TICOM

TECHNICAL INTELLIGENCE COMMUNICATIONS

Issue #3, April 2005

http://www.iirg.net/~ticom/zine/ – email: ticom@iirg.net

CONTENTS:

VHF/UHF Radio Communications Monitoring and Communications Intelligence (COMINT)

*"**Communications Intelligence** – Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called COMINT."*
– DOD Dictionary of Military and Associated Terms

Introduction

This work originally started as a series of messages on a BBS many years ago. It was later expanded into a text file, made its way to the Internet, and was published in a few hobbyist magazines. A few years have gone by since it was last updated, and some new developments in the hobby have occurred since then. With the advent of Ticom 'Zine I decided it was time to update and re-release this article to serve as a guide to all the scanner dweebs out there who aspire to reach higher ground.

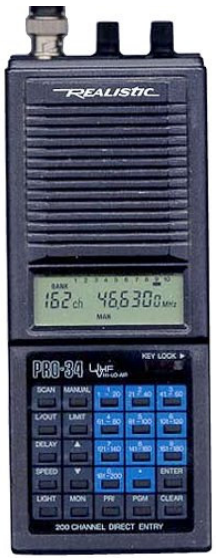
A common "police scanner" is one of the most potentially useful tools a hacker could have. Scanners have come a long way from bulky, crystal-controlled affairs with a handful of channels. Contemporary scanners fit in the palm of your hand, have a thousand keyboard-programmable channels, and have wide-band frequency coverage from 100 Khz. To 2+ Ghz. Certain models even have the ability to follow communications on trunked radio systems used by government and business, and can demodulate APCO-25 (P-25) digital modulation now becoming popular on both conventional and trunked radio systems. For the uninitiated, a scanner is a VHF/UHF communications receiver that has the ability to step through multiple channels or "scan", stopping on a frequency it detects traffic on. Scanners monitor frequencies used by government agencies, the military, public safety, emergency services, utility companies, businesses, and wireless telecommunications devices. Some of the more deluxe units even cover the "HF" shortwave region. While the use of mobile data systems and encryption is on the rise, there is still plenty of activity to be monitored for the foreseeable future.

Equipment

Generally speaking, the purpose of a full-scale COMINT set-up would be the following:

- RF spectrum search for new frequencies and fingerprint of local RF spectrum
- Monitoring of applicable local & regional RF activity

- Monitoring of local "indicator" frequencies that provide notification of unusual events or activity
- Monitoring of 1-50 "priority" frequencies of interest.
- Detection and monitoring of nearby RF activity
- Identification of previously unidentified RF activity.
- Recording of select RF communications.



With the exception of the newer models that feature P-25 demodulation and 2+ GHz. frequency coverage, 90% of your equipment needs can be acquired at a significant savings by purchasing it used. There is always Ebay for those who are willing to pay premium prices, buy equipment sight unseen, and deal with fascist policies undoubtedly created by lawyers. I much prefer checking out local hamfests, ham-oriented electronics stores (such as Lentini Communications and Ham Radio Outlet), and pawnshops. There is no way you would, for example, be able to buy a mint condition Icom R-10 for $100 or a $75 Radio Shack PRO-43 off Ebay. Yet, that is exactly the price my friends and I paid for them at local pawnshops.

There are some specific models of receivers that deserve specific mention. The first two are the classic Radio Shack PRO-2004/2005/2006 and PRO-43 base and handheld scanners. These units are considered to be the ones that started it all in respect to custom modifying scanner receivers, and were the focus of the Scanner Modification Handbooks written by the late Bill Cheek. Out of the three base units, the last in the series, the PRO-2006, is considered the "primo" unit. Another highly regarded unit is the Radio Shack PRO-26 handheld that featured full 25-1300 MHz. coverage when properly modified. Two other notable scanners are the Radio Shack PRO-2035 and PRO-2042. While post-1994 units, they were the first units to have prompted the discovery of the virtual downconverter mod, and were considered some of the last units that were easily customizable. Of the two, the PRO-2042 is considered the better unit. The Uniden/Bearcat BC-780XLT is yet another unit that should appear in used equipment circles and worth a look at. Icom and AOR communications receivers for the most part are always worth acquiring when found on the used equipment market, despite their high resale price. There exist many sites on the Internet that contain equipment reviews, and I recommend checking them out when you have a specific piece of equipment in mind. In the next section I have listed mostly pre-1994 scanners that were capable of being modified for full 800 MHz. coverage that you may use as a guide when looking for used equipment.

Full 800 MHz. Reception

The Electronic Communications Privacy Act and subsequent legislation has been a sore point with me since its inception in the 1980s. The ECPA is now approaching

Some classic scanners that would be of interest to the COMINT hobbyist. From top to bottom is the Radio Shack PRO-34, PRO-26, and PRO-2006. All of these units are capable of full 800 MHz. reception.

the twentieth year of its abhorrent existence, and remains an example of how idiotic this country has become. Back before the advent of Advanced Mobile Phone Service (AMPS) in the 800 MHz. region and when the 800 MHz. land mobile band (including cellular phones) belonged to TV channels 60-69, mobile phones used a handful of channels in the VHF and UHF land mobile bands. Mobile phone service was then called IMTS (Improved Mobile Telephone Service), and few people could afford it. The few users were well aware of the fact that people could listen in, and either spoke accordingly or didn't care.

