E.D.I.T

Electronic Deception, Interception & Terrorism : The Radio Shack Reality!

presented by

Ian A. Murphy, President & CEO

IAM / Secure Data Systems Inc.
1225 North Second Street
Philadelphia, Pa 19122
(215) 634-5749

"Electronic Deception, Interception & Terrorism : The Radio Shack Reality!

Objective and Scope of the Problem

The use of personal computers and the growth of electronics into the mainstream population, will allow almost anyone with basic understanding of common technology, the possible interception and collection of information that would not be available under normal conditions. Suppliers of basic electronic equipment now provide a number of different devices for the unknown numbers of possibilities for interception of tele-communications, data communications, and microwave and satellite communications for a small price. Some equipment is advertised to be a small as a dime and may be purchased from the back of many electronic magazines for under $30.00. Other devices are a bit larger and need more expertise to operate, but are still in the hands of many.

To all of this, we add the entry of the personal computer and its ability to collect millions of bits of data in seconds instead of the human needing to ingest and store such information. The information can be collected onto tape or floppy disk and removed to a safer location with ease as compared to the removal of such volumes of information in paper or book form.

Other problems involved with possible comprimised conditions include outside data communication contact persons who have no authorized access. Groups known to both law enforcement and the public media have surfaced from time to time and with some most embarassing information about corporate and goverment networks and computer systems.

Most invasions occur with little notice at the time of entry and are only detected when major system problems or audit information are scanned. Public (private) domain systems are accessible around the clock without cost to thousands and provide the underground with an excellent source for information.

These systems contain information for the compromise of various communications networks and operating systems to the construction of explosive devices and different methods for gaining physical access to such networks. All is known to be in the hands of a vast majority of minors, but if such information is available to anyone with computer communications ability, then the threat of such incidents occurring increases tenfold.

The reason is due to the ease of access from anyone with the right information available to call these outlets of sensitive knowledge. The statement from Thomas Jefferson, represents the spirit of the words, "Knowledge is Power." as frightning truth in today's information society.

"Electronic Deception, Interception & Terrorism : The Radio Shack Reality!

Results to Date

With the continued expansion of computers, many individuals and groups have been brought to the attention of law enforcement authorities. Groups with names such as The Legion of Doom, Knights of Shadow, The 414 Gang, The Brotherhood of Ohm and others. These groups consist of minors who trade information on a number of computers and telecommunications systems.

These individuals have become known due to their actions on the systems of their choice. Reasons for discovery include the blatant posting of about plans to attack such systems, pieced-together information from telephone company records, credit card frauds committed to obtain computer hardware and software, and systems security violated numerous times by outside telecom contacts.

These groups have a small impact on overall communications insecurity and pose little threat to national and corporate security. But the major problem associated with the leak of sensitive knowledge, comes from the lack of true indicators of such incursions in these networks. If persons with little directed intent are able to gather sensitive data from a number of public and underground sources, then a directed force will have a much easier time gathering facts and building upon them. Such fact gathering abilities come from eastern bloc countries with representives in this country, using "listening posts" stationed in major urban areas under diplomatic immunity to average citizens with back yard satellite dishes, personal computers and home-built or store-bought electronics.

An example; According to statements made by David L. Watters before the Senate Select Committee on Foreign Intelligence in Febuuary 1977, the Soviet embassy in Washington, D.C. was in a direct line of interception for most of the federal goverment microwave communications. The embassy had the ability to receive any transmissions from sites such as White House, Tennely Tower, the Pentagon, Ft. George Meade, Ft Belvicur, Andrews Air Force Base, Walter Reed Medical Center and other such governmental sites.

Costs of such methods do not come cheaply and require industrial communications equipment to gather and process large amounts of such traffic in an urban environment. It should be noted that the embassy is located on the highest piece of land in the city of Washington and that alone allows for very easy signal reception from such generating facilities in the metropolitian area.

"Electronic Deception, Interception & Terrorism : The Radio Shack Reality!

Results to Date (con't.)

With common sense applied, one must assume that the goverment is using encryption methods to transmit information over communications channels. The one benefit the such methods allow is for the useful lifetime of the information to remain valid as well as keeping such information guarded from unauthorized sources. But since this information is secured from such easy desemenation, the value of interception decreases to a point where the ability to decipher such information becomes too costly in a time value stance.

