronic audio surveillance and concentrates on devices utilizing the telephone. Both hard wire and transmitting devices are pictured and briefly explained. One page of this article shows the circuit diagram of a common telephone and tells 12 ways of tapping it. Some discussion of countermeasure devices is included near the end of the article, along with some predictions as to what the future will bring in the advancement and sophistication of electron audio surveillance.

- [11] NILECJ-STD-0203.00, *NILECJ Standard for Personal/Portable FM Transmitters*, National Institute of Law Enforcement and Criminal Justice, U.S. Department of Justice, GPO Stock Number 027-000-00293, Oct. 1974.

This document establishes performance requirements and methods of test for frequency modulated personal/portable transmitters used by law enforcement agencies. Equipment that meets these requirements is of superior quality and is suited to the needs of most law enforcement agencies. This standard may be referenced in procurement documents and used to determine whether or not purchased equipment meets stated requirements.

- [12] NILECJ-STD-0208.00, *NILECJ Standard for Personal/Portable FM Receivers*, National Institute of Law Enforcement and Criminal Justice, U.S. Department of Justice, (in press).

This document establishes performance requirements and methods of test for frequency modulated personal/portable receivers used by law enforcement agen-

cies. Equipment that meets these requirements is of superior quality and is suited to the needs of most law enforcement agencies. This standard may be referenced in procurement documents and used to determine whether or not purchased equipment meets stated requirements.

- [13] Oliver, B. M., and Cage, J. M., editors, "Electronic Measurements and Instrumentation," *Inter-University Electronics Series*, Vol. 12, McGraw-Hill Book Company, New York, N.Y., 1971.

This is a comprehensive book on the theory and techniques of a very wide variety of electrical and electronic measurements. Of particular importance to the subject of this report is chapter 14, which deals with measurements on transmitters and receivers. This chapter also includes a comprehensive listing of specifications concerned with radio receiving or transmitting equipment used for communication or navigation purposes. Specifications listed include those of the Electronic Industries Association (EIA), Aeronautical Radio Incorporated (ARINC), Federal Communications Commission (FCC), Military Specifications (MIL), and the Defense Communications Agency (DCA).

- [14] Olson, H. F., *Acoustical Engineering*, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1957, Ch. 8.

This book contains a very detailed chapter covering microphones. Theoretical relationships, equivalent mechanical and electrical circuits, and frequency response curves for the various types are given, along with cross section drawings to illustrate operating principles. The book also has an excellent chapter on recording.

- [15] Pollock, D. A., *Methods of Electronic Audio Surveillance*, Charles C. Thomas Publishing Co., 301-327 East Lawrence Avenue, Springfield, Illinois, 1973.

This book is presented as an electronics manual for detectives. Following an introductory chapter on basic electricity and electronics, the principles of audio, telephone, and radio frequency communication systems are explained. A practical applications section on operational techniques is included, followed by some material on countermeasures. In the concluding section of the book are chapters on legal aspects, administrative control, and ethics. An appendix comprising several sections includes a glossary of terms and a partial listing of distributors of audio surveillance devices and essential electronic components. The section on operational techniques is quite explicit in the explanations it gives for installing room bugs and telephone taps of various kinds.

- [16] Randall, R. H., *An Introduction to Acoustics*, Addison-Wesley Press, Inc., Cambridge, Mass., 1951, pp. 240-246.

This is a college text that provides a discussion of various types of microphones, including carbon, capacitor, electrodynamic, and crystal types, and gives a comparison of their relative sensitivities.

- [17] Rice, L. P., Radio Transmission and Buildings at 35 to 150 Mc. *The Bell System Technical Journal*, Jan. 1959, pp. 197-210.

Work done in an attempt to determine the relative merits of two frequencies for propagation into buildings is reported and analyzed statistically. Although not greatly different, the 150 Mc coverage was found to be better than that at 35 Mc in most instances. At both frequencies, reception was better on upper floors of the building than on lower floors, although this latter phenomenon may have been due to the elevation of the transmitting antenna used in the experiments.

- [18] Shrader, R. L., *Electronic Communication*, Second Edition, McGraw-Hill Book Company, Inc., New York.

Nortel DMS-100 Office Parameters Overview

Introduction

Office parameters are initially set by Northern Telecom (Nortel) to meet end-of-design criteria and switch configuration. This overview is intended to assist operating company personnel responsible for administering office parameters by providing guidelines to using the available tools.

Office parameters examined in this document are located in table OFCENG (Office Engineering). These parameters allocate resources (memory) for switch activities such as call throughput and custom calling usage. These parameters are initially calculated using operating company input, high day/end-of-design criteria, and standard engineering formulas. The formulas are designed for standardization and simplified operating company and Nortel use. The formulas are constructed to cover a wide variety of applications and are considered set up for end-of-design for most applications.

An ongoing process should take place to determine if parameter settings are appropriate for each office's requirements. This process should include the monitoring of actual parameter usage compared to the parameter setting in the switch. Offices may have to adjust individual parameter settings to match the changing office requirements.

Offices not at the end-of-design could reclaim memory for a period of time by reducing office parameter settings. Caution should be used in lowering office parameters to prevent impact to switch operation during high-day operation. Some parameters are not recommended for value reduction. See the section "*Office Parameters that are Not Recommended to be Modified*".

Memory allocated for office parameters can be reclaimed during the software delivery by way of dump and restore if the decision is made to lower office parameters. However, office parameter changes should be safely and systematically implemented before a dump and restore.

What to Collect

The following data should be collected to determine the usage of many of the office parameters in table OFCENG:

- Operational Measurement groups CP2, EXT, and FTRQ.
- DMSMON report.
- Listing of table OFCENG.

Operational Measurements

The Operational Measurements (OM) and especially the high watermark OMs can be used as a bench mark of the levels of traffic-dependent activity in the switch during the current interval. The high watermark OMs display the highest level of simultaneous usage reached in critical office parameters for the collection period. Overflow OMs display the number of times that the parameter was required but no resources were available.

The following OM groups should be monitored:

- CP2
- EXT
- FTRQ

CP2 measures Call Processing software resources such as call processing letters, call condense blocks, and wakeup blocks. EXT measures Extension Block usage such as special billing records, data extensions for operator services, and custom calling features. FTRQ measures Feature Queuing Resources for Meridian Digital Centrex (MDC) features such as call hold, last number redial, and call waiting. Refer to the *Operational Measurements Reference Manual* for information on the registers and corresponding office parameters measured.

An OM accumulating class made up of CP2, EXT, and FTRQ should be defined with the same collection period as office parameter OMXFR in table OFCENG. When datafilling tables OMACC and OMPRT, field WHEN set to AUTO guarantees this. The collection period and transfer period should be the same to ensure that the high watermark registers present a valid picture of peak activities. With a 1-hour collection period and a 30-minute transfer period, the peak levels are summed.

The following is an example of setting up an OM class that contains OM groups EXT, CP2, and FTRQ. The symbol ">" represents commands to be entered.

The OM class to be defined is called REALTIM3. Double precision is used.

```
>OMCLASS REALTIM3 DOUBLE
```

List table OMACC to see the tuple added.

```
>LIS ALL
```

The table is listed. Position on the newly added tuple.

```
>POS REALTIM3
CLASS      ENABLED   WHEN
REALTIM3  N           AUTO
```

Change the tuple.

```
>CHA
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT.
>Y
ENABLED: N
>Y
REP: AUTO
TUPLE TO BE CHANGED:
REALTIM3 Y AUTO
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE CHANGED. WRITTEN TO JOURNAL FILE AS JF NUMBER 544
>QUIT
CI:
```

Add OM groups to the OM class.

```
>OMACCGRP REALTIM3 ADD GROUP CP2
OK
>OMACCGRP REALTIM3 ADD GROUP FTRQ
OK
>OMDUMP CLASS REALTIM3 COMMANDS
OMCLASS REALTIM3 DOUBLE
OMACCGRP REALTIM3 ADD GROUP CP2
OMACCGRP REALTIM3 ADD GROUP EXT
```

```
OMACCGRP REALTIM3 ADD GROUP FTRQ
```

```
>TABLE OMPRT
```

```
TABLE: OMPRT
```

```
>LIS ALL
```

Table OMPRT is listed. Position on an unused position. Position 228 is chosen in this example.

```
>POS 228
```

Change the tuple.

```
>CHA
```

```
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
```

```
>Y
```

```
ACTIVE: N
```

```
>Y
```

```
SUPZERO: N
```

```
>
```

```
ID: ALL
```

```
>ALLCLASS
```

```
CLASS:
```

```
>REALTIM3
```

```
REP: MONTHLY
```

```
>AUTO
```

```
BUFFOUT: N
```

```
>
```

```
OUTDEV: SINK
```

```
>
```

```
TUPLE TO BE CHANGED:
```

```
228 Y N ALLCLASS REALTIM3
```

```
AUTO N SINK
```

```
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

```
>Y
```

```
TUPLE CHANGED
```

```
WRITTEN TO JOURNAL FILE AS JF NUMBER 547
```

```
>QUIT
```

```
CI:
```

```
>LOGUTIL
```

```
LOGUTIL:
```

```
>ADDREP TATSPRT OMPR 228 Note: TATSPRT is a local printer defined for this example.
```

```
1 report(s) Added
```

```
>LISTROUTE DEVICE TATSPRT
```

```
Device TATSPRT print classes:
```

```
ADD REPORTS:
```

```
OMPR 228 (OM REPORT)
```

```
DELETE REPORTS:
```

```
>STARTDEV TATSPRT
```

```
Log device TATSPRT has been started.
```

```
Number of devices started : 1
```

```
>STOPDEV TATSPRT
```

```
Log device TATSPRT has been stopped.
```

```
Number of devices stopped : 1
```

DMSMON

DMSMON is used to gather switch data as well as high watermark OMs. The switch data can be used in calculating office parameters in place of the engineering estimates used at initial load time.

DMSMON uses OM results as inputs for the DMSMON high watermark report. DMSMON itself keeps a running tab of a subset of parameter high watermarks over a 30-day period. For the parameters that are currently reported by DMSMON, this report is the easiest for the administrator

to use. However, since all the high watermark OMs are not included in DMSMON, the OM groups mentioned previously should be collected. Also, parameter overflows are not reported in DMSMON output, only in the OM groups.

The following command produces the needed DMSMON information from the CI level of the MAP display:

```
>DMSMON  
>HIGHPARMS
```

The following DMSMON example shows a subset of actual counts of switch data and high watermarks for office parameters:

```
-----  
Number of nodes: 379  
Number of networks: 0  
  
Number of TM8 PMs: Insv: 3 Comm : 0  
Number of MTM PMs: Insv: 53 Comm: 0  
Number of LGC PMs: Insv: 12 Comm : 0  
Number of LCM PMs: Insv: 48 Comm : 0  
Number of DTC PMs: Insv: 13 Comm : 0  
Number of DP_POTS lines: 3  
Number of DGT_POTS lines: 15  
Number of DP_IBN lines: 185  
Number of DGT_IBN lines: 2835  
Number of TOTAL_UNEQ lines: 15962  
Number of TOTAL_OFFL lines: 5373  
Number of PPHONE_STATION lines: 152  
  
Number of DISPLAY_PPHONE_STATION lines: 35  
Number of M3009_STATION lines: 6705  
  
Number of M5112_STATION lines: 618  
Number of M5209_STATION lines: 144  
Number of M5312_STATION lines: 37  
Number of DNs on keysets: 35403  
Number of IBN lines with CALL WAITING FEATURE: 8  
Number of IBN lines with CALL FORWARDING FEATURES: 508  
Number of IBN lines with SPEED CALL FEATURE: 225  
Number of KSET lines with CALL WAITING FEATURE: 4  
Number of KSET lines with CALL FORWARDING FEATURE: 6613  
Number of KSET lines with SPEED CALL FEATURE: 6327  
Number of trunks: 4704  
Number of unequipped trunks: 10655  
Number of offline trunks: 554  
Number of trunk groups: 715  
Number of IBNTI trunks: 893  
Number of IBNTO trunks: 334  
Number of IBNT2 trunks: 49  
Number of OP trunks: 52  
Number of RCVRMF receivers: 8  
Number of RCVRDGT receivers: 4 (expected:8) *****  
  
Number of RCVRATD receivers: 32  
Number of CF3 ports: 70  
Number of CF6 ports: 83  
Number of LTUs: 6  
Number of TTUs: 5  
Number of VDUs: 39  
  
Number of customer groups: 253
```

Number of consoleless customer groups: 250
 Number of customer subgroups: 2
 Number of attendant consoles: 30

Tables of Daily Usage for Critical Office Parameters

The following partial report shows 20 days of high watermark values with the most current one (yesterday) being printed first.

Example 1

NUMCPLETTERS	NCCBS	NUMCALLPROCESSES	NUMOUTBUFFS	NMULTIBLKS	NUMCPWAKE
13	97	4	51	2	6
12	105	4	51	3	3
17	914	4	51	13	28
18	908	4	51	16	32
16	893	5	51	14	29
14	761	5	51	11	27
13	63	4	51	2	4
12	70	4	51	3	7
12	85	4	51	3	8
12	457	4	51	7	19
18	504	4	51	9	18
11	435	4	51	8	19
12	273	4	51	5	13
12	63	4	51	3	4
12	66	3	51	2	4
12	80	4	51	3	8
12	512	4	51	9	21
14	796	5	51	12	31
23	941	5	51	15	50
16	874	5	51	13	31

-End-

Example 2

FTRQAGENTS	FTRQ0WAREAS	FTRQ2WAREAS	FTRQ4WAREAS	FTRQ8WAREAS	FTRQ16WAREAS
9435	0	3437	6230	0	0
9437	0	3511	6179	2	1
9451	0	3862	6120	12	3
9445	0	3865	6185	11	3
9459	0	3784	6330	14	2
9451	0	3587	6360	10	2
9435	0	3334	6361	0	0
9436	0	3345	6342	0	0
9435	0	3377	6337	0	0
9443	0	3469	6359	7	2
9441	0	3458	6390	7	2
9440	0	3456	6396	6	3
9437	0	3458	6327	8	3
9430	0	3451	6283	0	0
9430	0	3454	6271	0	0
9429	0	3450	6265	0	0
9439	0	3582	6261	4	2
9435	0	3796	6174	10	3
9438	0	3935	6090	14	3
9433	0	3923	6090	16	2

-End-

Table OFCENG

Table OFCENG lists the setting of parameter values. This table should be listed to provide the parameters to be considered and their current settings. The table can be listed with the following CI command:

```
>TABLE OFCENG;LIST ALL;QUIT
```

The following example shows a subset of table OFCENG:

Parameter Name	Parameter Value
ACD_MIB_OUT_EVENT_BUFFER_SIZE	110
ACD_TOLL_DELAYED_BILLING	N
ACT_MAX_DURATION	255
ALL_ACD_LOGIN_IDS_VALID	Y
ALT_TTT_USAGE_PERCENTAGE	50
AMA_FAILURE_FREE_CALL	Y
AMA_LONG_DUR_AUDIT_INTERVAL	24
ATTLOG	1000
AVG_NUM_TGS_PER_OHCBQCALL	4
BELL_ANI_ALARM_ID	9
BELL_ANI_INTERCEPT_ID	9
CABLE_LOCATE_TIMEOUT	180
CABLE_SHORT_TIMEOUT	180
CC_ENGLEVELE_WARNING_THRESHOLD	77
CFD_EXT_BLOCKS	3500
CFW_EXT_BLOCKS	350
COINDISPOSAL	IGNORE_COIN
COMMAND_SCREEN	Y
COPP_RELAY_OPEN_TIME	80
CPSTATUS_SWITCHABLE	Y
CBLINK_ALARM_THRESHOLDS	30 60
CUSTOMER_GROUP_IBNGRP_OM_COUNT	512
DATA_COS	0
DEBUG_HUNT_SWERRS	N
DEFAULT_CARRIER_OR_TREAT	C 288
DEFAULT_COMMANDCLASS	0
DEFAULTLANGUAGE	ENGLISH
DISC_TIME_BILLED	Y
DISCTO_TIMEOUT_VALUE	13
DM_PCM_ENCODING	DM_MU_LAW
DTER_AUTO_DEACTIVATION_ENABLE	Y
EA_CCIS6_TANDEM_BILL	N
EA_OCS_AND_DP_OVLP_NEEDED	N
EA_OCS_DIGCOL_METHOD	PXFALL
EA_OVERLAP_CARRIER_SELECTION	Y
EA_WITH_CD	N
EADAS24H_BUFFER_SIZE	7100
EADAS30M_BUFFER_SIZE	32000
EADAS60M_BUFFER_SIZE	7100
EBS_BUZZ_SPLASH_ON	Y
EBS_TO_TRUNK_TRD_TIME	50
ENHANCED_DEAD_SYSTEM_ALARM	Y
EXPIRED_PASSWORD_GRACE	3

-End-

How to Interpret What is Collected

The OMs provide an indication of overflows. If there are insufficient resources for a given office parameter, the OMs indicate this with an overflow peg. Parameter usage should be monitored in all offices, not only those interested in reducing office parameters for the purpose of memory reclamation.

When examining registers FTRQHI and FTRQSEIZ of OM group FTRQ and the FTRQ entities in DMSMON HIGHWATER, it should be noted that these parameters reflect the number of blocks simultaneously in use. The corresponding FTRQ office parameters reflect the number of blocks allocated in multiples of 10. For example, a setting of 300 for office parameter FTRQAGENTS allows for a FTRQAGENTS high watermark of 3,000. This multiple of 10 factor applies only to FTRQ parameters (that is, FTRQAGENTS, FTRQAUDIT, FTRQ0WAREAS, FTRQ2WAREAS, FTRQ4WAREAS, FTRQ8WAREAS, FTRQ16AREAS, FTRQ32WAREAS, FTRQ0WPERMS, FTRQ2WPERMS, FTRQ4WPERMS, FTRQ8WPERMS, FTRQ16PERMS, and FTRQ32PERMS).

The following example shows that FTRQAGENTS is set to 1261 in table OFCENG. This setting allocates 12,610 FTRQAGENT blocks as indicated in field FTRQOM_INFO in the OM group FTRQ. For the sample period, the high watermark, field FTRQHI, indicates a maximum of 6,137 feature queue blocks in simultaneous use.

```
CI:
>TABLE OFCENG : POS FTRQAGENTS
TABLE: OFCENG
FTRQAGENTS 1261
>LIS 10
PARMNAME PARMVAL
FTRQAGENTS 1261
FTRQAUDIT 10
FTRQ0WAREAS 1
FTRQ2WAREAS 1575
FTRQ4WAREAS 799
FTRQ8WAREAS 800
FTRQ16WAREAS 1
FXOGS_REMSY_BITS A_OFF_B_OFF_HK
GLOBAL_CUTOFF_ON_DISCONNECT Y 80 N
GROUND_START_DELAY Y
>OMSHOW FTRQ HOLDING
FTRQ
CLASS: HOLDING
START: 1990/01/12 14:00:00 FRI:
STOP: 1990/01/12 14:15:00
SLOWSAMPLES: 9 :
FASTSAMPLES: 90 :

KEY (FTRQOM_TUPLE_KEY)
INFO (FTRQOM_INFO)
      FTRQSEIZ      FTRQOVFI

FTRQHI
0 FTRQAGENTS
      12610
      369      0      6137

1 FTRQ0WAREAS
      10
      0      0      0
```

2 FTRQ3WAREAS	15750		
	509	0	3394
3 FTRQ4WAREAS	7880		
	238	0	2828
4 FTRQ8WAREAS	8000		
	72	0	30
5 FTRQ16WAREAS	10		
	0	0	0

Referring to the tables in *Example 1* and *Example 2*, the high watermarks can be interpreted. The last 20 days of high watermarks are displayed. For FTRQ4WAREAS, 6,396 is the highest value displayed. For this office, parameter FTRQ4WAREAS in table OFCENG is set to 693. Accounting for the factor of 10, this allows for 6,930 blocks. Operating company personnel may decide to raise this parameter since the high water value is so close to the parameter setting.

For parameter NUMCPWAKE (number of call processing wakeups), 50 is the highest 20-day value. For this office, parameter NUMCPWAKE in table OFCENG is set to 425. Assuming the high day for this event is during the sample period, the operating company may decide to lower the parameter slightly to recover memory, or leave the parameter set as is.

As can be seen in the above two cases, if the value is increased or decreased, office memory is impacted. If a parameter value is increased and made active, more memory is allocated for that resource from spare or not in use pool of office memory. On the other hand, if a parameter value is reduced, made active, and taken through the dump and restore process, office memory is returned to the spare pool of memory. Complete memory reclamation cannot take place without a dump and restore.

How Often to Collect

It is imperative that the operating company monitor the actual usage regularly to account for high day busy hour for each of the critical office parameters and changing calling traffic patterns. Each of these factors should be taken into account to establish the time interval for examining OMs.

High day busy hour for each event must be considered. The high day busy hour for POTS features may be very different than that of Meridian Digital Centrex features. Based on this criterion, usage must be monitored based on the office parameters being analyzed. For example, CFW_EXT_BLOCKS allocate the number of simultaneous active call forwarded calls.

Traffic patterns can change dramatically over time, and therefore, the actual usage could fluctuate dramatically. Actual usage must be monitored on a regular basis to determine if trends are evolving. The decision to collect daily, weekly, or biweekly is the decision of the individual operating company.

How to Make a Decision

Criteria must be chosen to decide whether to lower or raise parameter values. An operating company engineer can choose criteria such as never reducing a given office parameter at all or never reducing an office parameter below three times (or more) the highest ever high watermark.

Lowering office parameter values should be carefully considered. In general, Nortel does not recommend lowering office parameter values unless office memory is in jeopardy.

Factors such as planned large office additions and office history play an important role in deciding how large a buffer to add to the office data. The operating company is responsible for determining how large to make the buffer above the high watermark OMs. It is strongly recommended that the office be monitored for many months before making a decision.

Most operating companies will probably decide never to reduce office parameter values, unless office memory is exhausted.

Office Parameters that are Not Recommended to be Modified

In general, the memory-allocating office parameter values in table OFCENG can be considered for lowering. However, Nortel does not recommend changes to the following parameters. Any changes are made at the operating company's discretion.

- NCCBS defines the number of Call Condense Blocks (CCB) required that are held up through the life of a call. NCCBS is provisioned to provide for 100% use of network facilities. No change is recommended.
- NUMCALLPROCESSES defines the number of Call Processes (CP) required that are associated with a call during set up, take down, and feature processing. The current formula is sufficient to provide for high calling volumes. No change is recommended.
- NUMCLETTERS defines the number of call processing letters required that are used to pass messages between call processes and the rest of the DMS-100 switch. NUMCLETTERS is set at 2,000 to provide for overload protection during peak traffic periods. No change is recommended.
- NUMTLBS defines the number of Terminal Linkage Blocks (TLB) used in the input/output system. NUMTLBS is provisioned based on the number of hardware nodes present in the office. No change is recommended.
- PPMBUFFS defines the number of Peripheral Process Message (PPM) buffers used for sending messages to the peripheral modules. If PPMBUFFS is underprovisioned, switch degradations can occur. A margin of safety is built in to prevent degradation during high-traffic periods and unexpected high maintenance situations. No change is recommended.

Reducing Office Parameter Values

The preferred method of implementing office parameter reductions is to gradually make changes in the existing office parameter tables, performing the necessary restarts as required during very low-traffic times. Changing two or so parameter values downward at a time, then verifying that the changes had no adverse effect is the safest way to implement reductions. Possible problem variables are kept to a minimum and a known safe fallback is available. If troubles do arise, reverting back to the old values can be done quickly. The OMs should be monitored closely to ensure proper engineering. All changes should be made at least three weeks prior to the dump and restore or One Night Process (ONP). At least three weeks is required to allow the software delivery process to capture the new values.

Memory is not reclaimed until the dump and restore is performed. At that time, the reduced values are copied from the existing load into the new office load.

If parameter reductions are required, the operating company should communicate their intentions and work with the Nortel regional software systems engineering manager.

Increasing Office Parameter Values

Increasing parameter values is a safer process than reducing them. The major issue with increasing parameter values (other than timing related parameters) is the increased memory requirements. Unlike reducing parameter values, memory is utilized immediately upon activation (usually a cold restart). Often, parameters in table OFCENG require more memory when increased. The memory requirements for parameters are in the data store area for NT40 loads, but in total office memory for SuperNode loads, where there is no distinction between data and program store.

A basic outline of when values should be increased follows:

1. Determine actual spare memory available in the switch.
2. Determine the established memory requirements indicated by the required parameter value increases.
3. Analyze and determine if the amount of increased memory does not exceed the amount of memory spare and available for use. Keep in mind the Nortel and individual operating company requirements for spare memory overheads. Reference "SEB 88-01-002" or contact a Nortel regional software systems engineering manager to aid in this task. After a determination has been made that the increased values will not exceed memory limitations including spare or overhead requirements, a safe implementation process can begin.
4. If only two or three parameter values are to be increased, all could be done at the same time, with the monitoring of parameters and memory after the change. If larger numbers of parameters values need to be increased, a staged increase should be implemented. Monitor two or three parameter changes and if all is well and memory usage is safe, move forward with others.

Notifying Nortel

To ensure propagation to future software releases of decreases made to office parameters, the operating company must contact their regional software systems engineering manager with a single point of contact at the operating company. The contact should be able to approve of any changes to the office parameters for a given office.

Nortel engineers office parameters based on operating company input and standard formulas. A wide variety of applications are covered by the standard formulas. These formulas yield a safe value in nearly every office. The operating company should monitor the office parameter usage on an ongoing basis to determine if the parameter settings are appropriate for the office application.

Any changes made to the office parameters discussed in this document result in a change in the memory allocated in the switch. An increase in a setting requires more memory. A decrease in value decreases memory requirements. A decrease in a parameter value only yields an actual memory decrease if a rebuild (that is, a dump and restore) occurs.

Nortel DMS-100 CDN SERVORD Command

Description

The CDN command changes Directory Numbers (DN).

Applicability

The CDN command is used on:

- One individual line.
- A Meridian business set.
- An ISDN set.
- All hunt group DNs, excluding the pilot DN.
- A remote call forwarding.
- Teen service Primary DNs (PDN), but not teen service Secondary DNs (SDN)

Example

The following is an example of the CDN command. This example changes the DN of an existing individual line from 621-5123 to 621-4040.

Example of the CDN Command in Prompt Mode, Different 7-digit DN

```
SO:
>CDN
SONUMBER: NOW 98 2 7 PM
>
OLD_DN:
>6215123
NEW_DN:
>6214040
INTERCEPT_NAME:
>OPRT
COMMAND AS ENTERED:
CDN NOW 98 2 7 PM 6215123 6214040 OPRT
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>Y
```

Example of the CDN Command in No-Prompt Mode, Different 7-digit DN

```
SO:
>CDN $ 6215123 6214040 OPRT
COMMAND AS ENTERED:
CDN NOW 98 2 7 PM 6215123 6214040 OPRT
ENTER Y TO CONFIRM, N TO REJECT, OR E TO EDIT
>Y
```

Example of the CDN Command in Prompt Mode, 10-digit DN

```
SO:
>CDN
SONUMBER: NOW 98 2 7 PM
>
OLD_DN:
>9196215123
NEW_DN:
>9196214040
INTERCEPT_NAME:
>OPRT
COMMAND AS ENTERED:
CDN NOW 98 2 7 PM 9196215123 9196214040 OPRT
ENTER Y TO CONFIRM, N TO REJECT, OR E TO EDIT
>Y
```

Example of the CDN Command in No-Prompt Mode, 10-digit DN

```
SO:
>CDN $ 9196215123 9196214040 OPRT
COMMAND AS ENTERED:
CDN NOW 98 2 7 PM 9196215123 9196214040 OPRT
ENTER Y TO CONFIRM, N TO REJECT, OR E TO EDIT
>Y
```

Example of the CDN Command in Prompt Mode, Same 7-digit DNs