When cellular phones came out, the FCC reallocated TV channels 60-69 for land mobile service and 666 cellular phone channels (later expanded to 832). Now mobile phone service became more affordable and available, and a larger segment of the population purchased them. Privacy concerns were raised, and congress with the help of bribes from the cellular phone industry passed the Electronic Communications Privacy Act that made listening to mobile phone communications illegal. At the time even the U.S. Justice Department stated that there was no way the ECPA could be enforced, but sellers of mobile phone service could now tell their potential customers that there was a law protecting the privacy of their unencrypted radio communications. At the time if I recall correctly there was no law prohibiting the sales of cellular-capable scanner receivers, but manufacturers cooperated by manufacturing receivers with this frequency coverage blocked. What was known among hobbyists is that the firmware was programmed to block coverage if a certain line on the receiver's microprocessor was active. This was so they could easily manufacture and sell full-coverage units to other countries. By cutting that particular control line, usually done by clipping the diode attached to the line, full 800 Mhz. coverage was restored.

This charade went on for a few years until the declining IQ of scanner dweebs and the increase in cellular phone usage resulted in a few instances of people getting caught doing stupid things as a result of what they heard from monitoring cellular phone conversations. It came out in public that the whole cellular privacy thing was a sham from the onset of the ECPA, and the Feds reacted by taking action against the special interest groups that would give them the least amount of hassle. The FCC in April, 1994 declared that they would not provide certification of any scanning receiver capable of being readily modified to receive cellular phone signals. Manufacturers redesigned their receivers, and other than some more complex (than clipping a diode) "virtual downconverter" modifications in a few models, that was the end of scanner cellular mods.

The relevance of all this to the present state of monitoring is that mobile phones have gone digital. The analog AMPS service was replaced with D-AMPS, and there is now Nextel and 1.9 GHz. PCS phone service; which are both digital. There now exists a surplus of analog cellular phones ranging from 3-watt bag phones about the size of a hardcover book, to portables that put out 300-500 milliwats. There are also decommissioned AMPS base stations available from various electronic surplus outfits. This obsolete equipment is being converted for various applications ranging from electronic surveillance to covert communications systems. It is not illegal as of yet to monitor communications of this nature, but currently manufactured receivers can not cover the frequency ranges. The use of a full 800 MHz. coverage receiver at present is not for monitoring mobile telecommunications, but for the more interesting stuff that's hiding in the same frequency range.

Due to the increase in trunked and P-25 digital radio systems, many of the average scanner dweebs are trading in their old equipment to be able to afford the new generation of digital trunktracker scanners. Since D-AMPS has eliminated all those "juicy" (read: boring to anyone with an IQ above 70) phone conversations that used to occur in the cellular phone band, they felt

no need to keep the equipment; especially when the state police have switched over to ASTRO trunking. This has resulted in an increase in the availability of older scanners with full 800 MHz. coverage. I wrote an article entitled "Cellular Interception Techniques" that appeared in the 22nd issue of the IIRG's Phantasy Magazine. The article is somewhat obsolete as it was aimed at monitoring AMPS, but there is still applicable information in it for those who want full monitoring access to the 800 MHz. land mobile band.

The list to the right contains all the Radio Shack and Uniden/Bearcat scanners that I was able to find a mod for continuous 800 MHz. reception. In addition to this list, Icom and AOR receivers made before 1994 are capable of being modified if they don't already have full coverage. Use this list when you are looking for used equipment at hamfests and pawnshops. When going the used equipment route, I'd say about eighty percent of the time when you find a model on this list it has already had the mod done to it.

Someone will invariably mention how certain models of AMPS cellular phones, particularly Motorola, can be placed into test mode and used as 800 MHz. cellular phone receivers. While that is the case, they can only monitor the base station output frequencies on the standard 30 KHz. channel spacing. They are unable to monitor the mobile input frequencies where one is more likely to hear something interesting, nor are they able to tune between the 30 KHz. channels. Certain models of VHF/UHF amateur radio transceivers are also capable of being modified for full 800 MHz. receive coverage, such as the early models of the Yaesu FT-50 and the Alinco DJ-580.

Radio Shack Handheld Scanners
PRO-26
PRO-34
PRO-37
PRO-39
PRO-43 (not the 20-0300A model)
PRO-46

Radio Shack Base/Mobile Scanners
PRO-2004
PRO-2005
PRO-2006
PRO-2022
PRO-2026 (not the 20-0148B model)
PRO-2030
PRO-2032
PRO-2035 (virtual downconverter)
PRO-2042 (virtual downconverter)

Bearcat Handheld Scanners
BC-200/205XLT
BC-2500XLT

Bearcat Base/Mobile Scanners

BC-760XLT
BC-780XLT (virtual downconverter)
BC-800XLT (factory default)
BC-855XLT
BC-8500 (virtual down-converter)

Finding Frequencies

Eventually, the serious scanner hobbyist gets the urge to go beyond listening to the standard widely available public safety and business frequencies. They get the desire to look for the good stuff that you will not find listed in the scanner frequency directories or FCC web site. The object of the hobbyist's listening might also be something mundane like the local mall security force, but a search through the directories fails to uncover their operating frequency. In either of these situations, the hobbyist can resort to using these techniques to acquire an elusive frequency.