One interesting twist to the encryption methods used by both the public and some goverment agencies, is the use of the DES (Digital Encryption Standard).The DES is an encryption method endorsed by the federal goverment for use in the public domain. This method is currently protected from disclosure outside the U.S. and selected NATO countries and has been classified as a "Material of War". The method was introduced as a secure method of encryption for information with the possibilities of the correct information being decoded in a one to a 72,000,000,000,000,000,000 chance.

These odds are not to be ignored and do prove to be most formidable to unauthorized access with the exception of major goverments. The method was adopted by the commerical sector and has been deployed over a number of years in multiple sites, with little hesitation from the users. User confidence was quite high with this method, but a question must be raised about the release of such methods into the public domain.

Since this method is secured from decryption in a time value stance according to goverment information, then why is such a method in the hands of the public? Can it be possible that the method has accessible trap doors imbedded to allow inspection of the encrypted information? Would the federal goverment release a method so secure into the hands of the general public so that not even they could read such information? And why is the method not being re-certified by the goverment? Has the usefulness of this technique reached a saturation point where the time needed to decrypt the information, has become a matter of hours or days instead of the reported years?

The weakness of the DES system has been shown by a number of underground technicans working on the problem of encrypted satellite television transmissions. In one recent 90 day period, both the Oak Orion and the HBO scrambling systems have been cracked with skill. Chips for the decryption of these signals are on the underground market and can be produced as easily as most other commercially produced chips.

"Electronic Deception, Interception & Terrorism : The Radio Shack Reality!

Continuing Development Activity

In addition, the increased skill of persons with directed intent who are able to obtain knowledge for the invasion of networks and systems allows for penetration of systems with ease. These individuals are seeking ways to gain entry with little detection involved and may be using the underground sources of information as roadmaps to targets. These entries will be planned and used to the fullest possible extent without the owners of systems being any wiser.

Computer and communications facilities are being attacked by a vast group of computer literate persons seeking information and challenges that are not available in a normal data processing environment. People are seeking out connections to systems that answer and allow connection to same. The general public is being fed a constant diet of computers and communications. Society as a whole is undergoing a major re-education process in information processing and storage. Technology that needed space larger than any desk could contain is now available to sit on that desk and has more power than its predecessor, performing the same functions in half the time.

Individuals without computer skills are now able to use the technology to work better and faster. Others are able to solve problems that could not be solved 10 years ago due to the technology, and now most commerical products have some form of directed artifical intellegence in place and operational.

Information of a special or technical nature about electronics, communications and computer safeguards, is traded like baseball cards on the street. Persons have in-depth knowledge of hardware and software security methods and discuss such topics in open public electronic forums around the country. Information on software such as IBM's RACF, (R)esource (A)ccess (C)ontrol (F)acility, Computer Associates "Top Secret", and DEC Vax / VMS Security methods and the like are discussed as common topics in underground circles. Meetings are held each and every Friday evening in New York for the discussion of these topics and more. Conferences held for science fiction readers contain large populations of these persons and allow for information to flow to sources not normally exposed to such.

The possibility of information of a sensitive nature being in the hands of individuals who should not have access to such, is a problem that stems from the ability of persons to research information from a variety of sources available to the public. First Amendment rights allow for the discussion of information and technology and provide the needed stimulation to continue research and provide for new developments. Many areas offer small insights to overall changes in technology and invite inspection of other areas.

"Electronic Deception, Interception & Terrorism : The Radio Shack Reality!"

Continuing Development Activity (con't)

Home-made satellite transmissions stations are being constructed by HAMS and such for under $100 dollars, while current orbiting systems are completely vunerable to outside interference and jamming. The classic example is the Captain Midnight caper in early 1986. "Tempest" frequencies readers or scanners may be built for under $150.00 dollars and plans for such devices may be purchased for $19.95 through the mails. Cable location service is just an 800 number call away, and still the industry does nothing about the problem, cause or solution!

Summary

The use of common electronics and standard research in public domain databases will allow for the possibilities of simple terroristic activities happening with regularity to major telecommunications and computer centers. Already, computer centers in western nations have become the target of terroristic organzations. Computer hackers are reported as standard news today, and reports of special frauds and thefts continue with predictable time periods between each case and the results always being hidden from view to authorities due to the lack of understanding. Some results of such frauds are presented in plain view at times, and the investigators cannot "see the forest for the trees." The general population does not see computer intrusions as a problem related to them.