```
SO:
>CDN
SONUMBER: NOW 98 2 7 PM
>
OLD_DN:
>6215123
This Local DN is not Unique.
Please Use the Full National DN.
6215123
*** Error ***
TYPE OF MEM_DN IS SO_DR
PLEASE ENTER
OLD_DN:
>9196215123
NEW_DN:
>9196214040
INTERCEPT_NAME:
>OPRT
COMMAND AS ENTERED:
CDN NOW 98 2 7 PM 9196215123 9196214040 OPRT
ENTER Y TO CONFIRM, N TO REJECT, OR E TO EDIT
>Y
```

Prompts

The system prompts for the CDN command are shown in the following table:

 Input Prompts for the CDN Command

Prompt	Valid input	Explanation
SONUMBER	An entry in the format: abnnnnnc yy mm dd {AM} {PM} Where: * a = Obligatory Alphabetical Character (A-Z) * b = Optional Alphabetical Character (A-Z) * nnnnn = 5 Obligatory Numerical Characters * c = Optional Alphabetical Character (A-Z) * yy = Year (00-99) * mm = Month (1-12) * dd = Day (1-31)	The unique number of the service order to be entered. Date the service order is to be processed.
OLD_DN	Seven or ten digits. Refer to the "Notes" section that follows this table for information on mandatory 10-digit input.	Enter the DN being replaced by a new DN in a CDN service order.
NEW_DN	Seven or ten digits. Refer to the "Notes" section that follows this table for information on mandatory 10-digit input.	Enter the new DN that replaces the previous DN.
INTERCEPT_ NAME	AINT = Attendant Intercept (IBN lines only) ANCT = Machine Intercept BLDN = Blank DN CANN = Customer Announcement (IBN lines only) OPRT = Operator Intercept PODN = Ported-Out DN UNDN = Undefined DN	Enter the type of intercept. If the DN is unknown, enter BLDN. Office parameter SO_CICP_OFRT_ICP_ALLOWED in table OFCOPT lets you toggle between OPRT and BLDN intercepts. Refer to the "Notes" section that follows this table. PODN is an line portability treatment that designates a ported-out DN.

 -End-

Notes

The following notes apply to the CDN command:

- Use the CDN command to change the DN of a Directory Number Hunt (DNH) group member.
- The CDN command cannot change the pilot number of a hunt group. To change the pilot of a hunt group, remove the hunt group with the `DEL` and `OUT` commands.
- The CDN command:
 - ◆ Does not add options.
 - ◆ Does not delete options.
 - ◆ Does not change a Line Equipment Number (LEN).
 - ◆ Does not change a Line Class Code (LCC).
 - ◆ Does not change a Line Treatment Group (LTG).
 - ◆ Does not change the ringing code.
- The last seven digits of the new DN must not be the same as the last seven digits of the old DN. The system generates an error message if the DN digits are the same.
- If the operating company enters a seven-digit DN and the office code exists in multiple Service Numbering Planning Areas (SNPA – area codes), the system displays an error message. A reprompt occurs.
- With NA010 and up, the CDN command is no longer blocked by `SERVORD` for `MADN CACH`. `KSETLINE` table control performs the changes for a `MADN CACH` group and the underlying data for all members of the `CACH` group.

Spread Spectrum Surveillance Bug



Spread Spectrum (SS) audio surveillance transmitters are used to prevent the accidental, or intentional, reception of the RF signal by an external party. They offer fairly strong protection from small-time listeners (ham radio/scanner operators) and even protection from some of the "lesser-informed" Technical Surveillance Counter Measures (TSCM) sweepers. Anyone with a good spectrum analyzer (or a good physical sweep) will be able to track this transmitter down.

The best part about this particular transmitter is – there is nothing to build! Direct Sequence (DS) and Frequency Hopping (FH) spread spectrum audio transmitters can be bought at your local consumer electronics store in the form of "high-security" cordless phones. You can even pick these phones up at thrift stores and rummage sales for only a few dollars. People will often throw away the entire phone when the rechargeable battery pack dies. I've picked up a few of these phones, and *every single one* worked when powered from a new battery or external DC power supply.

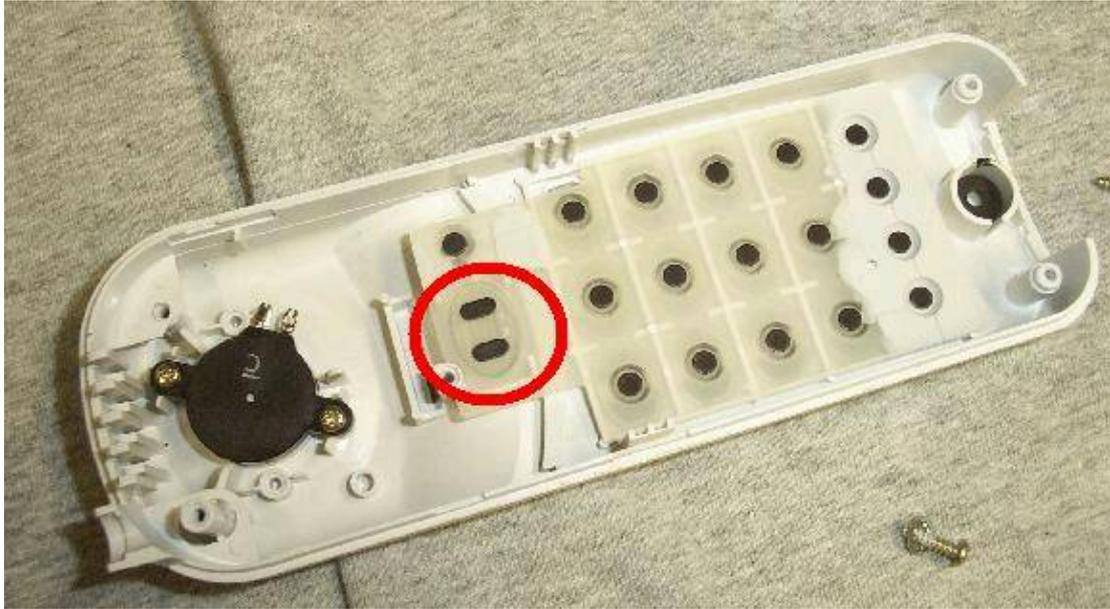
The cordless phone used in this project is a GE Model No. 2-911SSTA, labeled: "Digital 900 MHz Spread Spectrum Cordless Phone", and the FCC ID is G9H2-910SST. The base transceiver requires +9 VDC at around 600 mA and the handset needs +3.6 VDC / 200 mA. The handset transmit frequency is centered around 926 MHz and is about 4 MHz wide.



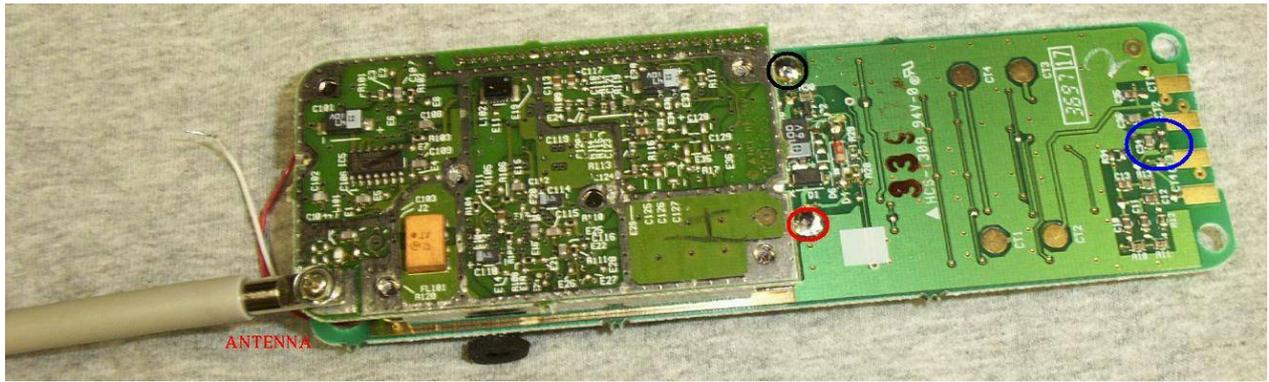
Tools you'll need. Clockwise from the upper left, a length of 3/8-inch I.D. flexible tubing, a RJ-11 phone jack which terminates with a set of alligator clips, the spread spectrum cordless phone, and a "Radio Shack Mini-Amplifier / Speaker", part number 277-1008C. You'll also need some sort of adapter to connect the RJ-11/alligator clips to the mini-amplifier, if you don't want to take the amplifier apart.



Inside view of the cordless phone's handset. This will become the actual "bug." The plastic case, keypad, speaker, and battery can be removed.



Make a note of the **"Talk"** button on the keypad. You'll need to solder jumpers across the circuit board pads for this key to permanently place the handset into "transmit" mode.

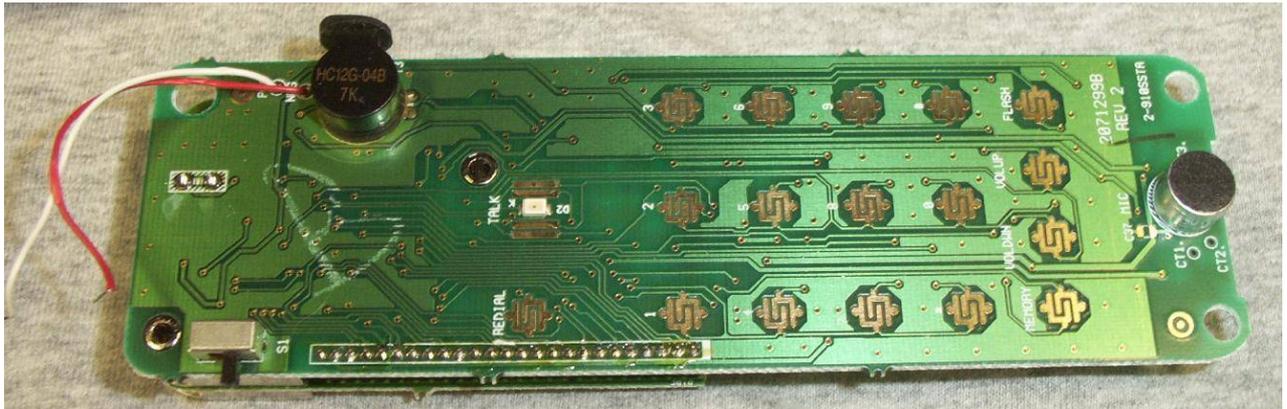


Closeup internal view of the handset. The antenna/RF section is on the left. The **RED** circle indicates the **POSITIVE** (+3.6 VDC) connection for the battery, the **BLUE** circle indicates the **NEGATIVE** or **GROUND** connection for the battery. The **BLACK** circle is the solder connection for the handset's internal electret microphone. You may want to replace the phone's original electret mic with one that has better sensitivity and signal-to-noise ratio, but that's optional.

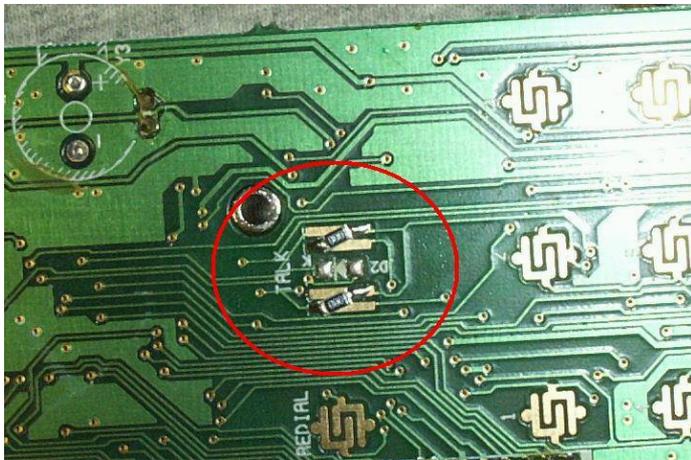
Also, some cordless phones utilize "noise-cancelling" microphones. These should be replaced as they don't offer the best sensitivity for surveillance purposes.



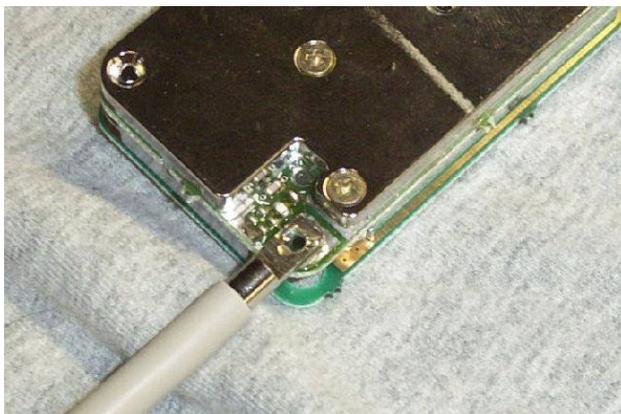
Alternate view of the above connections.



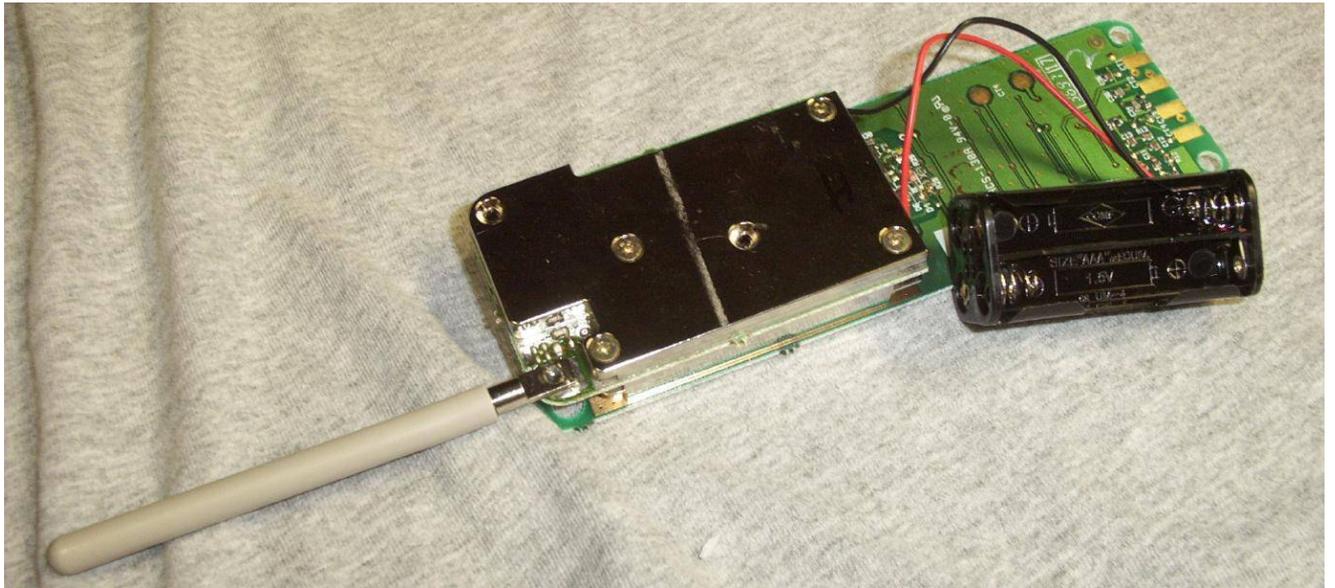
Closeup view of the keypad side of the handset's circuit board. The speaker has been removed. The black plastic thing on the left is the handset's ringer/buzzer. The handset's electret microphone is mounted on the right. Note the circuit pads marked **"Talk"**. That is a surface-mount LED between them.



Closeup view of two zero-ohm resistors installed across the exposed pads of the **"Talk"** button. Most phone's will be different, but the overall theory should be the same. This forces the handset into "continuous transmit" mode the instant it powers up. The surface-mount LED and the ringer/buzzer have also been removed.



The handset is put back together. The antenna has been soldered to its circuit pad instead of using hardware. This actually increases the output RF power slightly as the electrical connection is much better.



The completed surveillance bug. The DC power supply comes from four "AAA"-size batteries. You should use NiCad rechargeable batteries as these only output 1.2 Volts each (+4.8 VDC total). The use of regular alkaline batteries will require the use of some type of voltage regulator to reduce the input voltage to under +5 Volts.

As soon as the batteries are put in, this bug will start transmitting. Be sure the cordless phone base station is powered and ready (and in radio line-of-sight) so the handset can "sync" its signal, otherwise the handset will require a complete power-down (removal of the batteries), and this could be difficult in covert operations.



This is what the tubing is used for. When you don't want, or can't, extend the wires of the electret microphone, just place a piece of tubing over the mic and run the tubing to the location which needs to be monitored. The tubing can be run a considerable distance with no degradation of audio quality. Be careful not to break the microphone leads though.

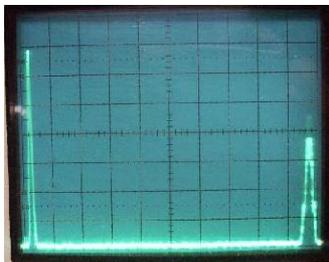
Placing your transmitter/microphone at the end of a length of tubing is also a good way to defeat some metal detectors and non-linear junction detectors during a TSCM sweep.



Base station "listening post" setup. Not really much is needed. Power the base station off the phone's standard wall-wart power supply. Instead of connecting the base station to the phone line, connect the output of the RJ-11 jack (via the alligator clips / adapter) to the mini-amplifier. You can also use a tape recorder in place of the amplifier, or even a lineman's handset. Polarity of the audio coupling should not matter.