There are two basic approaches to finding frequencies. The first approach is to go on an electronic fishing expedition. This is how hobbyists operate most of the time. You simply take a small piece of the frequency spectrum that your radio is capable of receiving and listen to see what you can find. The second approach is to pick a specific target to be the focus of your monitoring attention and attempt to find the frequencies they use. During the course of using this second approach you will find other users; which you might find

interesting later. I recommend that you use the first approach once in a while. Knowing the usual activity around you will help determine how far you can listen, and especially important, when a transmission out of the ordinary appears. I recommend you acquire frequency directories for your area. The most common one is Police Call. Police Call is available at Radio Shack or by mail order. It is excellent for public safety listings, but only average when it comes to identifying businesses. There are other excellent directories available for particular local areas.

The tool that every monitoring hobbyist has is the "search" function on his or her scanner. Most of them however, do not know how to use it. You should know the frequency band that your target uses. You should have an idea of where in that band they would be operating. You should search probable areas in small sections.

Knowing what band a target operates on could be a matter of general knowledge. If your local police's dispatch channel is on VHF-high band, then it is a good bet their unlisted tactical channel is also there. It can also be determined by looking at the antennas on vehicles; unless the vehicle has a disguised antenna. A VHF-low band antenna will be a 60 to 100 inch whip or a 35-inch whip with a 5-inch coil on the bottom. A VHF-high band antenna will be either an 18-inch whip or a 40-inch whip with a 3-inch coil on the bottom. UHF band antennas will be either a 6-inch whip or a 35-inch whip with a plastic band in the middle. 800 Mhz. antennas are either a 3-inch whip or a 13-inch whip with a "pig tail" coil in the middle. A cellular phone antenna is a common example. I suggest ordering the catalogs of various antenna manufacturers to get a visual idea of what antennas on each of the bands look like. You can do the same thing with handie-talkie antennas. A VHF-low band antenna will be about a foot long. A VHF-high band antenna will be about six inches long and about as thick as your index or middle finger. UHF antennas will be either 6 inches long and slender compared to the VHF-high band antenna, or three inches long. 800 Mhz. antennas are about an inch and a half long, or about a foot long with two different thicknesses.

Once you know the frequency band, you determine where in that band they might be operating. In most non-federal cases this is as easy as looking at the Consolidated Frequency List on the Police Call CD. The two types of users you might have problems with are police departments and the federal government. Police departments can use any public safety frequency for "tactical" communications on a non-interference basis. The FCC now also categorizes all public safety agencies into a single frequency pool. The Intergovernmental Radio Advisory Committee (IRAC) handles licenses for the federal government. IRAC listings have been exempt from the Freedom of Information Act since 1983. The mundane agencies have been using the same frequencies for the past 20+ years, but some of the more interesting ones have changed frequencies. The IRAC listings in the Consolidated Frequency List are still fairly accurate. Remember that they are only fairly accurate.

You should search a range that covers three to five seconds, and with the scanner's fastest speed. This seems to be the average duration for a radio transmission. Let us say you are searching the VHF-High band with a scanner that does 50 steps a second. Channel spacing for VHF-high band is 5 KHz. You should search your target areas in sweeps of 750 KHz. to 1.25 MHz. Search a range for one to two weeks at different times; to catch everything in that range.

One little known trick is to use one of those old tunable public safety band receivers that predate scanners. An example would be the Realistic PRO-2. It covered 30-50 MHZ. and 152-174 MHz. You can pick one up at a flea market or hamfest for as little as $5. While these units lack the sensitivity and

selectivity of a scanner, they are excellent for doing high-speed searching. Once you get a hit, you will have narrowed the possible frequency range down to roughly 500 KHz. You then use your scanner's search function to find the exact frequency. They are also good dedicated single channel receivers for things like NOAA weather radio and the local fire department's dispatch frequency. If you ever find an old multiband portable that covers UHF-TV, remember that channels 70-83 are now the 800 MHz. public safety, business, and cellular phone band.

A frequency counter is a useful tool for the COMINT hobbyist. A frequency counter works by locking on the strongest radio signal in an area, and displaying the frequency. Until recently, I was recommending the Optoelectronics Scout frequency counter because of its features that make it useful for COMINT. Recently, I became aware of other brands of frequency counters that will accomplish the same task at almost half the price. One such brand is the Aceco FC3000 series of frequency counters that are also sold under other names. The useful feature of these counters is a CI-V interface. This is essentially a TTL serial interface and command language that enables the counter to connect to a PC for automatic frequency logging, or to a receiver for reaction tuning. Reaction tuning is a feature in which the frequency counter automatically tunes a CI-V equipped receiver to the frequency it detects. Most computer controlled Icom receivers (such as the R-10) are CI-V equipped. AOR receivers have a different command language and interface, but both the Optoelectronics Scout and Aceco counters are capable of switching between the two. The second issue of Ticom 'Zine has an article on interfacing frequency counters to a PC for logging hits.