Public knowledge of "computer crimes" comes from embellished stories presented by the media. Crimes committed against the different telephone carriers are responded to with a sense of wonder and awe from the general populace. The resident problem stated comes to the simple premise of basic "today" education. But if the education teaches the populace how to interact with the systems, is it able to police the same with confidence? Can the users be educated with the basic instruction for security as they have been about other forms of security? Do they understand what is being presented in the new age and are they willing to learn new methods for insuring security for all users? Can the security be maintained for the information as the information and its vessel grows?

Conclusion

The need for security in today's information age will require more thought and understanding of a criminal nature to secure the assets. A new form of asset transference is as available as the six shooter was in the early days of the West. To close, the words of Thomas Jefferson once again state the truth for this age, " If you remove a little bit of freedom for the sake of security, then in time you will have neither.".

Ian A. Murphy

Copyright Ian A. Murphy , IAM / Secure Data Systems, Inc., 1987

"Electronic Deception, Interception & Terrorism : The Radio Shack Reality!

Continuing Development Activity (con't)

Collection of information by electronic methods has become very standard in today's society. Multiple devices can be placed in locations never suspected as being active listening posts, and size is no longer considered a problem due to the development of integrated circuits. Some support devices can offer close unlimited range with proper set-up. Others allow for the interception through standard off-the-shelf technology and completely bypass any common physical security methods used to enforce.

Low cost systems may be purchased and bastardized for the required purpose. Small radio transmissions systems with ranges stated to be in excess of one mile are very easy to obtain by calling or writing the manufacturer. Others are discussed in the general print media and complete volumes are available with plans, parts lists and construction methods needed for operation.

All this information and equipment is in the hands of the general population and if it is so available, then what is the way to protect such information from interception and use? Is the trust of the user of this information questioned? Is the information real or placed in the media to dis-inform possible threats? What is the truth of the matter? Facts presented in one media are contested in others. Papers are presented and discussed with point and counter-point. All offer a number of possible facts that allow for the gathering of small but connected thoughts that provide the necessary details.

Techno-fables are widespread; goverment, industry and the general public refuse to accept such stories due to lack of understanding. Capabilities well beyond what most of us would think are in the hands of common persons. Simple electronics offer a whole new world of eavesdropping and collection abilities for under 200.00 dollars and still we have persons who think such things are science fiction.

Imagine using a common household microwave oven for such actions. Most would not see the use of such a device, but microwave ovens may be purchased for under $59 dollars in most areas and with a bit of component re-structuring, can produce frequencies well within commerical transmission range as well as front-end equipment damage to such sites. Belief in the "tap proof" security of fiber optics has been smashed. Simple fiber technology is the way, and counter-devices may cost 100 to 1000 times more for the detection and protection of such circuits.

§ Electronic Warfare §

Intro

Electronic warfare plays an important part in military operations today because of the integration of high-tech in the battlefield. The definition of Electronic warfare is "Military action involving the use of electronic equipment to gain in intelligence; to exploit, reduce, or prevent an enemy's use of electronic equipment while taking action to ensure use of electronic equipment by friendly forces." (Burton, Pg. 66) While this may seem a tall order, the nuts-and-bolts of it are pretty simple, and easy to accomplish by any one with moderate knowledge in communications electronics; such as a ham radio operator. The definition above covers three basic tasks: signals intelligence (SIGINT), electronic countermeasures/jamming (ECM), and electronic counter-countermeasures/anti-jamming (ECCM). For about $500 (new retail value) one can assemble a complete, effective EW setup. For about $2500 one can assemble a top-of-the-line EW station. The equipment can also serve as part of your regular commo station, and should be considered part of it.

EW is an integral part of guerilla warfare resistance operations. By using SIGINT to gain information on enemy activities and order of battle, and by denying an enemy the use of his radio communications facilities, one can gain the added edge for successful operations. ECCM knowledge is also very useful, thus allowing you use of your communications capability should an enemy attempt to deny you use of the airwaves. When the proper techniques are used, EW can act as a psychological warfare device, demoralizing the enemy, and further contributing to his defeat. In the U.S. Military, EW information and techniques are considered a subset of military intelligence have a Top Secret (highest known) security clearance; which should act as an indicator of the importance they assign to it. However, the techniques are simple in theory and applications, and are presented here in a scale most suitable for resistance activities, and put into easily understandable form.