If the base station needs to see phone line "off-hook voltage" before it starts to transmit, connect a +9 Volt battery to the tip & ring of the RJ-11 connection and take the audio off the line via a 0.1 μ F DC blocking capacitor.

See *GBPPR 'Zine* issue #7 for more information on a high-performance 900 MHz receiving setup.



GBPPR Spectrum Analyzer view of the RF output. A conventional narrowband FM transmitter at 845 MHz is shown on the left, the direct sequence spread spectrum signal (at approximately 926 MHz) is on the right.

Schematics for the GBPPR Spectrum Analyzer are available at:
<http://www.gbppr.org/spec/index.html>

Notes

The following was from a post on the "TSCM-L" list maintained by James M. Atkinson:
<http://www.tscm.com>

To: TSCM-L@tscm.com
From: "James M. Atkinson, Comm-Eng" <jmatk@tscm.com>
Subject: Spread Spectrum Update

Several weeks ago I had a chance to examine a number of spread spectrum microwave bugging devices.

Since that time I've conducted some analysis and gathered further intelligence on the circuit.

Here are a few of my observations.

=====
C O N F I D E N T I A L
=====

1) Most of the products use a high bandwidth QPSK/BPSK modulator, multi channel audio CODEC, and a RISC micro-controller chip (all components are either surface mounted ICs or multiple dice potted in epoxy).

2) RF Circuit seems to be a simple homodyne audio transmitter (6 Ghz Gilbert Cell Mixer) which is driven by a single CPU/microcontroller (with a clock speed of 180 Mhz).

3) Frequencies used for the ultra low power device are clean from 130 Mhz to 4 Ghz, circuit starts to fail above 5.5 Ghz (but is still operable to about 8 Ghz).

4) Emitter is driven directly from vector modulator chip, with no power amp circuits. PIN diode found on output appears to provide gain control or disconnect of circuit, but provides no amplification of signal.

5) Noise floor of circuit is -135 dBm (below 2 ghz), -142 dBm (2-4 ghz), and -150 dBm above 4 Ghz.

6) Signal has a variable bandwidth which varies between 350 Mhz and 900 Mhz. Appears to be designed for a 900 Mhz bandwidth signal. Device operates "deep" inside the noise floor.

7) Virtually impossible to detect at close range with a conventional RF spectrum analyzer (492/494/8566/etc).

8) Detectable with most wideband systems (with IF BW above 300 - 900 Mhz, 700 Mhz ideal).

8) VCC = +3.0 VDC, all circuits functional 2.3 to 6.8 VDC

9) Output applied to PIN diode ranges between -28 and -42 dBm (depending on frequency and span)

10) Device enters some type of sleep mode when power is present but audio level is low (seems to auto squelch). Total current draw when in sleep mode is 12 μ A. Device does not emit RF energy when in sleep mode.

11) One of the devices has no type of connection for external power, but instead uses a network of

Schottky diodes and capacitors which constitute an effective RF to DC converter.

12) The RF to DC circuit requires an un-modulated 10-15 Ghz RF signal, and seems to respond well to X-Band microwave motion detectors used for many corporate alarm systems.

13) Device also has a small microphone built onto the circuit, microphone measures 4.5mm * 1.6mm * 4.1mm.

14) Entire device measured 3.2 cm * 5.2 cm and about 3 mm thick (or about the thickness of a standard business envelope).

15) Device contains some type of adhesive on both sides of a foil backing. Suspect it's applied as some type of "sticky label". Once the device is installed any attempt to remove results in its total destruction (unless you freeze it off).

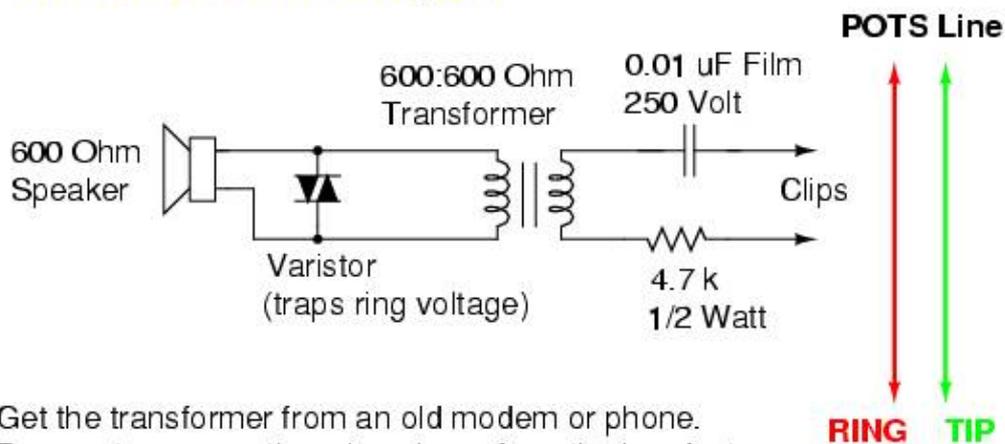
16) The French government has been know to use a similar device in some of its "Diplomatic" activities.

-jma

POTS Audio Interceptor

Modify a Bell 2500-type telephone handset into an audio monitor for the base station listening post or for monitoring an analog phone line. The audio level will be quite low, but useable. The transformer/capacitor/resistor help isolate the line to reduce any induced noise.

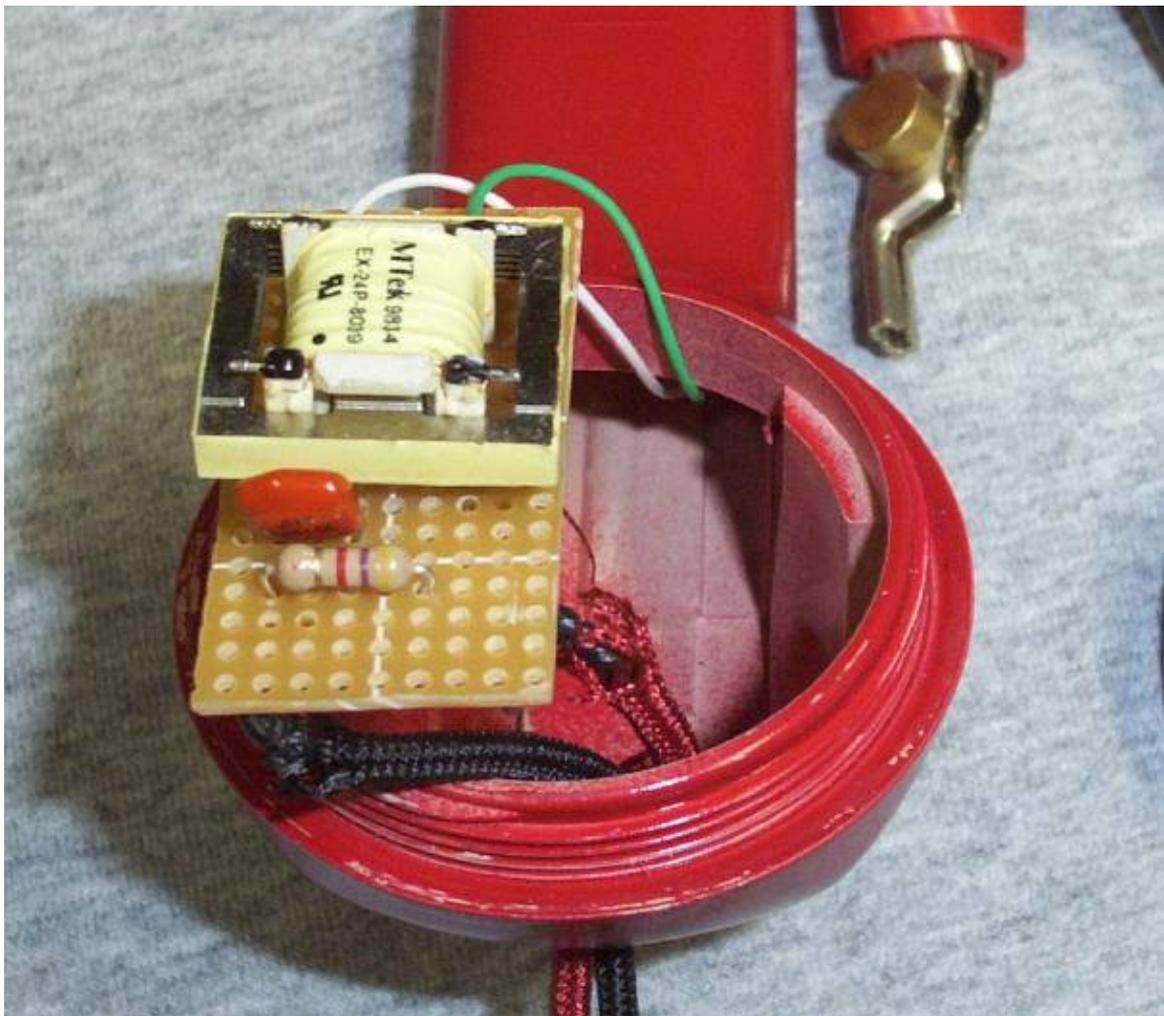
POTS Audio Interceptor



1. Get the transformer from an old modem or phone.
2. Be sure to remove the microphone from the handset.
3. Be sure to leave the varistor across the speaker.
4. Hook-up is not polarity sensitive.
5. When connecting to an "active" line, bridge the gap between the line and your alligator clip with your finger, then slide the clip to the line along your finger. This helps remove the "click".



Picture of the POTS Audio Interceptor. The coupling transformer is from an old modem.



Closeup view.

"Shotgun" Directional Microphone

Introduction

The multitube "shotgun" directional microphone, as seen in some movies, may just be one of the biggest hoaxes of all time. The physics which originally created it for a *Popular Electronics* article back in 1964 revolved around one living in an ideal, perfect world. Many of the thousands of people who ran out to build one of these microphones were often disappointed in its performance. Sorry, but simple, non-contact audio microphones can't hear through walls or intercept those whispers from a mile away (well, they can – but that's another story). Shotgun directional microphones only reduce the "receiving range" in which the microphone is pointed, *they don't offer any gain!* A fresh set of ears will often beat many fancy directional microphone designs...

But with today's modern electrical components, it is possible to overcome some of the performance obstacles inherent in its design. This article will be a detailed overview of the assembly and construction of a shotgun mic, and then following this article will be the scanned version of the original 1964 *Popular Electronics* article. The *Poptronics* article goes into much more detail on the actual hardware construction and theory, so you may wish to review that first. Also included is a scan of a page in the book *The Basement Buggers Bible*, one of the best homebrew surveillance books out there. This particular page has more info on the microphone and a schematic for a higher-performance audio amplifier than what was used in the original *Popular Electronics* article.

Overview



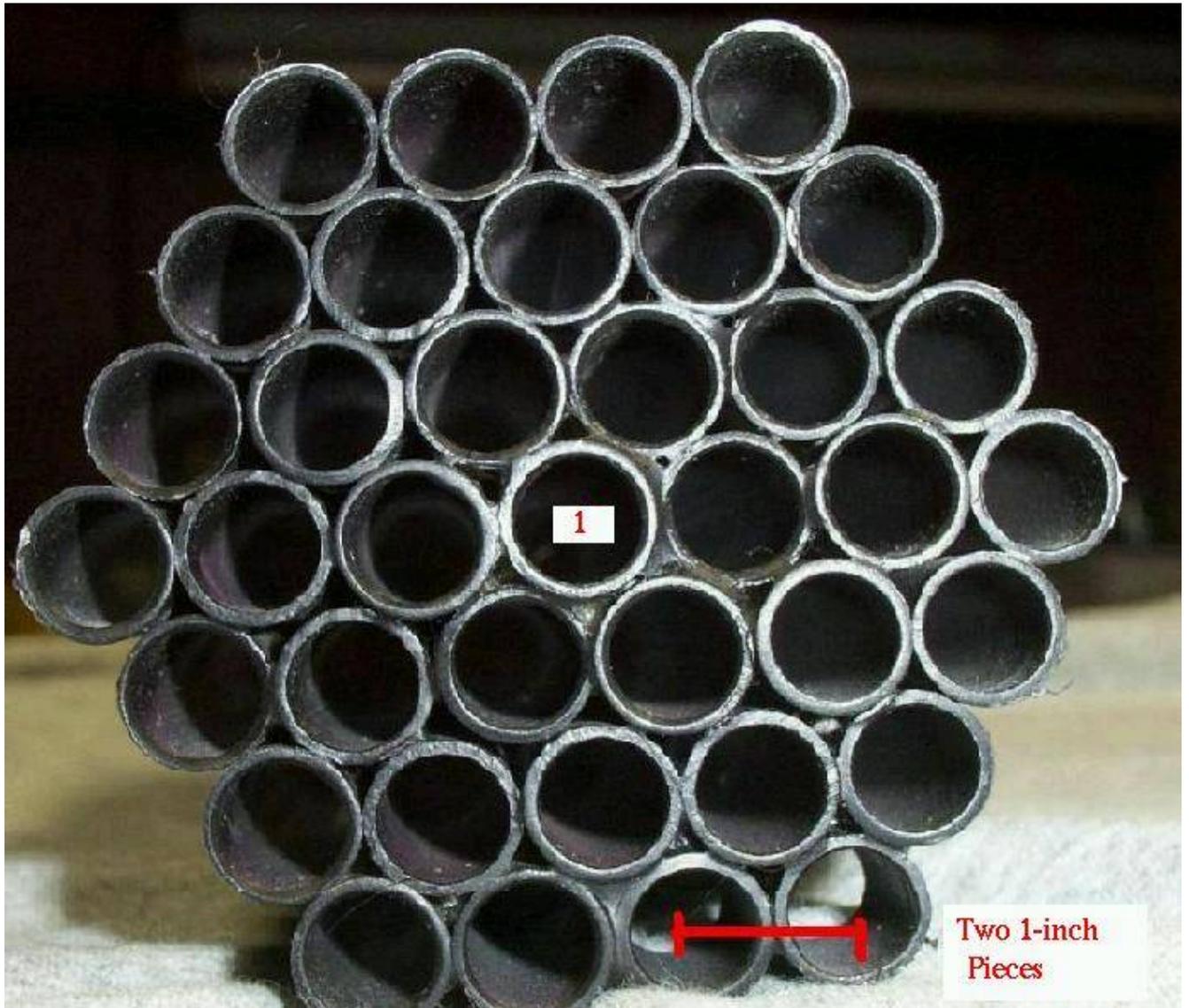
Start with about sixty feet of 1/2-inch O.D. aluminium tubing. The original article used 3/8-inch diameter tubing, but 1/2-inch seems to be much easier to find at the hardware store. Also pick up some two-part, fast-drying epoxy, and a *good* tubing cutter. Copper tubing can be used in a pinch.



Start cutting the tubing per the *Popular Electronics* article. Cut one 36-inch piece, one 35-inch piece, one 34-inch piece, one 33-inch piece, etc. until you get down to 1-inch. You'll need two of those. Deburr the fresh cut ends with a file and clean the tubing with steel wool and denatured alcohol to prepare the aluminium for the epoxy.



Starting with the 36-inch piece, apply some epoxy and surround this tube with the other pieces, going down in length (i.e. 35-inch, 34-inch, etc.). The tubing must be *very clean* for the epoxy to stick. Aluminium will oxidize quickly after being cleaned.



When finished, it will look something like this. The construction doesn't make any sense at first, but it will work out, provided you cut all the pieces to the right length. Notice how it looks like three rings around the original 36-inch tube. Remember that it needs *two* 1-inch pieces to finish off the sides, also be sure the tubing ends are all properly aligned!



Another (somewhat) finished view. I cleaned the aluminium tubing with a little bit of lye and hot water (**DANGER!** – *Doing that can give you an ouchy if you have the I.Q. of a \$2600 subscriber*) then I spray painted it with a zinc-chromate primer. Next, I sprayed almost a whole can of black Plasti-Dip spray-on plastic coating on the outside of the tubing. This was done to hopefully help in the reduction of accidental noise vibration pick-up while the microphone is in operation – I think it worked a little bit.



View of the mounting block. It's just a scrap piece of aluminium, with a 1/4-inch (20 TPI) tapped hole, epoxied to the approximate middle of the shotgun mic. This can be used for mounting the microphone tubes to a camera tripod.



Another overall view.



Full view of the shotgun microphone tubes.