Frequency counters work in a radio signal's near field. This means that you will generally have to be within a couple hundred feet of the target transmitter in order to acquire the frequency. The table to the right shows the average distances one will acquire a particular type of transmitter:

Transmitter	Distance
1.2 GHz. 3 watt radio	25 feet
870 MHz. 3 watt Cellular Phone	150 feet
UHF 1 watt radio	200 feet
FM Wireless Microphone	10 feet
VHF-high band 1 watt radio	90 feet
46/49 MHz. cordless phone	20 feet
27 Mhz. 5 watt CB	40 feet

There are a few things you can do to enhance a frequency counter's operation. The first technique involves antenna usage. The standard telescoping whip is good for many operations, but you can do better. With the standard whip antenna, the Scout will pick up a cellular phone at approximately one hundred fifty feet. Hook it up to a 5/8 wave 800 Mhz. antenna, and the range increases to approximately three hundred feet. A high-gain antenna designed for the band of interest will increase your range on desired frequencies and reduce interference from undesired ones. If you use a directional antenna, such as a yagi, you will be able to select a particular target location to investigate, and eliminate interference from another location. The second technique is using filters. Using filters will block out undesired frequency ranges and pass desired ones. An FM broadcast notch filter is very useful. Optoelectronics sells the N100. FM broadcasters are a major source of undesirable interference, and having one nearby will cause your counter to lock up on the broadcast station's frequency.

There have been recent scanner models such as the Radio Shack PRO-83 and Uniden Bearcat BC-246XLT that feature a near field signal detection mode. They offer an advantage to the frequency counter/reaction tune receiver combination in that the signal detection range is greater, specific annoying frequencies can be locked out, and the region of RF spectrum searched is limited to the frequency coverage of the scanner. The units are also less

expensive than the frequency counter/reaction-tuned receiver combination. The primary disadvantage is that the lack of full-range frequency coverage means you will not detect a signal in some odd portion of the spectrum. One high-end unit does lack this disadvantage. The Alinco DJ-X2000 handheld communications receiver has a near-field detection & tuning mode and features "DC to daylight" frequency coverage (minus cellular, of course). I recently had the opportunity to evaluate a Radio Shack PRO-83 (made by Uniden), and was fairly impressed with its signal stalker performance. With a 5/8th wave two-meter mag-mount on the roof of the car, it was able to detect a 169 MHz. wireless microphone from a distance of about 100 yards while driving down the road. A similar range was also experienced testing the unit with an old AMPS cellular phone mag-mount and some Part 15 devices operating in the 902-928 Mhz. garbage band.


PRO-83

By using these techniques, you will find the frequencies you desire. How quickly you find a frequency depends on your skill as a COMINT hobbyist and how much the target uses their radios. You can acquire a target such as a mall security force in as little as thirty seconds. This was how long I had to loiter near a help desk with a frequency counter before a security officer keyed up a radio. Some of the less active federal agencies can take a week or two before you can tag them. If you do not find the frequency, there are two possibilities. The first is that your target either does not use radios or uses them very infrequently. I will assume that your target does indeed use radio communications. The only solution to tagging an infrequent radio user is persistence and patience. Eventually they will key up and you will have their frequency. The second possibility is that you found their frequency, but failed to identify it properly. Learn who operates on what frequency ranges. Listen to what frequencies you have found during previous COMINT attempts over a period of time. My COMINT experiences have taught me that sometimes the true nature of the parties using a frequency may take a while to become apparent. Certain users use encrypted or spread spectrum (frequency hopping) communications. Until recently, it was thought that receiving spread spectrum communications was beyond the ability of the average hobbyist. Then the first issue of TICOM 'Zine came out. With the right equipment and under the right conditions it is possible to not only detect but also monitor FHSS communications. Refer to TICOM 'Zine issue #1 for more information, available via http://www.iirg.net/~ticom/zine or check a search engine. Encrypted communications present a low to almost impossible technical difficulty in regards to cracking them, and are also illegal to listen to under the Electronic Communications Privacy Act. Encrypted communications system users will sometimes have equipment difficulties and operate in the clear. A patient listener will wait for this opportunity.

Introduction to Signal Analysis

I will assume that you, in the course of your COMINT endeavors, have come across a genuine unidentified ("unid") user while searching the spectrum. You've checked all the scanner frequency lists, e-mail lists, web sites, and Usenet postings and have come up with nothing. You wish to identify the unid, and determine the extent of its communications network. To do this, you ask the following questions:

- Frequency (or talkgroup/subfleet if monitoring a trunked system)
- PL/DPL tone, if any? Single PL/DPL used, or multiple?
- Encrypted or clear? Type of encryption: digital or analog?
- How many stations do you hear?
- How do they identify themselves?
- Signal strength of stations communicating?

- What are they talking about?

The first five characteristics are noted as soon as you discover the unid. You will have some initial information about the others, but as time goes on you will acquire more information. What you should be doing now is noting what information you do have on the unid. Some people like using a computer database, others like 3x5 index cards. The more info you have, the easier it'll be to identify the unid.

The frequency in question can help tell you the approximate range, extent and purpose of the unid's communications net. For example, the VHF low-band would likely be used for regional communications between base stations and maybe mobile units. UHF on the other hand, would be for short-range tactical-type communications between several mobiles and portables. UHF portables are limited to a few miles. A VHF low-band base station can communicate a couple hundred miles under the right circumstances. What other identified users operate on nearby frequencies? For example, the Connecticut State Police employ several frequencies in the 42 MHz. Region that they are licensed for. They also use a number of frequencies in the same region for covert purposes that are not licensed. When the band conditions are right and the skip comes in you'll hear both their operations and SP communications from across the country on the same frequency.