SIGINT

SIGINT has three aspects. The first aspect is the interception and decryption (if necessary) of enemy radio communications. The second is the determination of enemy plans and order of battle (force strength) by way of these intercepted communications. The third is the determination of enemy location via RDF (Radio Direction Finding) techniques. Since most tactical, and an average amount of strategic communications go out via radio, SIGINT is a viable means of getting information about the enemy.

Interception/Decryption

This is both the easiest and most difficult aspect of SIGINT. In this stage, one finds the enemy communications, records it for future analysis, and if necessary, converts it into a readable form by descrambling it, or decoding the message content.

For optimum interception operations a listening post should be able to do the following:

1. Cover as wide a bandwidth, and as many signal modes as possible.
2. Signal-

6. Decoding of known scrambling modes in order to provide understandable communications.

Equipment

The main piece of equipment needed for a listening post are radio receivers capable of picking up the frequency range(s) of interest. For most purposes, this would cover 100 khz. to 2 Ghz. Certain non-communications interception application s (such as RADAR), and point-to-point microwave link interception will extend the upper frequency limit. One will also need antennas which will cover the necessary frequency ranges. Also necessary for non-voice interceptions are RTTY (Radio Teletype) Demodulators. Another handy item is a good-quality tape recorder for saving intercepted signals for future analysis, and for performing automated interception when no one is able to man the listening post.

Once one has the basic set-up, certain accessories can be bought which increase the effectiveness of one's listening post. Audio and RF Filters are inexpensive to buy/easy to build, and can help clarify signal reception. Spectrum Analyzers make finding communications signals easier by providing a "picture" of RF activity in your area. Oscilloscopes make analyzing non-voice audio communications easier; along with frequency counters; which can also aid in determining operating RF frequencies of enemy communications during field investigations. Finally, there is the computer. A good system will help you in, among other things, unattended operation of your listening post, logging of your communications intercepts, analyzing them, and in assisting in cryptoanalysis of encrypted communications. Fortunately, for the budding signal intelligence interceptor/ analyst; there is a wide variety of equipment available to serve myriad of operational situations. While by no means exhaustive , this list will hopefully act as a starting point to assist you in finding your optimum equipment set-up for your needs.

Receivers

There is a lot of good receiving equipment out there which will suit one's purposes well. Starting at the top of the line are the Icom R-9000, and the Sony CRF-V21. These units feature frequency coverage from 100 Khz. to 2 Ghz., large memory capacity, built-in spectrum analyzers, and built-in demodulators for RTTY and FAX communications. They retail at an expensive $5000 each. Also just released by Kenwood is the RZ-1 which is a standard scanning receiver with coverage from 500 Khz. to 905 Khz. They are most suited for frequency search operations with their spectrum analyzers, and "all-wave" frequency coverage, although one doesn't need a spectrum analyzer for effective frequency searching, and for $5000, one can get a complete communications station.

Besides the units mentioned above receiving equipment covers one of two ranges: either 100 Khz. to 30 Mhz. (shortwave), or 25/30 Mhz. to 2 Ghz. (VHF/UHF). Of the two, most of your activity will be focused on VHF/UHF, as this frequency range is most suited and used for tactical communications that will most affect your operations. This is not to say that shortwave isn't important either. Shortwave contains international broadcasters which are essential in keeping your group in touch with the news "out there" (see Alternate News Gathering Techniques Chapter), and also many strategic channels, and national/regional/worldwide coordination frequencies which transmit information that may aid larger operations, such as a "resistance command", or operations involving different groups in a large area.

Shortwave Receivers

In the realm of shortwave receivers. The top three are the Japan Radio NRD-525, Kenwood R-5000, and Icom R-71A. These units feature standard shortwave coverage, memories, memory scanning functions, and extra filtering to improve signal read ability. They are also are standard equipped to accept RTTY/FAX demodulating equipment. These units cost $850 for the Icom and Kenwood, and $1200 for the Japan Radio Model. If one has the need for highly sophisticated shortwave capability, then thee units are it. I've heard very good reviews about the NRD-525, although the high price puts me off. I personally prefer the Icom R-71A, as the price is less expensive, and it still has enough features to get the job done in style.