These are the components which will be needed to make the "funnel" for the audio amplifier which will attach to the back of the microphone tubes. Clockwise from the the upper left is a PVC 3–inch to 2–inch reducing coupler, a plug–in thingy to add threads to the reducing coupler, and the matching threaded coupler for that part. Next, is some rope caulk, and finally, a high–output piezoelectric microphone element, Mouser (<http://www.mouser.com>) part number 25LM024. I'm kinda guessing at this point, so if you can think of something better for your own design, use it.

All the PVC parts are painted with a copper "flake" paint to help in the attenuation of any electromagnetic interference.



Use the rope caulk to mount the piezoelectric microphone element inside the threaded plug-in. Secure it from both the front and the back.



Alternate view of the microphone element inside the threaded plug-in.



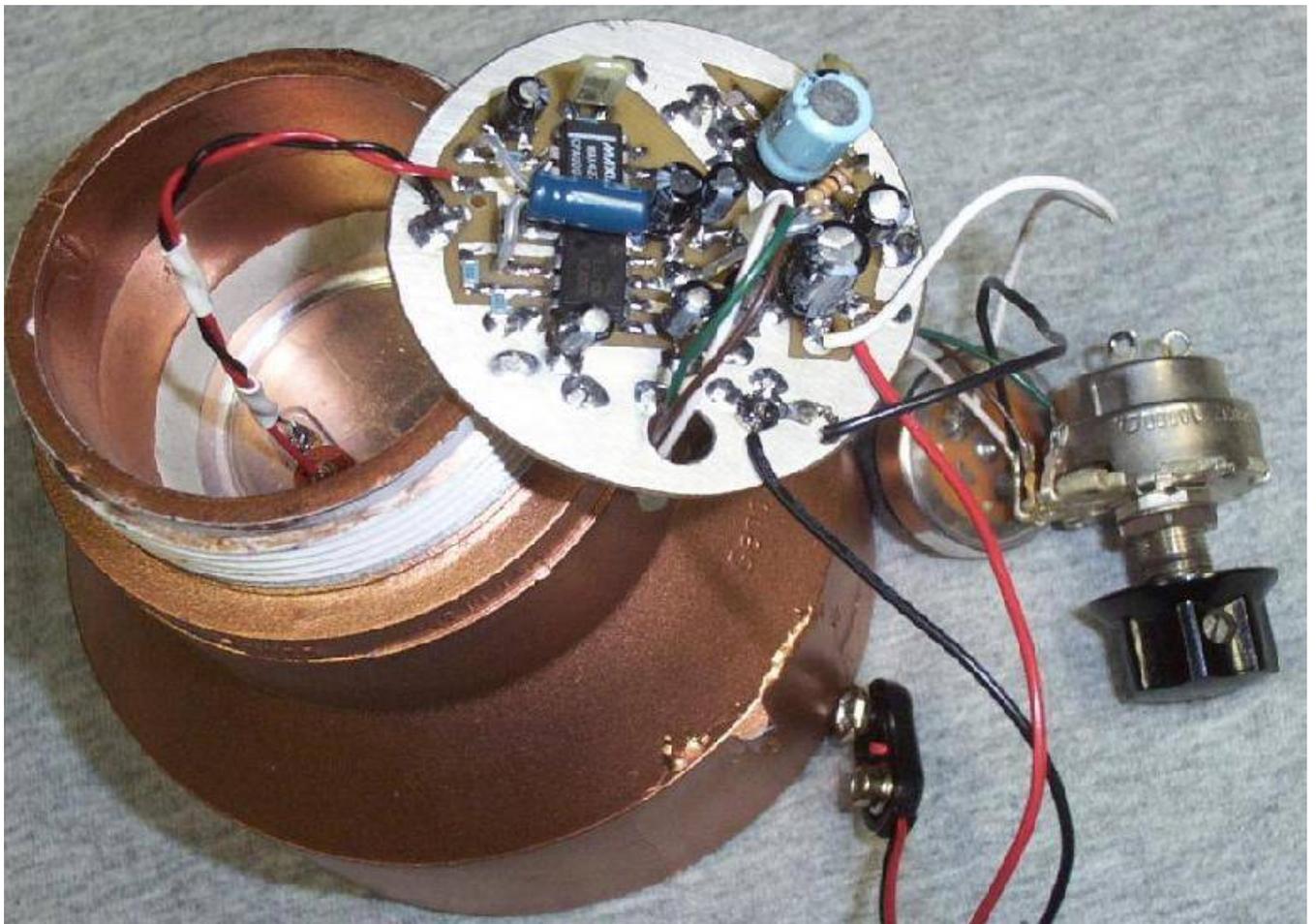
Rear view of the microphone element inside the threaded plug-in. The isolated (red) pad is the microphone's **POSITIVE** terminal, the other tab is **CASE GROUND**.



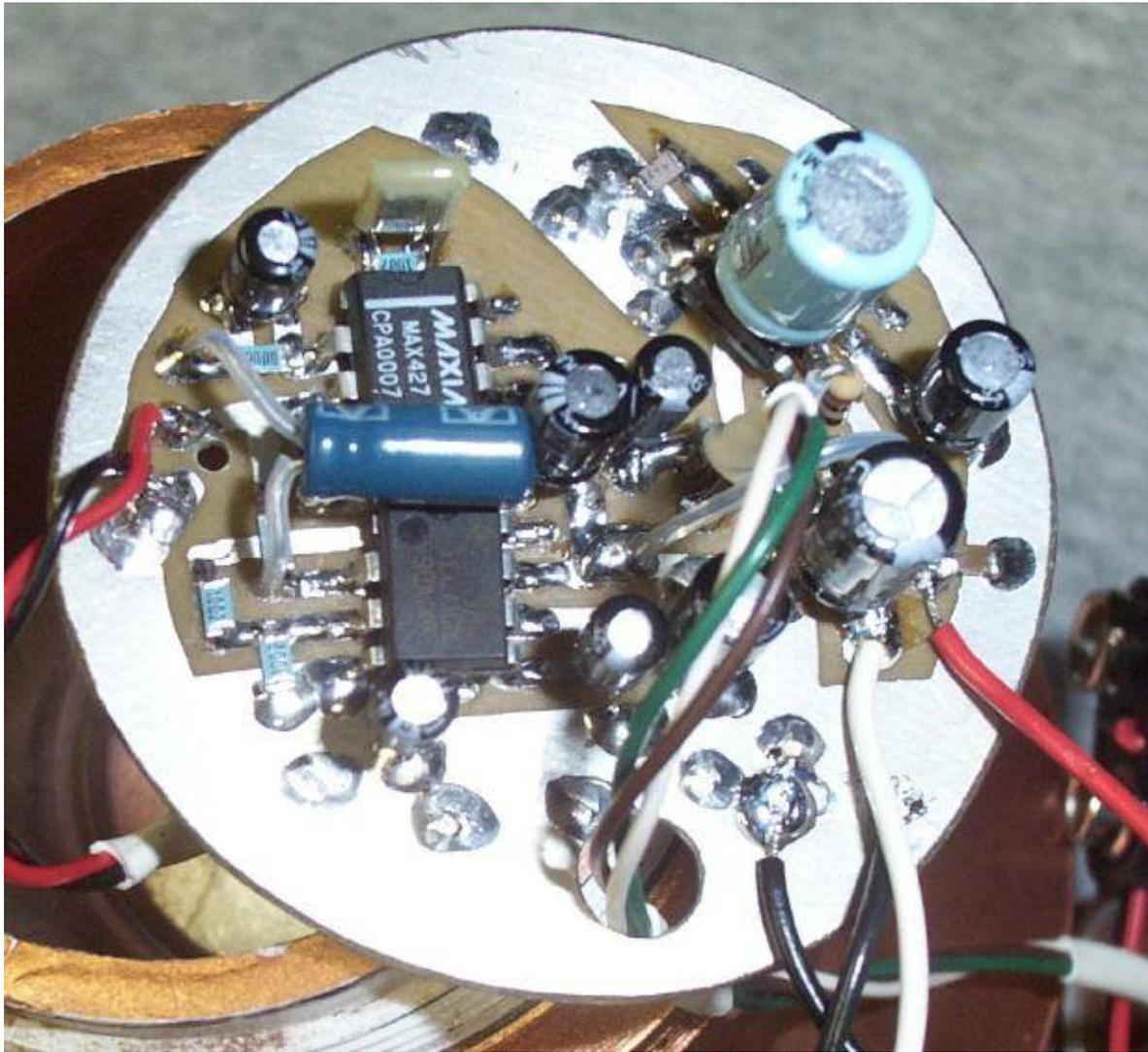
Then slide the threaded plug-in into the 3-inch to 2-inch reducing coupler. It should look something like the picture.



This is how the PVC parts should look when connected.

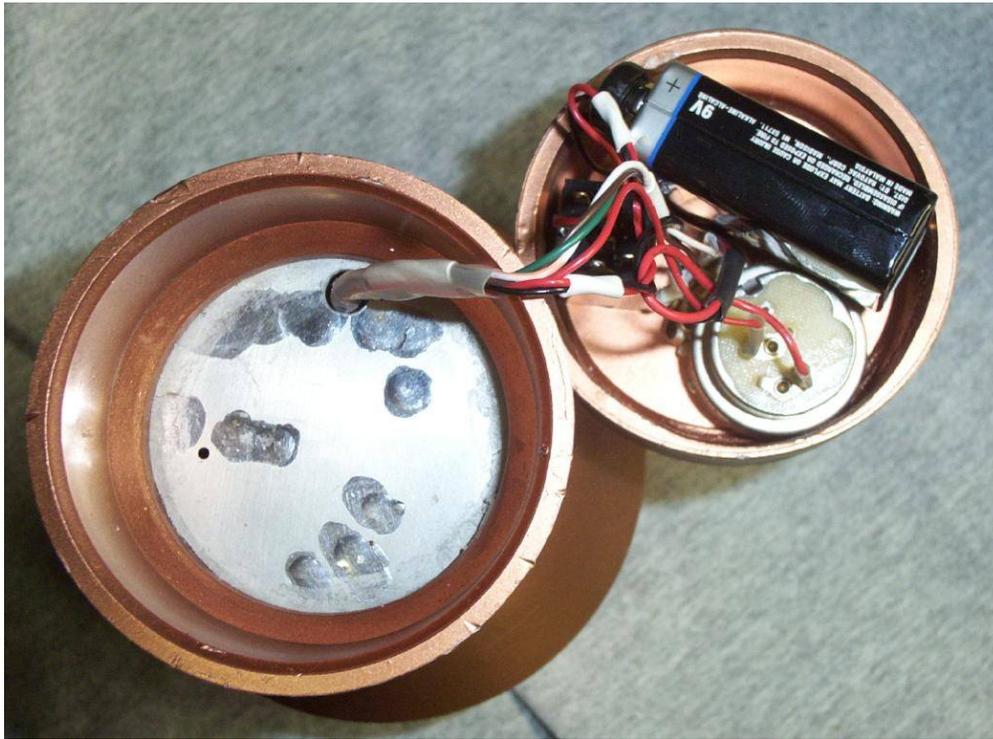


Audio amplifier circuit board. Test setup.

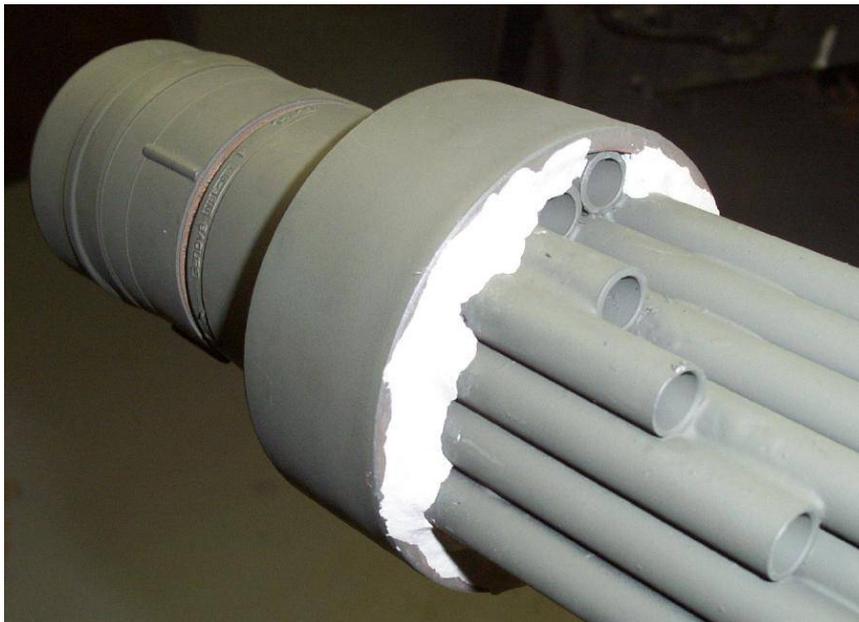


Closeup picture of the audio amplifier circuit board. A combination of both surface mount and leaded components are used to reduce space. The red/black leads on the left are for the microphone element. The white/green/brown wire bundle is for the volume control potentiometer. The white/black leads out the bottom are for the speaker and the red/black leads are connected to a 9 Volt battery.

Try to use 1% metal-film resistors, as they offer the lowest noise. Electrolytic capacitors should be of high quality. Digi-Key carries a good Panasonic line. Low value capacitors should be of polystyrene or polypropylene dielectric material. Keep the areas around the feedback resistor/capacitor in the MAX427 clear of any solder flux.



Picture of the audio amplifier board mounted between the threaded PVC adapters. The PVC end cap contains the volume control potentiometer with an integrated on/off switch. The audio output is via a 1/4–inch mono headphone jack. The end cap is taped to the other PVC pieces.



The funnel is fitted to the microphone tubes. You may have to grid the PVC reducing coupler with a Dremel tool for it to fit the tubing. Then pound the coupler onto the tubes with a rubber mallet. It should be a tight fit. Seal the funnel with rope caulk.



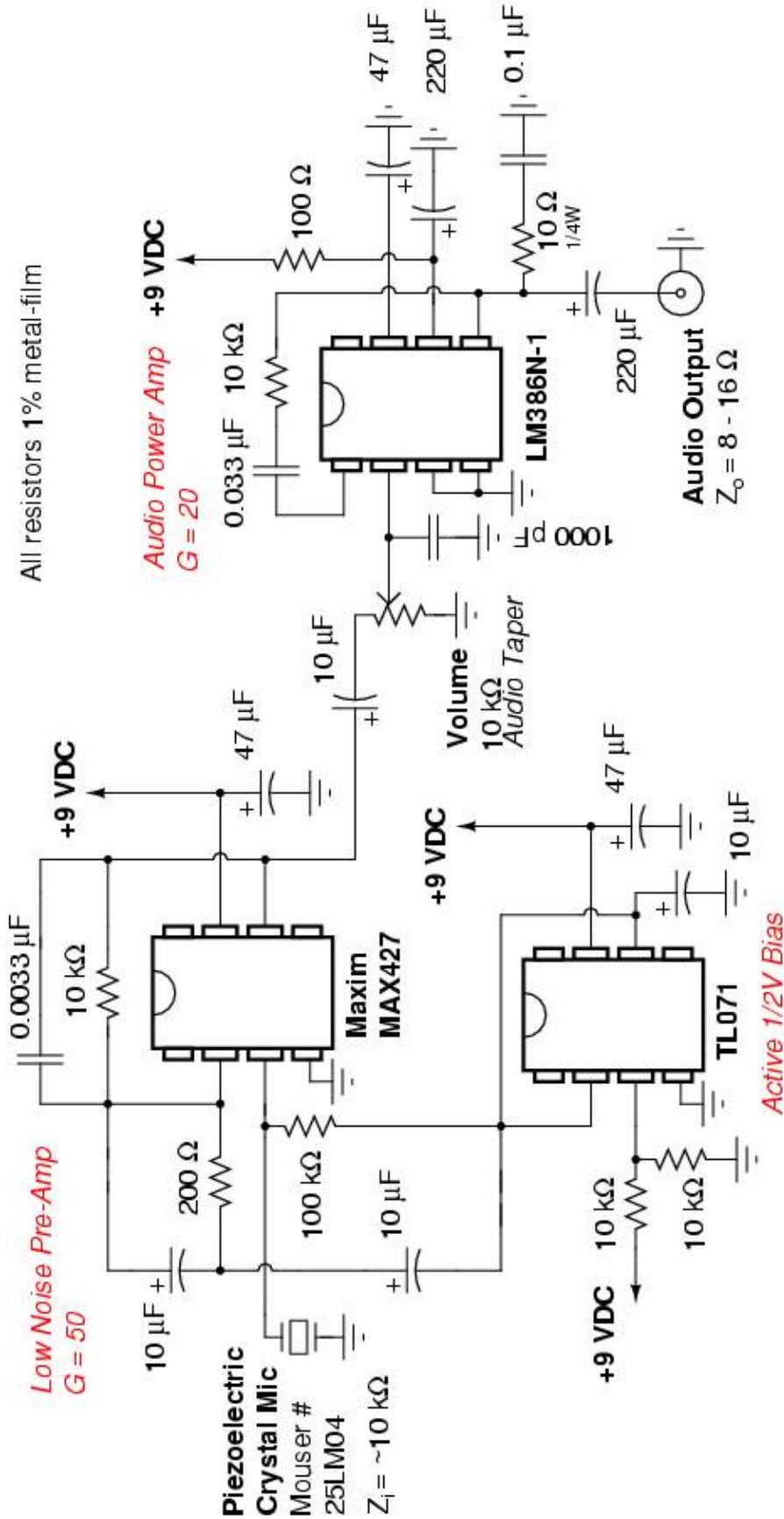
Finished microphone. Apply a coat of olive drab paint or some other form of camouflage. It works pretty well, but don't expect any miracles. The audio is quite "tinny" due to the microphone element's poor bass response. Use an external equalizer to correct this. Increase the value of the 10k resistor in the MAX427's feedback to increase the overall amplifier gain.

Low Noise Microphone Amplifier PCB Pattern

Etch on an approximate 2-inch diameter board. Use good FR-4 laminate. Tin, and wash away any left over solder flux.



"Shotgun" Directional Microphone Audio Amplifier



"Shotgun" Directional Microphone

From *Popular Electronics*, June 1964

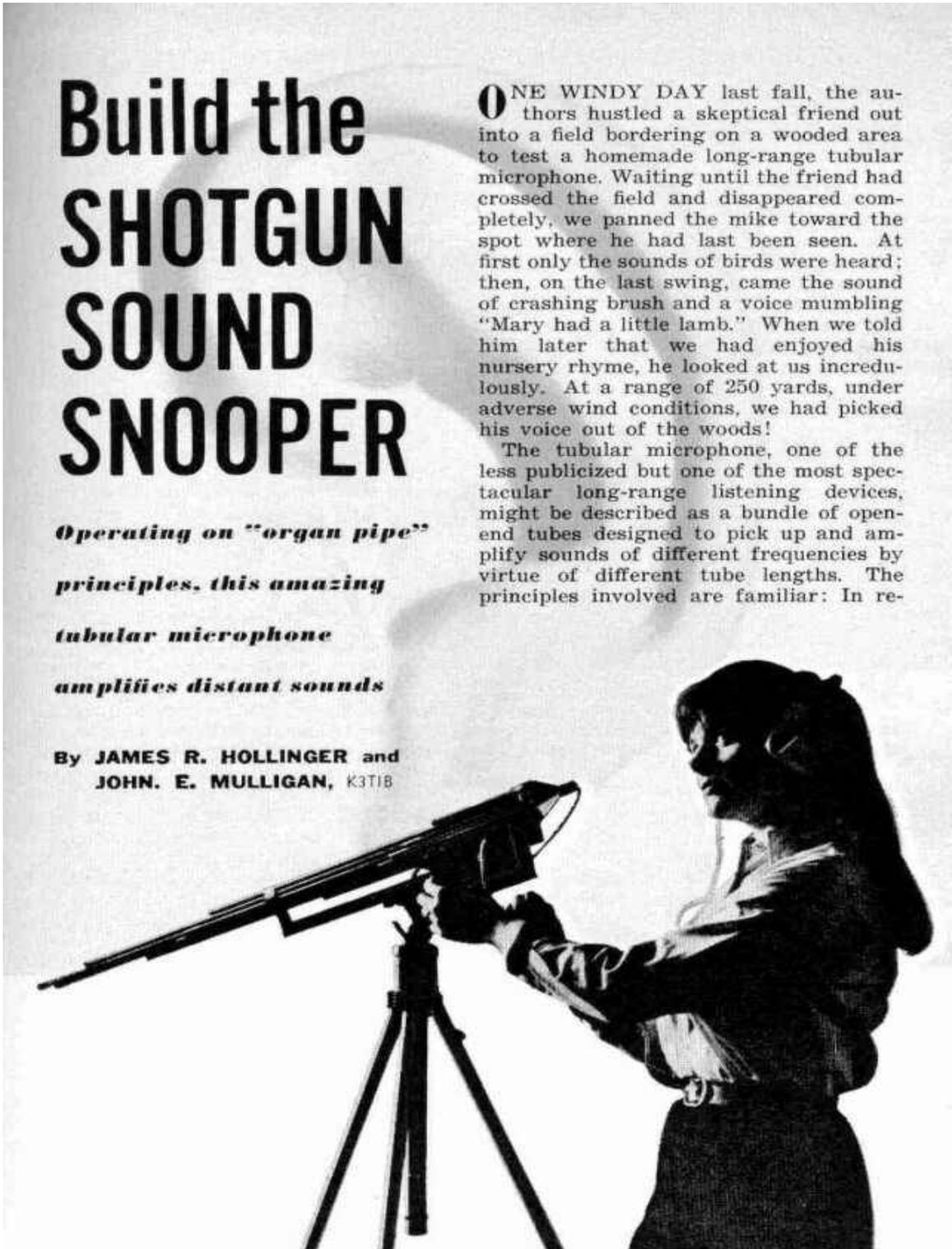
Build the SHOTGUN SOUND SNOOPER

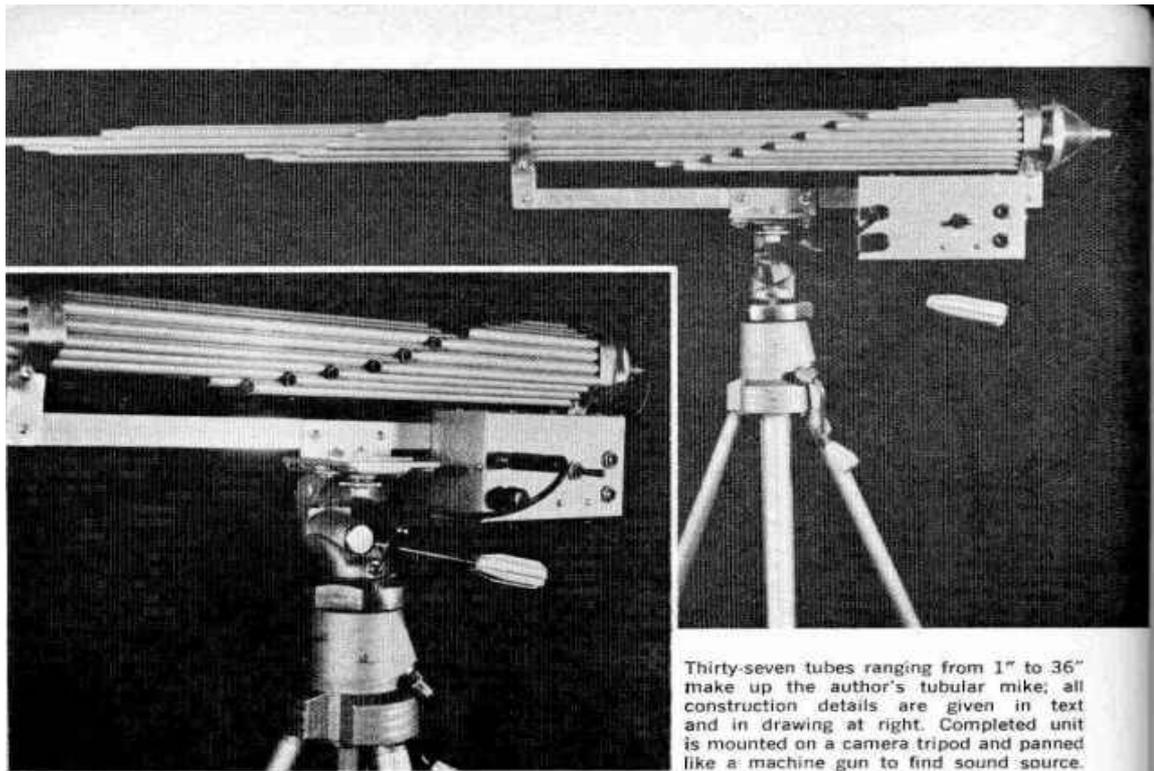
Operating on "organ pipe" principles, this amazing tubular microphone amplifies distant sounds

By **JAMES R. HOLLINGER** and
JOHN. E. MULLIGAN, K3TIB

ONE WINDY DAY last fall, the authors hustled a skeptical friend out into a field bordering on a wooded area to test a homemade long-range tubular microphone. Waiting until the friend had crossed the field and disappeared completely, we panned the mike toward the spot where he had last been seen. At first only the sounds of birds were heard; then, on the last swing, came the sound of crashing brush and a voice mumbling "Mary had a little lamb." When we told him later that we had enjoyed his nursery rhyme, he looked at us incredulously. At a range of 250 yards, under adverse wind conditions, we had picked his voice out of the woods!

The tubular microphone, one of the less publicized but one of the most spectacular long-range listening devices, might be described as a bundle of open-end tubes designed to pick up and amplify sounds of different frequencies by virtue of different tube lengths. The principles involved are familiar: In re-





Thirty-seven tubes ranging from 1" to 36" make up the author's tubular mike; all construction details are given in text and in drawing at right. Completed unit is mounted on a camera tripod and panned like a machine gun to find sound source.

sponse to sounds of various frequencies, the air columns within each tube vibrate and, in doing so, amplify the original sounds.

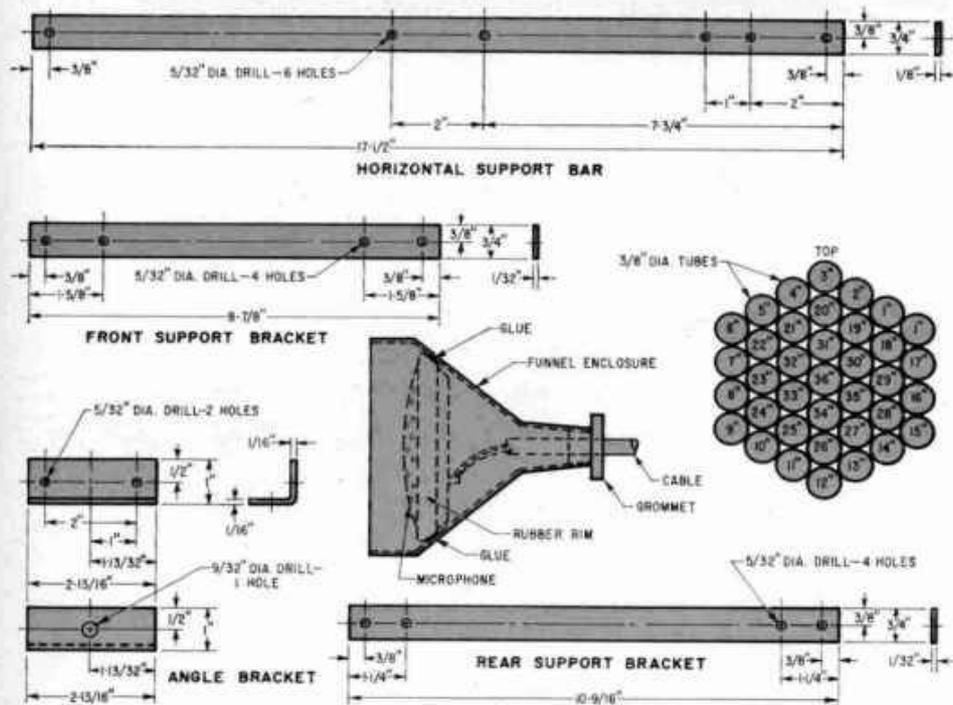
Applications of the tubular mike, which has far greater sensitivity, better frequency response, and superior directional characteristics than parabolic types, are many. Bird and animal watchers are delighted with the added dimension of sound when it is applied to nature studies. Small boat operators may find the unit of value as a navigational aid, especially in fog or conditions of poor visibility. The tubular mike can pick up conversations from busy streets, and under the right conditions, can actually pick up conversation through closed windows 40 or more yards away. The mike described in this article works well with tape recorders, and has even been used with a 100-mw. CB walkie-talkie.

Design and Construction. As you might assume, tubes are cut to resonate over a specific range of frequencies. To calculate tube length, first find wavelength by dividing the speed of sound (1100

feet per second for practical purposes) by the frequency. For example, the wavelength of 256 cycles equals $1100 \div 256$, or 4.296 feet. *Tube length*, however, is half this, or 2.14 feet, since tubes open at both ends resonate at a wavelength twice as long as their length.

In designing a tubular mike, it is necessary only to assemble enough tubes to cover the frequency range of sounds you want to hear. The exact number of tubes is not critical, but should be the greatest number that can be efficiently covered by the microphone element. The graduated lengths should be stepped evenly from the shortest to the longest so frequency nulls are avoided.

The "Shotgun Sound Snooper" is built with 37 aluminum tubes, $\frac{3}{8}$ " O.D., ranging from 1" to 36" in length, and graduated in 1" steps. The 37th tube is an extra 1" length added to complete the hexagonal symmetry of the pickup. The tubes can be conveniently cut from ten 6' lengths, using a tubing cutter or fine-tooth hacksaw. Dress the edges with a fine file to remove burrs. Assemble the



Easily worked aluminum is used for fabricating the pickup. The tubes can be conveniently cut from ten 6' lengths of 3/8" diameter stock, the support brackets

from a sheet or strip of 1/32" aluminum. The horizontal support bar is made from heavier stock. Angle bracket mounts to standard camera tripod.

BILL OF MATERIALS FOR MICROPHONE

- 1—56' length of 3/8"-O.D. aluminum tubing (ten 6' lengths preferable)
- 1—Crystal microphone cartridge, approx. 2 3/8"-diameter (Lafayette PA-27 or equivalent)
- 1—Household funnel, 2 3/8"-diameter
- 1—3/8"-wide, 1/32"-thick aluminum stripping for support brackets, battery bracket (approx. 2' required)

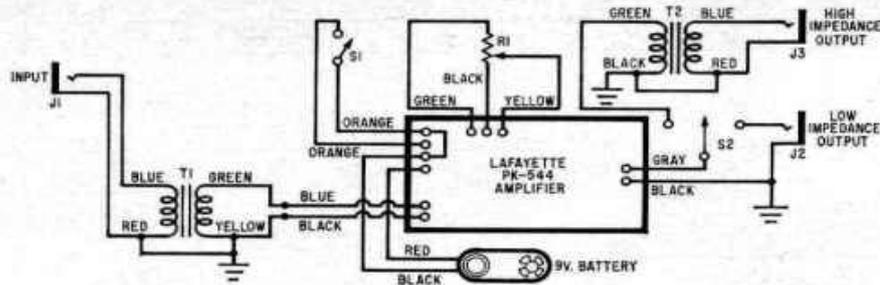
- 1—3/8"-wide, 1/8"-thick aluminum strip for horizontal support bar (approximately 1 1/2' length required)
- 1—Standard camera tripod
- Misc.—Glue (fast-drying rubber base contact cement or epoxy glue), 8-32 machine screws and nuts, rubber grommet, microphone cable, solder, etc.

tubes as shown in the drawing above, starting with the 36" length and gluing the 35" tube to it at at least three spots. The authors used fast-drying rubber base cement, but epoxy glue can be used for greater strength. In any case, be sure the tubes are flush at one end by checking each one against the others as you glue them in place.

Cut and drill the front and back support brackets from easily worked 1/32"-thick aluminum as shown in the drawings. The brackets are shaped around the tubes to form a tight fit; it will help if you bend each one at the exact center