PL/DPL tones are another identifier. Knowing the PL/DPL tone of an unid enables you to cross-reference it to other frequencies. If a police department uses a certain PL on their repeater, and an unid with surveillance activity is noted on the same band with the same PL, then it's quite possibly an unlisted channel for that police department. Knowing how many different PL/DPL tones are in use on a given frequency tells you approximately how many different nets, or distinct groups of communicators, are active on that freq. On a low-power portable frequency such as 154.600 MHz., users will use a "unique" PL/DPL tone so they don't have to hear everyone else. There are only a limited number of PL/DPL tones however, so duplication by different nets is inevitable. Other users won't want to spend the extra money for radios with PL/DPL capability, run without it, and tolerate the other users on the channel breaking their squelch. If you hear an unid running DPL, then you can be 99% sure they are running real "commercial land mobile" equipment. There are only a couple ham rigs, such as the Yaesu FT-50, that have DPL.

Most radio communications businesses maintain commercial trunked radio systems and the occasional community repeater. The license for the system is in their name, and they rent airtime to various businesses and organizations. The individual users will not be licensed; instead running under the radio shop's license. Each subscriber will be assigned his or her own talkgroup on the system, or PL/DPL tone on the repeater. Motorola sold all their commercial SMR systems to Nextel who took them off the air and replaced them with iDEN (digital) systems. This prompted many radio users to seek out alternatives to Nextel. Many radio shops have set up LTR trunked systems, which have replaced their community repeaters for the most part. LTR is an open protocol. This not only means a wide availability of equipment for the business offering these services, but equipment for the monitoring enthusiast as well. There are also a few commercial SMRs running the GE/Ericsson EDACS system on 800 MHz. Each system can have several dozen users on it, making them a nice challenge for the monitoring hobbyist who wishes to map them out.

If an unid is encrypted, you will at least know whether or not the encryption method is analog or digital. If they are using a simple single-frequency inversion method, then it is possible, although illegal, to decrypt their communications and proceed. If they are using something advanced such as DVP, DES, or Rolling Code then you will not be able to monitor the actual communications. You will still at least be able to note how often the

frequency sees activity, and the signal strengths of the stations communicating. Voice encryption is often subject to failure, and you might catch a station operating in the clear if you monitor long enough. DIY-types should note that single band frequency inversion is the same system used in the Ramsey Electronics SS-70A.

At this point, you have all the immediate characteristics of the unid noted down. The rest is just a matter of time. The remaining questions you have in identifying the user are:

- How many stations do you hear?
- How do they identify themselves?
- Signal strength of stations communicating?
- What are they talking about?

All these will eventually answer the main question, "Who am I listening to? The best thing to do at this point is take a receiver and dedicate it to the given frequency. You can acquire basic 16-50 channel scanners for under $100 at flea markets, pawn shops, and hamfests for this purpose. If you want 24 hour monitoring of the frequency, attach a VOX-operated tape recorder to the scanner. Many scanners come equipped with a "tape out" jack for easy connection. Otherwise, go to Radio Shack and pick up one of the suction cup telephone microphones. This is attached to a telephone receiver by the earphone to record phone calls. Attach it near the speaker of the scanner. Experiment to find the best place to attach it to the scanner. For those of you who really want to get into things, the late Bill Cheek's Scanner Modification Handbooks contain a wealth of information on modifying your scanner to make COMINT easier. You can add event counters to see how many times the frequency breaks squelch, time-stamping for monitored communications, and a whole host of other enhancements.

You will be able to initially discern IDs used on the frequency and the signal strength (even if approximate) of the stations on the net. You will also know what they are saying if it's in a language you can understand, although you might get a little tripped-up on any specialized jargon. Log it all down. Eventually you'll also be able to recognize the voices of the various people on the frequency, and match them to IDs. The signal strength of each user will tell you how approximately how far away they are from your location, and whether they are base or mobile/portable stations. Consistent signal strength will indicate a base station or repeater. Mobile and portable stations will have varying signal strengths and often "mobile flutter" on their signal.

When listening to an unid with the intent of identifying it, two things you should listen for are locations and specialized trade jargon. They can be cross-referenced to assist in identifying the user. Street maps of your nearby locales are good reference to have. I don't advocate "call chasing", going to the site of an incident that you've heard on your scanner. This can be dangerous, and complicates matters for public safety personnel who are working the incident. If however, you've determined you are listening to an obviously civilian unid on a trunked system or community repeater who was just sent on a service call to a location that's a few blocks away from you, it would be a different matter. It would be worthwhile to take the dog for a quick walk to see whom you are listening to. On that note, information you discover on community repeaters or trunked systems is transitory in nature. The talkgroup or PL may belong to a different business next month.

If you listen long enough and pay attention to the communications you are receiving, you will identify the user. The amount of time will vary with the nature of the user, and how often they are on the air. Once you identify the user, the rest is up to you. You can become quite intimate with the operations of a business by monitoring their communications. Monitoring local public safety communications will often give you a better handle on what's going on

in your community than the local newspaper. The possibilities are endless. As an intellectual exercise your COMINT endeavors will be delving into such diverse areas as electronics, geography, sociology, research skills, and current events. At any rate, COMINT analysis is far better a pastime than sitting in front of the television (although having Fox News running in the background while you're working on something is a good idea). Chances are, you'll have some questions regarding communications systems or activities in your locale that could be answered by using COMINT analysis. Some questions that might come to mind are:

- Who are the users of local community repeaters and SMR systems?
- What are high crime areas in my community?
- What are the most common crimes in my community?
- What is the reliability of the local utility infrastructure (electrical, telephone, CATV, gas)?
- "X" is obviously employing radio communications, but no license is listed for them. What's their frequency?
- What frequencies and/or radio systems are the local public safety agencies using other than the publicly listed ones?