Going down in price are Kenwood R-2000 and Yaesu FRG-8800 ($600-$700). These units are less "fancy" than their higher-priced models, but are still have the same features as them, just a little less sophisticated. These two mid-level units offer the best value for someone desiring to have a fairly sophisticated shortwave listening setup; offering the best compromise between price and performance.

For the individual who just needs occasional shortwave monitoring capability, there are several low-priced ($200-$300) units which fit the bill; such as the Sangean ATS-803A, Sony ICF-2010, Magnavox D2935, and Radio Shack DX-440. While not having all the handy bells-and-whistles of the other units, these units are perfect for someone who mostly monitors shortwave broadcasters, and occasional non-broadcast "utility" voice transmissions. They can also be rigged to receive "non-voice"/RTTY, but the performance is a bit lacking. These units are best suited for someone who wants to be able to receive shortwave, and still wants adequate performance.

For someone on a very limited budget, there are the "multiband portable" radios such as the Radio Shack DX-360, SW-60, and Sony ICF SW20 going for about $100. These are very basic, linear display, AM mode only shortwave receivers designed for reception of high-powered shortwave broadcasters, which is all they are suitable for. Some of models also cover VHF/UHF, such as the SW-60. Unless all you will ever want to listen to on shortwave are broadcasters, I would advise springing the extra $100, and getting the next higher step. These multi-band portables are also available at flea-markets and garage sales for about $15. If one can get a multi-band portable with SW and VHF/UHF coverage in decent condition at such a price, then it would make a worthwhile addition to one's listening post as an expendable back up unit, "fast-search" unit, or single-channel monitor. The tuning-dial function enables one to get a quick-fix on nearby enemy troops who are using commo equipment without having to do a mad rush programming in scanner search limits. One can use it to listen to, say the local police/military tactical/surveillance channel, your group's operations, or any other priority-type frequency which constant monitoring is nee needed without tying up other equipment; particularly if you don't want to miss anything on your special frequency when your scanner is cycling through it's other channels, or to listen to a continuously active channel; such as some ham repeaters, broadcasters on AM, FM, and/or Shortwave, surveillance equipment (bug) frequencies, NOAA weather broadcasts, or TV/radio station studio-to-transmitter links; which would lock-up your scanner, and make you miss the stuff on the other channels.

VHF/UHF "Scanner" Receivers

The mainstay of your listening post will consist of VHF/UHF receiving equipment, as most of your listening activity will be centered there. Just like shortwave equipment, there are several price levels of VHF/UHF scanners which offer different performance levels, features, and purposes. There are so many different specific makes out in the market, so I will only cover some of the more noteworthy types. The major brands are Radio Shack, Regency, Uniden/Bearcat, Cobra, and AOR. The ham manufacturers Icom and Yaesu also make notable VHF/UHF communications receivers as well; although they cannot really

be considered "scanners" per-se.

Starting at the top is the Icom R7000 @ $1000 featuring 25 Khz. to 2 Ghz. all mode coverage (USB, LSB, FM, AM), 99 memories, optional shortwave coverage, audio noise blanker, infrared remote control, and optional computer control and voice synthesizer. While a top-line performer, particularly with the computer control option installed (more on that later), there are several lesser-priced models which will do the same thing; however if you can afford an R-7000, go for it. Figure EW-1 lists commonly available VHF-UHF receiving equipment, their prices, and important features. All the equipment listed in the table is of good to excellent quality, and will serve well.

Spectrum Analyzers

A spectrum analyzer is a oscilloscope-like device which enables one to get a video representation of a section of the RF spectrum. It is very efective in counter-surveillance operations, and in frequency hunting. Up until recently, they were very expensive pieces of equipment., but now there is a device which will hook up to a standard oscilloscope, and turn it into a spectrum analyzer. The plans for this device are in the September and October 1989 issues of "Radio Electronics" magazine, or you can get a reprint of the articles, along with some more notes on spectrum analysis for $4 from OCL/Magnitude, P.O. Box 64, Brewster, NY 10509.