to form a slight V before you shape it. Make the horizontal support bar from 1/8" aluminum as shown, and cut off a piece of aluminum angle to form the angle bracket.

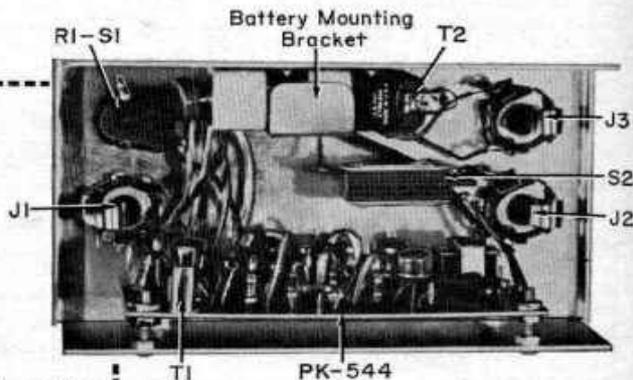
Cartridge Mounting. The microphone cartridge enclosure is made from a 2 3/8"-diameter household funnel. Hold the wide end to the tube cluster and mark the sides to indicate the corners of the hexagon shape. Place the funnel on a smooth, solid surface, and make dents at each of the six corners of the hexagon with a small ball peen hammer. With the flat head of the hammer, flatten the areas



Wire amplifier and other components as above; T2, S2, J3 are optional.

AMPLIFIER PARTS LIST

- J1, J2, J3—Standard open-circuit phone jack
- R1—10,000-ohm miniature potentiometer with s.p.s.t. switch S1 (Lafayette VC-28 or equivalent)
- S1—Part of R1
- S2—S.p.s.t. toggle switch
- T1—Transistor input transformer; 200,000-ohm primary, 1000-ohm secondary (Lafayette TR-120 or equivalent)
- T2—Transistor output transformer; 2500-ohm primary, 11-ohm secondary (Argonne AR-114 or equivalent)
- 1—Lafayette PK-544 5-transistor audio amplifier or other high-gain amplifier
- 1—9-volt transistor battery (Burgess 2U6 or equivalent)
- 1—Aluminum box, approximately 2 1/8" x 3" x 5 1/4" (LMB #136 or equivalent)
- 1—Miniature knob (Lafayette MS-185)
- 1—18" length of single-conductor shielded microphone cable
- 1—Set of headphones, high or low impedance
- Misc.—4-40 x 5/8" machine screws and extra nuts, scrap aluminum, contact cement or epoxy glue, wire, solder, etc.



Follow parts placement indicated (unit is inverted in this photo) to avoid possible feedback problems.

between the indentations for about 1/4" in from the edge of the funnel. Place it over the end of the tube cluster and peen again if necessary. A tight sliding fit is desirable, but a loose fit can be remedied with tape.

As shown in the drawing on page 53, the microphone cartridge is mounted in the funnel with glue. First connect a length of mike cable and install a rubber grommet in the small end of the funnel; apply glue to the rubber rim of the mike cartridge and to the funnel. Press the cartridge into the funnel, truing it up and clamping it into position until the glue is dry.

Final Assembly. Place the rear support bracket over the tube cluster 1/4" forward

of the flush end and tighten it onto the cluster with a 6-32 x 3/8" machine screw and bolt. Install the front bracket the same way, and slide the horizontal support bar between the brackets, aligning the holes in the bar with the lower ones in the brackets. Bolt the horizontal bar in place along with the angle bracket for mounting the microphone to the pan head of a camera tripod. Now fit the microphone enclosure over the tubes; it can be taped on if necessary with a strip of masking or metalized Mylar tape around the enclosure and the rear support bracket. The Mylar tape is not necessary, but looks better.

The Amplifier. Weak or distant sounds naturally require a high-gain amplifier. For this purpose, the five-transistor Lafayette PK-544 is ideal, and the cost is low. The high-impedance microphone cartridge is matched to the low-impedance amplifier input with a transformer. The high-impedance output shown in the
(Continued on page 84)

Shotgun Sound Snooper

(Continued from page 54)

schematic on page 54 is optional; *T2*, *S2*, and *J3* may be omitted if low-impedance output will suffice.

The PK-544, *R1*, *S1* (part of *R1*) *T2*, *S2*, and *J1*, *J2*, and *J3* are mounted in half of a 2½" x 3" x 5¼" aluminum box (LMB #136). As a matter of convenience, the authors first mounted input transformer *T1* to the board of the PK-544 amplifier. To do this, you bend off the mounting tabs of the transformer. Then apply quick-drying cement to the bottom of *T1* and to an open area on the amplifier board near the input leads. Mount transformer *T1* in this area.

When the cement is dry, remove the PK-544 input leads where they fasten to the board. Referring to the schematic, trim the low-impedance leads of *T1* and solder them to the board where the original input leads were attached. The high-impedance primary of *T1* is later connected to *J1*.

As shown in the photo on page 54, the PK-544 is mounted with four 4-40 x ⅝" machine screws and extra nuts to the top of the box. Tighten the screws with nuts, then use eight more nuts, four above and four below, to mount the board so it is well away from the metal box. Mounting holes are already drilled in the PK-544; disregard the mounting hardware that comes with it.

Drill holes in the front of the box for mounting the three jacks, controls *R1-S1*, and transformer *T2*. Drill a hole in the bottom of the box for the battery mounting bracket which is made of a piece of scrap aluminum. Referring again to the photo and schematic on page 54, mount and wire the remaining components, cutting any excess leads. In general, it's a good idea to follow the arrangement shown to avoid possible feedback problems.

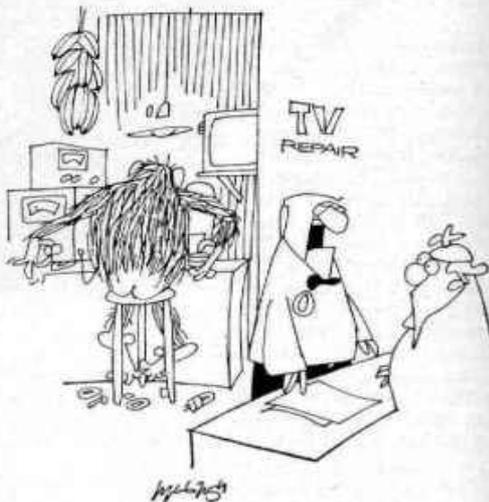
The bottom section of the box is fastened to the horizontal support bar of the tubular pickup unit by means of two 6-32 ⅝" screws and matching nuts. Place the top section of the box with the mounted amplifier components onto

the bottom section, fasten with the screws provided, and the completed unit is ready to use.

Operation. Operation of the "Shotgun Sound Snooper" is simple—just connect a pair of headphones and turn on the amplifier, adjusting the volume control carefully to avoid painful sound volume. The tubular mike must be aimed toward the location from which sound pickup is desired—sight along the tops of the tubes and turn the volume up gradually. Wind has the effect of carrying sound, so straight-on reception is not always possible.

Under windy conditions, the unit should be panned until the best reception is achieved as determined by ear. Noisy winds can spoil listening—especially if the tube ends cannot be sheltered a bit—but moderate wind noise can be cut down by draping the mike with a cloth. Annoying sounds of consistent frequency can often be partially blocked by simply plugging the tubes which are carrying them.

If you enjoy experimenting, you'll find the "Shotgun Sound Snooper" a unique, fascinating project. Endless variations are possible, of course—in tube length and diameter, in the microphone cartridge, the amplifier, etc. Just as endless are the applications you'll find for the microphone. Construction is easy, and the cost is reasonable. Don't delay! —50—



"Now what would banana peels be doing in your set?"

Rugged J-Pole Antenna Design

Overview

The J-pole antenna is one of the most widely used antennas in amateur SIGINT/EW radio due to its low cost and ease of construction & installation. Its design dates back to the early 1940s when it was trailed behind blimps (Zeppelins) for radio communications during the EuroSavage's annual little scuffle.

The antenna is called the "J-pole" because its elements are in the shape of a "J", duh. The antenna elements consists of a main radiating 1/2-wavelength vertical element which is fed by a (non-radiating) 1/4-wavelength matching stub. It is actually designed to be fed with a balanced transmission line (i.e. not coax), but there are tricks to overcome that. The radiation pattern is very close to that of a common dipole, but is skewed slightly due to interactions between the main element and the matching stub.

This article will cover the construction of a rugged, portable J-pole antenna that was designed to be used with FRS radios operating in the 465 MHz band. J-pole antennas are useful & scalable for any frequency between 50 and 900 MHz. The gain of this particular style antenna will only be around 1 dBd, based on EZNEC models. Testing shows it to give approximately the same performance of a 1/2-wave dipole. Contrary to what others may say, this antenna has *no gain* when constructed with only a single main radiating element. Increasing the main radiating element to 5/8-wavelength also *does not* improve the antenna's performance.

Schematic / Construction

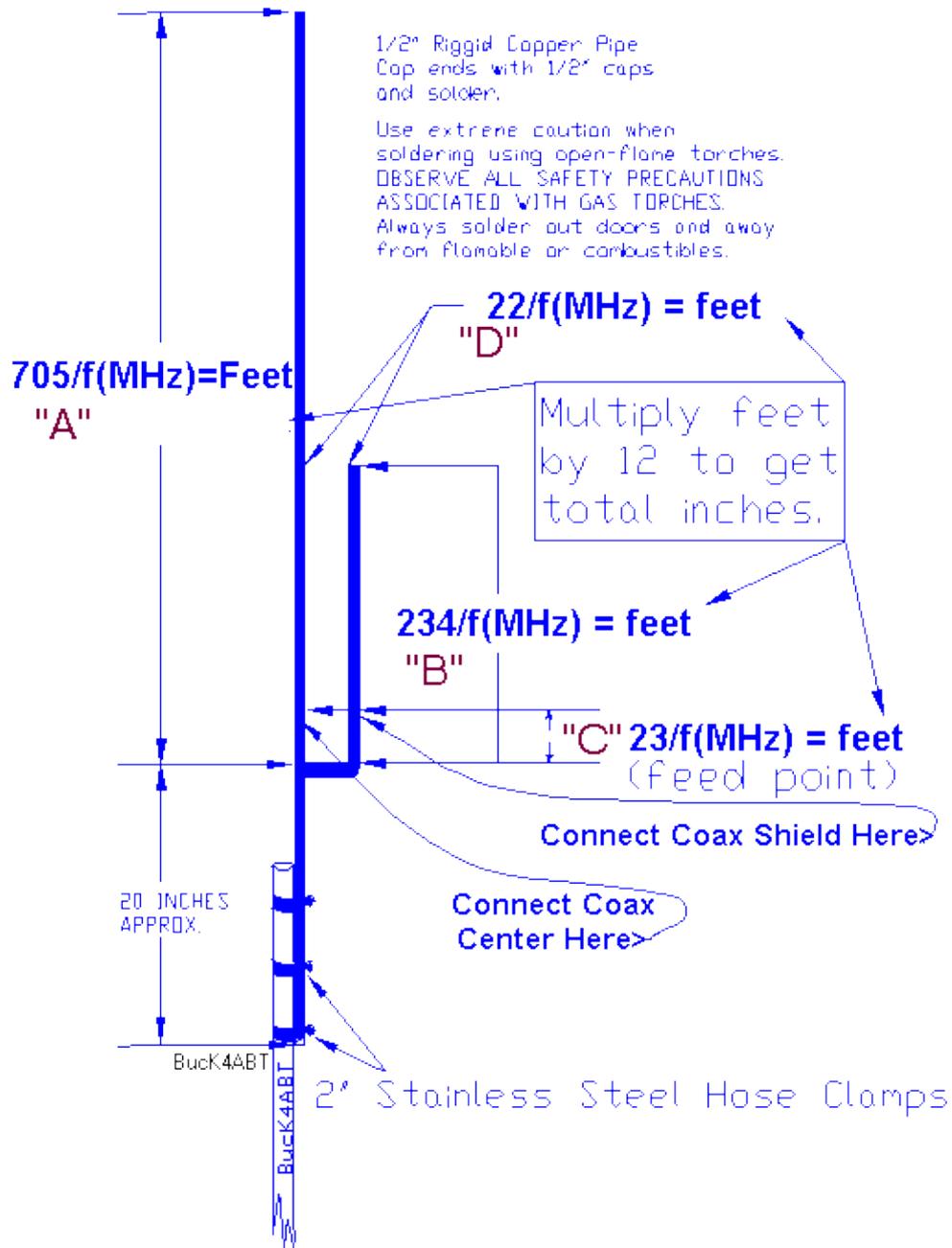
The best material for this antenna is 1/2-inch diameter rigid-wall copper pipe and fittings used for plumbing. 3/4-inch and 3/8-inch diameter pipe can be adapted when more strength or less weight is required. All the pipe and fittings must be properly fluxed and soldered for the antenna to work.