The best way a beginner can start is to just do it. Pick something, like a local community repeater or SMR system, and see how much information you can acquire on it. You might have some specific questions regarding a communications user or system you already have some information on, which you can go investigate. You might even be interested in something non-technical, such as crime statistics in your local community. Whatever your specific interest happens to be, remember that patience and persistence is a good thing.

Excerpts From FM 34-45
Tactics, Techniques, and Procedures
for Electronic Attack

The most-recent issue of a certain pusedohacker magazine featured an article on electronic warfare that was bogus. The author claimed to have been trained in EW, and I would like to see his MOS training certificate from Fort Huachuca or Goodfellow Air Force Base. He claims that the military publishes no EW manuals, so therefore is unaware of the U.S. Army's FM 34-series that covers intelligence and electronic warfare operations. He also claims that specific information is "classified". That reminds me of the old military joke "My job is so classified, that not even I know what I'm doing." While one is required to hold a "Top Secret/Specially Compartmented Information (TS/SCI) clearance in order to have a 98 series MOS many EW manuals are not only unclassified, but also have an "Approved for public release. Distribution is unlimited." distribution restriction. Having run some of the terms he makes use of in his article through a search engine, I find almost no mention of them on any website that I would take seriously. This article is an example of something that looks good on the surface, but in reality is pretty much useless. In the interest of providing the hacker community with correct and useful information at a price everyone can aford, I'm reprinting selected excerpts from U.S. Army Field Manual FM 34-45 Tactics, Techniques, and Procedures For Electronic Attack, that I feel may of interest to my readers. This manual is unclassified, and available from different places on the Internet. Those of you who are interested in downloading and reading the whole manual can do a Google search and find it in PDF format easily enough.

DEPLOY ELECTRONIC SUPPORT AND ELECTRONIC ATTACK ASSETS

GROUND MANPACK PLATFORMS

5-12. Manpack collection teams can be deployed alone or in conjunction with other elements. Independently deployed assets will have the additional responsibility of team security and added supply considerations.

Ground Manpack System

5-13. Manpack collection systems provide the commander with unique capabilities when conducting initial entry, stability operations, and support operations. Found in both light and special operations forces (SOF) units, manpack systems have characteristics not found in vehicle systems. Manpack systems are characterized by the following:

- Deployable in areas that are normally not accessible or usable. This access can be constrained by threat forces and/or routes to site. The manpack allows the commander to place teams in areas where vehicle mounted equipment would present too large of a footprint and terrain is too restrictive for air assets. Due to this, manpack systems are often close to or past the forward line of own troops (FLOT).
- Manpack systems also have a lower battlefield signature due to placement and equipment. Thus they can be used in more low-profile operations and are especially helpful in urban situations.

5-14. Limitations of manpack systems:

- Very limited mobility of collection teams.
- Teams may have to rely on outside assets (airlift in most cases) to deploy on the battlefield.
- Manpackable systems are usually not netted, so DF will be limited to lines of bearing (LOBs) from each system.
- Collection teams will be limited on mission duration (normally 3 to 5 days) and METT-TC dependent.
- Current reporting may be limited to voice communications or short data bursts depending on equipment.

- Limited communication link, high security requirements, difficult resupply, and deployment asset.

Special Considerations

5-15. Special considerations must be made for small low-level voice itercept (LLVI) teams which will be deployed close to the FLOT if not beyond it. These teams are dependent upon stealth for battlefield survival. The teams will usually be inserted by air, either air assaulted in or jumped in. Slow movement due to the weight of these small systems will make security escorts hard to plan and coordinate. For these sites, situational awareness is imperative. Evasion plans are briefed and planned with rally points and extract points fully detailed. If contact is made, team members will move as a group or as individuals back to the predesignated points.

COLLECT ELECTRONIC SUPPORT DATA

5-23. Collection of ES (communications intelligence [COMINT]) data falls into two categories: voice and digital or analog data. This data will be used to identify and target receivers for EA.

COLLECT VOICE DATA

5-24. This function has six subfunctions that when combined and analyzed provide intelligence on targets and nodes for the effective use of EA against these nodes.

Intercept Signal

5-25. ES systems will search across the spectrum for enemy communications (either voice encrypted or clear).

Target Acquisition

5-26. Collection for target acquisition is the process where the ES system has been given specific tasking to locate a particular target. It can be as simple as finding a particular frequency to provide orientation data for an EA system. Or it can be as complex as searching the full spectrum for a particular entity that has met the criteria for EA. The ES system then tips that frequency and location to an EA system for attack. The length of time that it takes the ES system to fulfill the tasking is directly tied to the amount of technical data that is supplied with the tasking. The ES system that has been tasked to provide tip-off data is also usually tasked to monitor the effectiveness of the attack. The tasking for this type of mission originates in the ACE and is refined by the GS or DS company POC prior to being sent to the system.