Power

One of the first accessories you'll need is a good power set-up. It should be capable of not just 120v operation, but also be independent of the standard power lines. Ideally, it should be as self sufficient as possible. For your 120v connections where, and when it's available, get some EMI/noise filters, a good surge suppressor, and a multiple outlet "power strip". No problem there, as all of that is available from Radio Shack. Then, the fun starts when you go "independent". There are basically two ways to go; batteries, and generators.

On the low-end are rechargable batteries. Standard battery operated equipment can run on ni-cads, whereas the 12v stuff can run on heavy-duty gell-cells, or car batteries. One should also be able to charge said batteries without relying on 120v AC. A small solar-cell array, or wind/water powered generator should do the trick. The idea when using batteries is to keep two sets. You run on one set while charging the other.

For those of you desiring style, you can go with a heavy-duty (at least 1000 watt) generator. This is different than the small-scale generator discussed above as you need a far greater power capacity as you are running equipment rather than charging batteries. This equates to about 10 times more current capacity. The problem with generators is getting one that doesn't run on gasoline, as the idea here is to keep it going after civilization collapses. I'd say the best way to go would be alcohol fuel, methane, or small-scale hydroelectric. Also, if one lives near an ocean, or tidal shore, one could also use the tidal movement of water to generate electricity. We get further into independent power sources in the "Survival Residences" chapter.

Computers

While not necessary, a dedicated computer for your commo set-up is a handy thing to have, and a necessity if you want to get into digital communications interception. There is also CRIS, a software/hardware package which automates certain brands of communications equipment, most notably the Icom receivers.

With computer automation, one can either run the LP with less personnel, or run it on a limited scale with no human assistance. You can also use the computer for logging your intercepts an frequency information, as well as in assisting you in decoding encrypted digital commurications .

The two machines which seem to have the market cornered for LP operation are the Commodore 64 and 128, and the IBM PC/clone. The PC clone's virtue is that it has CRIS, as well as various digital commo software available for it. The Commodore; while not having CRIS (Although I'm sure a good programmer could rig something), is less expensive, and has less expensive digital commo equipment available for it. Another contender are the old 8-bit Atari computers with the 850 interface. The 850 interface was and still is the most flexible digital commo RS-232 (AND 20ma current loop) ever made. Too bad it's been discontinued. Most people who are familiar with Atari equipment are well aware of the value of the 850, and price it accordingly. However, if you come across one in working condition somewhere at a reasonable (under $100) price, BUY it! The 8-bit machines are available easily enough, and a little looking around in Atari circles should get you the software you'll need.

However, if you're looking for something inexpensive to use to receive digital commo, go buy a Commodore 64.

Decrypting data is a different story. You'll want as powerful and fast a machine as possible for any cryptoanalysis you might be doing. Sure, you can do it on a Commodore 64, but it'll take you a loooong time. The best machines currently out which would do the job would be one's that use the Motarola 68000, and the Intel 386. Co-processors are also nice to have as well. The problem is that these machines are expensive, but you asked; however they are coming down in price, and will continue to do so. Consumertronics sells our Cryptoanalysis Techniques publication, which includes software for IBM PC/Compatable Systems (this includes 386 machines). Also, read the "Cryptography" chapter in this publication.

Computer RTTY Equipment

There are several different software packages available which enable RTTY ("radio teletype", digital radio commo) demodulating. Just about all commercially available RTTY packages are designed to work with a home computer.

What is basically the top of the line unit for digital radio communications is the PK-232 Multimode Data Controller made by AEA. Costing $319, this unit will modulate and demodulate weather FAX, morse code, Cyrillic (Russian) morse, baudot, Cyrillic Baudot, ASCII, AMTOR, Japanese Katakana digital commo, and AX.25 packet signals. It is capable of automatically analyze an incoming signal, determine it's type, and decode simple baudot encryption schemes. It can also interface to a higher-speed modem for use with the new 19.2 kilobaud digital radio networks, and uses an RS-232 interface, and programs are available for both the C64/128, and IBM PC/Compatible for easier operation.

For those desiring RTTY reception on a more limited budget, one can assemble a demodulator out of an XR-2211 IC, and a couple support parts. This is a straight demodulator with no translation features whatsoever; which means you'll have to write some software for your machine in order to receive non-ASCII signals.