The copper pipe should be cut using a tube cutter and not a hacksaw. This will help maintain the fine dimensions required for the element lengths.

Every copper piece that is to be soldered should be rigorously cleaned with fine grit emery cloth. After cleaning the connection, apply a very thin coat of solder flux. Solder will *only* stick to the copper with the solder flux. Avoid using too much flux.

Soldering the connection is the most critical step. There are two main points you should follow when soldering copper pipe. First, avoid using too much solder. It will look messy and is really pointless as the mechanical/electrical strength comes from the metal-on-metal connection and not the solder. Second, avoid getting the solder connection too hot. Use a slowly rotating propane torch to heat the *entire* area to be soldered. Solder will also only flow where there is heat. Too much heat can weaken the solder connection and copper pipe.

Schematic is from this excellent website: <http://www.packetradio.com/JpoleCALC.htm>



Pictures



Example components used in the construction of a portable J-pole. From the left, is a large air chamber. This makes a perfect mounting pole. Next, the white parts, are threaded PVC couplers. WTF? Yes, if you isolate the J-pole antenna from the mounting pole, the antenna's

radiation angle will be much closer to the ground. This isolation is *optional*, as the PVC parts significantly reduce the ruggedness of the antenna's construction. The rest of the components are standard copper pipe fittings (elbow, T, end caps, threaded adapters) and a length of rigid-wall copper pipe.



Example picture showing the components soldered together. The PVC couplers should be glued to the copper.



Example picture showing the components of a rugged (non-isolated) J-pole. This design is more suited for portable operations. The radiation pattern has a higher "take off" angle, but the antenna will still perform flawlessly in almost all situations.



The removable main radiating element should *only* be used for low frequency (VHF) antennas. At UHF and higher, it will harm the antenna's performance – and it's not really needed as the element lengths are not too long.



You'll need to make element feed tabs to connect the coax to the antenna. An easy way to do this is to flatten copper pipe hangers, and cut off the ends with the holes. When soldered to the antenna's elements, the holes are perfect for mounting hardware, or for soldering the coax directly.



At VHF and lower frequencies, you can use copper split-ring hanger clamps. This will make adjusting the antenna's SWR much easier. Connect the coax leads to the hanger clamps, and slide them up and down to get the best SWR. Then apply solder into the threaded hole to secure the clamp into place.



Closeup view of the feed tabs soldered to the antenna's elements. Measure from the center of the tabs when performing the feed length calculations.



Example of the coax feed connection using brass hardware. This should only be done at VHF or lower frequencies. Add ring terminals to the coax leads.



A neat trick for fine tuning the antenna's SWR is to add an adjustable tip to the main element. This consists of brass #10 (32 TPI) hardware soldered to the end cap of the main radiating element of the J-pole. To do this, first flux and solder the end cap. Also flux and solder one side of a #10 brass nut. Heat the end cap again until the solder forms a little pool. Using a tweezers, place the soldered nut into the pool of solder. Wait until it cools. Drill and re-tap the nut with a #10-32 tap. Add a 3/4 or 1-inch long brass bolt and another locking nut. Adjust the "tuning stub" while watching the SWR meter as you tune the antenna.



A UHF frequencies, you'll have to solder the coax leads directly to the element feed tabs. This helps keep the antenna's SWR low. Use "Liquid Electrical Tape" to seal and waterproof the solder connections and the coax.



Finished J-pole antenna at the test range. It has a 15 dB return loss (or SWR under 2:1) across the entire FRS band. Note the coil of coax forming a decoupling loop below the antenna's feed. This helps prevent RF from flowing on the outside of the coax and distorting the antenna's radiation pattern. This is an important step. Just loop about four or five turns of coax tightly right before the antenna feed.

Bonus

COMMUNICATORS AND RADIO OPERATORS

The Central Intelligence Agency has excellent career opportunities for individuals with experience in HF radio, Morse intercept, satellite communications, or radio-teletype operations. If you are looking for the challenge of a CIA career . . . you could join a very select group of dedicated men and women who use their professional skills in unique and rewarding assignments throughout the world.

Skills/Experience:

Applicants should have experience as communicators, telecommunications specialists, radiomen, Morse intercept operators, or be radio amateurs with general license or higher. Morse code ability at 12 gpm is preferred; other applicants will be tested for Morse aptitude. Minimum touch typing speed of 30 wpm is required.



Personal Qualifications:

U.S. citizen (self and spouse); high school graduate or GED; availability for extensive overseas service. Must meet security and medical standards. Civil Service status *not* required.

Starting salaries \$15,398-\$18,215 depending on qualifications, plus substantial overseas benefits.

Attention Military Personnel:

Apply now if you are scheduled for separation within the next six months.

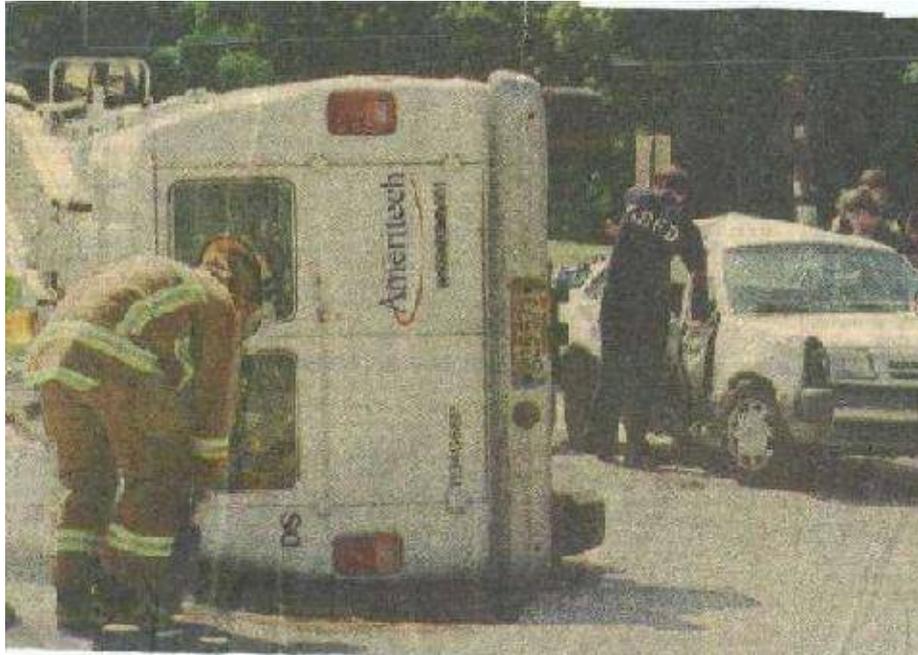
Send resume to:
Personnel Representative (JV)
P.O. Box 1925
Washington, D.C. 20013

TEXAS RESIDENTS:
CIA recruiters will be at
the ARRL "Com-Vention" in
Houston October 7-9, 1983.

Central Intelligence Agency

An Equal Opportunity Employer

End of Issue #16



Any Questions?

Editorial and Rants

The idea behind "African Aid" is to take money from poor people in rich countries and give it to rich people in poor countries.



Don't worry, those rich college professors and leftists thugs just *love* Marxist dictators.



Maybe if we all got together to hold hands and sing songs it will stop those bulldozers.



Where are those "human shields" now? I'm sure some California hippie will gladly lay down in front of that bulldozer, right after they get done making their "Bush is a Nazi" posters.



Those rich rock stars will be sending you some money from their album sales right away.



Don't worry... I'm sure France will help out.

Clear Skies End Global Dimming

May 5, 2005 – From: http://www.nature.com/news/2005/050502/pf/050502-8_pf.html

by Quirin Schiermeier

Earth's air is cleaner, but this may worsen the greenhouse effect.

Our planet's air has cleared up in the past decade or two, allowing more sunshine to reach the ground, say two studies in *Science* this week.

Reductions in industrial emissions in many countries, along with the use of particulate filters for car exhausts and smoke stacks, seem to have reduced the amount of dirt in the atmosphere and made the sky more transparent.

That sounds like very good news. But the researchers say that more solar energy arriving on the ground will also make the surface warmer, and this may add to the problems of global warming. More sunlight will also have knock-on effects on cloud cover, winds, rainfall and air temperature that are difficult to predict.

The results suggest that a downward trend in the amount of sunlight reaching the surface, which has been observed since measurements began in the late 1950s, is now over.

The researchers argue that this trend, commonly called 'global dimming', reversed more than a decade ago, probably following the collapse of communist economies and the consequent decrease in industrial pollutants.

The widespread brightening has remained unnoticed until now simply because there wasn't enough data for a statistically significant analysis, says Martin Wild, an atmospheric scientist at the Swiss Federal Institute of Technology in Zurich and an author on one of the reports.

Wild and his team looked at data on surface sunshine levels from hundreds of devices around the planet. They found that since the 1980s there has been a transition from decreasing to increasing solar radiation nearly everywhere, except in heavily polluted areas such as India and at scattered sites in Australia, Africa, and South America.