Gist Signal

5-27. The operator will provide the gist of the communication; callsign, ID nets (for example, artillery, infantry).

Locate Target

5-28. This subfunction will be performed either by the system which is netted or by the POC team using numerous LOBs.

Analyze the Signal and Build a Database

5-29. This subfunction will be performed primarily in POC and above by 98Cs to build net diagrams for the precise delivery of EA to delay, disrupt, divert, or deny spectrum to enemy.

Report Collection Results

5-30. Operators will report collection data as soon as possible to expand the SIGINT base.

COLLECT DIGITAL OR ANALOG DATA

5-31. This function has seven steps that somewhat mirror the subfunctions of collecting communications data.

Intercept Digital Analog Signal

5-32. Operator will scan and identify signal (for example, digital artillery nets).

Record Digital/Analog Signal

5-33. Operator will record the signal and make notes about the type of signal.

Identify Emitter Parametrics

5-34. Operators identify signal strength and width.

Identify Emitter Function

5-35. This step is completed by the POC team or higher through enemy historical data and threat models.

Locate Digital or Analog Target or Build Digital or Analog Database

5-36. This step is also performed by analyzing data at the SIGINT team level.

Report Digital or Analog Collection Results

5-37. This step is performed by the operator along with sending the recording back to the SIGINT team.

COLLECTION FOR DATABASE DEVELOPMENT

5-38. The collection manager develops clear, precise, and valid tasking to support targeting. In order to maximize collection, the EWO will coordinate with the collection manager to ensure the EW target annex is integrated into the collection plan for ES. Information obtained from this collection will help update local and national databases in order to perform situation development.

5-39. Collection will be geared to support the PIR and IR and the current operation. The collection manager can follow one of several methodologies when developing the EW target list (EWTL). These methodologies vary from EW support to targeting to collection for threat database development.

5-40. The collection manager can focus tasking by threat operating systems. The collection manager plans collection based on the operating system that he feels will be most beneficial to support PIR (for example, artillery, maneuver units, reconnaissance units).

5-41. Tasking is based on known frequency, callsign, net characteristics, or signal characteristics. Characteristics can determine the importance of a net. Example: If an artillery command observation post (COP) were known to operate on a specific frequency, that frequency is included in the tasking. Tasking is based on geographical location. Signals may be of particular interest if DF places it in an area that is of specific interest.

SEARCH TECHNIQUES

5-42. There are three main techniques of acquiring target emitters. They are **spectrum searches**, **band or sector searches**, and **point searches**. These techniques are best used combined, not independently. The techniques employed will depend on the mission, the number of assets, and their capabilities.

SPECTRUM SEARCH

5-43. A spectrum search entails a detailed mapping of the entire spectrum that is exploited by a particular system. This search provides an overview of the amount and type of activity and where in the spectrum it is located. No detailed processing is done on signals. The amount of time to identify the signal and produce an LOB or fix is kept to a minimum. This search technique is best used to first establish what activity to exploit. Spectrum search allows a single asset to locate and exploit emitters to fulfill mission requirements. In a multiple asset system, one position should always conduct a spectrum search to acquire new targets.

BAND OR SECTOR SEARCH

5-44. A band or sector search follows the same guidelines as a spectrum search but is limited to a particular segment of the exploitable spectrum. By limiting the size of the search band, the asset can improve the odds of acquiring a signal. This technique is used only in multiple asset or position systems. This search will allow for the development of new targets.

POINT SEARCH

5-45. The point search technique is used when a list of specific targets is provided for monitoring or exploitation. This technique allows for in-depth, long-term exploitation of signals in a defined environment. Point search should be used only after a thorough map of the environment is completed and in conjunction with a spectrum, band, or sector search. This technique is used to tip-off preplanned targets to EA assets.

CROSS CUE

5-46. When an ES asset acquires an EA target (for example, preplanned or target of opportunity), the ES asset is responsible for tipping the target information to the EA asset.

5-47. The EA ground systems have the capability to use either an omnidirectional antenna or a log periodic antenna (LPA). The difference is that the LPA increases the effective radiated power and the power is focused along a general azimuth. In order to use the LPA, the EA system operator must know the approximate target location prior to the start of the EA mission. This is one way the ES system supports EA missions

5-48. The EA aerial systems have only omnidirectional antennas. With both types of EA systems, the ES assets provide support by providing target acquisition, target tip off, target monitoring, and jamming effectiveness.

TA TEAM

5-49. The TA team will verify and assist the ES assets in target detection. The TA team will take the notification of a target from the ES asset and verify the target with the AGM or EWTL. If it is a valid target, the TA team will notify the ES asset in order to pass the target to the EA assets.

5-50. Along with tasking the EA assets, the ES assets are tasked to monitor the target in order to quickly identify information that would lead to valid targeting. Because information is time sensitive, quick reporting is vital.

5-51. The minimum information that needs to be passed to the EA assets are frequency, location of target, and signal characteristics (if available). This enables the EA assets to acquire the target and position their antennas in the correct azimuth.

PROCESS SIGNALS INTELLIGENCE DATA

5-52. The processing of SIGINT data will create and redefine the baseline of intelligence necessary for the commander to envision the threat, both current and future. The data produced by this process will provide support to targeting, SIR, and numerous other products to the commander. The processing of SIGINT data takes place at all levels of ES, from the ES asset operator to the SIGINT team and collection manager. The focus of the manual is on EA but it provides a brief overview of the process of intelligence as it applies to EA.