Antennas
========

There are various antennas out there. What is currently the rage in VHF/UHF receiving antennas is the discone. This omni-directional antenna, conical in appearance, presents a good match over the entire frequency range from 25-2000 Mhz., which is good enough to transmit over this range. They

cost about $70. For the budget minded person, and those seeking something more directional, one can pick up a TV yagi (beam) antenna at reasonable prices from Radio Shack, or any department store. They work well enough as is, but can also be modified for better reception. Figure EW-2 shows the dimensions for converting your basic VHF/UHF TV antenna into a VHF/UHF scanner antenna. When doing this modification, one should also remount the antenna so that it is vertical (just like the picture), as opposed to horizontal.

For the truly budget minded (almost destitute) person, one can assemble their own 1/4 wave vertical out of some pieces of coat hanger wire, and an SO-239 antenna connector. This is the exact antenna as the one described for cordless phones in the telecommunications techniques chapter. As a matter of fact, the dimensions described there work rather well for the VHF/Low band. For VHF/Hi and UHF, use a 19" length for the elements. It works.

Receiving antennas on shortwave are a different manner. With these, the best way to go is to make your own, as it really is too easy. For starters, get as long a length of wire (200'-300' is nice, but even 100' will do), and get it up as high as possible. Then add a good receiving tuner. Several manufacturers sell an antenna similar to this, usually a dipole with some traps. These work allright too, but the longwire is still your best bet as it works, and costs much less. One can also use commercially available ham shortwave antennas for the approximate band that most of their monitoring would be on. For those with very limited space there is also what is known as an "active antenna" which is a small (3'-5') whip antenna with an amplifier. I've heard a few ok reports about this, and in my opinion it's better than nothing if you have very limited space, although I would try as big of a longwire antenna as you can. With a long-wire, one can also run it inside along the ceiling molding, and still get a good length if one lives in an apartment, or similar situation.

Signal Types/Modes

There is quite a bit of stuff out there, and it's sent out many different ways, depending on the target service, and it's frequency. What this section will do is give you a run down on what's out there, where it is, and what it sounds like.

Voice:

FM - This is the most common mode used for commo in the VHF/UHF region. 90% of all voice commo in this region is sent out FM.

AM - Used mostly by international shortwave broadcasters, and for 90% of all Citizens Band commo. It is also used on the civilian and military aircraft bands. FM signals can also be received on an AM mode receiver by tuning to the side of the transmission. This is known as "slope detection".

SSB - Single Side Band. A form of AM which allows for a greater power with less wattage. This is used on the shortwave bands by non-broadcast "utility" transmissions (mostly government/ military), and for about 10% of Citizens Band commo. It is also the voice mode used by hams on shortwave. One can also receive AM signals on SSB by carefully tuning to the center of the signal until the hetrodyne signal disappears.

Non-Voice:

CW - Morse Code. Used mostly by hams and a few utility stations on shortwave. All a CW signal is, is an unmodulated AM carrier. It is basically received in SSB mode, where the signal is tuned slightly off center to provide a tone.

RTTY - Radio Teletype. Generic Term for digital radio commo. Sounds like

Jamming Equipment and Techniques

For wideband jamming, simply assemble the spark gap generator from the plans in this chapter. They work very well, and will make the RF spectrum within a mile of it's location almost unusable. For narrow-band jamming, it is necessary to procure a transmitter with the proper radio frequency, and PL (subaudible) tone frequency. The best way is to either steal the enemy's equipment, or acquire similar equipment, and change the frequencies and PL tones. For the field-expident type, get ahold of an RF sweep Generator with an external modulation feature, an audio sweep generator, an audio mixer, a proper antenna, and for extra power; and RF amplifier. Figure JAM1 shows the hook-ups. The way this works is that the RF sweep generator acts as a low power transmitter, which is amplified by the RF amplifier to make a pretty decent transmitter. You then mix your audio source (tape recorder, microphone, white noise generator, special-effects box, etc.) with the audio sweep generator set at low volume generating the PL tone frequency. And there you have it, a jamming set-up. Basically, when your jamming a radio signal, your operating an ordinary transmitter in a way that it messes up someone's communications network. and
have fun.

To protect your network from hac