A second study, led by Rachel Pinker from the University of Maryland, College Park, found a similar trend by looking at satellite data, although their research suggests the extent of the brightening is smaller. Unlike ground stations, satellites can sample the whole planet, including the oceans. However, satellite data are difficult to calibrate, and so are considered less accurate than measurements from the ground.

Surprisingly, Wild's study shows a brightening trend in China, despite the fact that there is a booming, fossil-fuel-intensive industry in that country. Wild says he can only speculate that the use of clean-air technologies in China might be more widespread and efficient than has been thought.

In contrast, India's vast brown clouds of smog, which result from wildfires and the use of fossil fuels, have reduced the sunlight reaching the ground.

Researchers will now focus on working out the long-term effects of clearer air. One thing they do know is that black particulate matter in the air has been contributing a cooling effect to the ground. "It is clear that the greenhouse effect has been partly masked in the past by air pollution," says Andreas Macke, a meteorologist at the Leibniz Institute of Marine Sciences in Kiel, Germany.

Uncertainties remain part of the game because scientists have only a limited ability to track cloud cover and particulates, says Macke. Increased cooperation in programmes such as the NASA-led International Satellite Cloud Climatology Project should help to close the gaps in our knowledge of how dirty air affects climate, he says.

EU Fails to Cut Greenhouse Gases

June 21, 2005 – From: <http://news.bbc.co.uk/2/hi/science/nature/4115670.stm>

Emissions of the greenhouse gas carbon dioxide rose in the European Union by 1.5% in 2003 after falling in 2002, the European Environment Agency reports.

Italy, Finland and the UK were named as the worst offenders while cold weather was blamed for a rise in the use of fossil fuels to heat homes and offices.

Some commentators now doubt the EU can meet its promise to cut emissions by 8% of 1990 levels by 2012.

A spokesman for Friends of the Earth called the new figures "shocking".

"The blame goes mostly to national economy and industry ministers, who constantly block any attempts to introduce mandatory targets for renewable energies, energy efficiency rules or fuel consumption standards for cars," Jan Kowalzig said.

Carbon dioxide emissions have risen by 3.4% since 1990, according to the EEA figures.

The Copenhagen-based EEA said emissions in the 15 old EU member states increased by 53 million tonnes, or 1.3%, in 2003, after a drop in 2002.

According to its figures, between 2002 and 2003, Italy, Finland and the UK saw the largest emission increases in absolute terms – 15m tonnes, 8m tonnes and 7m tonnes respectively.

EU Environment Commissioner Stavros Dimas called on member-states to meet their commitments.

National Public Radio Employment Application – "NPR_app.doc"

Here are our basic criteria for consideration. The "correct" answers are supplied in italics. Any applications that deviate from our high standards will be used as placemats for our pastrami and lox lunches and summarily thrown out.

1. Gender:

- A) Female
- B) Effeminate Male
- C) Homosexual Male
- D) Male but guilty about it, have a lisp, and am considering a sex-change operation
- E) Normal heterosexual male

Correct answers: A, B, C, or D

2. Race:

- A) White
- B) Negroid
- C) Jewish
- D) Hispanic
- E) Asian Indian with an unfathomable name like "Sneedeek Ungrapradesh"
- F) White but can manage convincing or empathetic pronunciations of "Neeearlagua" or "Barheeo" that suggest I actually hang out with spics in dangerous neighborhoods

Correct answers: C, D, E, F, or B if we need a token nigger

3. Religion:

- A) Jewish
- B) Reform Jewish
- C) Unobservant, secular Jew
- D) Atheist Jew
- E) Lapsed Catholic but I've been interested in the Kabbalah lately
- F) Lapsed Episcopalian but I have a lot of Jewish friends, really
- G) Unitarian Universalist

Correct answers: D, C, B, A, F, E, G in that order

4. Education:

- A) CUNY
- B) Columbia Journalism School
- C) Berkeley
- D) Brown
- E) The Hebrew School
- F) Wright State University

Correct answers: A, B, C, D, or E

5. Marital Status:

- A) Married to any influential male in New York or Washington who feeds me news leaks and would be glad to see me trot off to NPR every day so he'll be out of earshot of my all-knowing, smug, pseudo-intellectual voice
- B) Single, no one can stand me because I'm a yattering harpy or a fey excuse for a male
- C) Divorced, no one could stand me because I have a nasal, whining, supercilious voice that never stops
- D) Divorced more than once, absolutely no one could stand me because I'm a neurotic, hectoring termagant with serious mental problems

Correct answers: A, B, C, or D

6. Where is Indiana?:

- A) Somewhere west of 42nd Street
- B) I think it's next to Idaho, isn't it?
- C) West of Louisiana

Correct answers: A, B, or C

7. According to the the FBI's Uniform Crime Statistics; What Group Commits the Most Violent Crimes per Capita in the United States?:

- A) Young lazy black males
- B) Young lazy Hispanic males
- C) Working white crackers in the Midwest

Correct answer: C, despite all evidence to the contrary

8. What is Your Conception of the American Midwest?:

- A) A large agricultural and industrial region that was the engine for much of America's growth and prosperity, settled mostly by white European immigrants whose work ethic, honesty, and devotion to family made it a safe and enjoyable place to live
- B) A dark, forbidding, uncharted no-man's-land I've flown over on the red-eye from L.A., inhabited by inbred German farmers with huge gun collections and a seething hatred of Jews and nonwhites. No good delis. Useful for occasional "color" features to lead listeners to believe we know where it is.

Correct answer: B

9. On your desk are two possible story leads in Dayton, Ohio for "Morning Edition" handkerchief-wringers. You have a four-minute slot to fill and can only use one. David Kastenbaum has been booked for a fast flight out of JFK and is nervous about being so far away from a deli and being beat up by crackers, but he's agreed to interview your choice. They are:

- A)** A white high school student in traction who was set upon by a gang of African-Americans who gave him a "curbie," blinded him in one eye, collapsed a lung, broke four ribs, and deprived him of a football scholarship by crushing his kneecap. They needed his lunch money for wine. The student is only the latest in an alarming pattern of black-on-white violence at a large high school.
- B)** Linda Wertheimer's nephew by her sixth husband, a homosexual associate professor of comparative literature at Wright State University, was called a "homo" by a white who rejected his advances at the local Starbucks. He's had to increase his antidepressant dosage and psychotherapy visits and take a leave of absence until he recovers. Possible angle is the alarming rise in "gay-bashing" in the American Midwest.

Correct answer: B, of course

10. An Israeli Jew with a fake passport was arrested on the Ohio Turnpike with \$20 million worth of the dangerous psychedelic drug "Ecstasy" in his trunk. The state troopers had to Mace him when he resisted arrest. It's well-documented that Jews run the Ecstasy trade worldwide and most large seizures of the drug have involved Jews. We have no stories in the pipeline this morning on homosexual New York performance artists or Zimbabwean naturalists fighting to save the rare Bukkake Beetle from extinction as white farmers are raped and slain all around them. We may have to run this story. What spin should you put on it?:

- A)** The questionable legality of search-and-seizure laws under current interpretations of the Fourth Amendment
- B)** The alarming increase in police brutality in the American Midwest
- C)** The alarming increase in "racial targeting" methods employed by police in traffic stops
- D)** The widespread destruction and increasing dissipation of white American youth, especially impressionable females, through the use of a drug formulated and marketed by Jews reaping huge profits

Correct answers: A, B, or C

- AT LEAST OUR SIDE
DO NOT MAKE
PRISONERS DANCE
WITH THE PANTIES
ON HEAD!!



YOUR SIDE
DOESN'T
HAVE PRISONERS
WITH HEADS.