5-53. ES assets will transmit collection data via tactical reports (TACREPs) to the TA team. The data will include signal type, target identification, and gist of target activity.

5-54. The TA team will process the ES data, fusing the data to develop a battlefield picture and provide support in either a GS or DS mode. The TA team will provide limited processing using support from the SIGINT team via ASAS, doing limited work on simple voice matrixes, and using the OB and the EOB. These tools, along with intelligence disseminated by the ACE, provide a source for intelligence support to units supported in a DS mode.

5-55. The SIGINT team will further process ES data, having feeds from both the TA teams and, under certain circumstances, the ES assets. The data processed will depend upon numerous factors. Upon support from higher to decrypt communications data and intelligence feeds, the SIGINT team will also use the OB, EOB, and doctrinal templates to determine threat intent and actions.

5-56. The SIGINT team and the TA team will provide target data to FS channels. Using the ISM, these teams provide priority to targeting requirements to ensure intelligence is provided in a timely manner to engage HPTs. These targets may be engaged by either lethal or nonlethal fires.

SITUATION DEVELOPMENT

5-57. It is crucial that information pass between elements as quickly and as accurately as possible. Information development data will be passed from the ACE, down to the ES and EA assets, in the form of technical data and tasking. Technical information that is developed at the ES asset is also passed directly to the EA asset (as well as to the ACE) to help with database development.

5-58. Once the ES system has acquired the target, the operator must disseminate the information to the EA system. This is done most frequently with voice communications. The

data needs to include the frequency, location, and signal characteristics. The ES system operator also notifies higher headquarters that the target was acquired and that the necessary data was transmitted to the EA system. If the ES system fails to acquire the target, the ES system operator must notify higher so that the tasking can be shifted or changed.

ELECTRONIC ATTACK EFFECTIVENESS

5-59. During an EA mission, the ES asset will monitor the target to provide feedback to the EA asset and to provide the analytical element with an effectiveness report. The purpose of feedback is to keep the EA asset apprised of the status of the target. The immediate notice of changes to the frequency, location, or signal characteristic is vital to the success of the EA mission.

5-60. When a mission is completed, the ES or EA asset will send the analytical element a detailed effectiveness report in the form of a jamming effectiveness report (JER) or multiple assets effectiveness report (MAER), which will be sent digitally or by voice. This report will include the effects on the target from the perspective of that ES or EA asset. It includes but is not limited to frequency, location, signal characteristics, effects observed, and duration.

CONDUCT ELECTRONIC ATTACK

6-5. This operation has three functions. **Acquire target**, **reappraise and apply jamming equation**, and **jam target**.

ACQUIRE TARGET

6-6. This function has three steps: **Confirm target technical parameters**, **monitor target frequency**, and **confirm target acquisition**.

Confirm Target Technical Parameters

6-7. This step consists of three tasks:

- Confirm target frequency. The team leader will confirm with the TA team or POC the specific target frequency and ensure if jump frequencies were used that they were provided with jump sequence and correct jump frequencies.
- Confirm spectrum scan segments. The team leader will next use the scan function on the system to determine the exact frequency. This process is done because recalibration of a system is rare and the frequency may not correspond exactly.
- Confirm continued monitoring of target. The operator or team leader will confirm with the TA team the continued monitoring of targets.

Monitor Target Frequency

6-8. This step has three interrelated steps:

- Monitor designated frequency. The operator will monitor the frequency.
- Monitor designated scan sectors. The operator will monitor the particular sectors to ensure the system is still on target for the exact frequency.
- Revisit target frequency. The operator will periodically check on the target. How often the asset revisits the target is determined by the number of targets and the SIGINT team.

Confirm Target Acquisition

6-9. This step has four sequential steps:

- Acquire signal. This task is covered in the previous section.
- Identify signal. The operator will identify the particular signals with data passed by the SIGINT team.
- Confirm signal is designated target. The operator will use this data to confirm that the target is the same target passed by the SIGINT team. Examples of this confirmation would be callsigns, jargon, language, and essential elements of information.
- Confirm signal is preplanned target or target of opportunity. The operator will confirm that the target is either a preplanned target or a target of opportunity. This task is the last confirmation that the target is the correct target.

REAPPRAISE AND APPLY JAMMING EQUATION

6-10. This function will be performed by the SIGINT team to ensure that the EA asset can acquire the target and the target will be within range of the EA asset. The jamming equation will give the SIGINT team a range of each EA system with regard to particular emitters and receivers. Doctrine and equipment capabilities dictate quick and overpowering EA attack; therefore, this equation is not used for minimum power. An example of this are targets of opportunity. The EA team will not have the time to perform the equation and fine-tune the EA asset to hit the target with minimum power (minimize the asset's signature). The requirement for this technique is no longer valid because these assets deliver quick overpowering attacks.

JAM TARGET

6-11. This function has four steps.

Review Jamming Control

6-12. This step will ensure that there is a "stop jam" frequency being monitored by the system.

Program Jamming Power Output

6-13. This step will pass from the tasker to the jammer the power output for the system. This step is usually bypassed with the assumption that maximum power for precise overpowering EA will be used.

Jam Target Using Predetermined Techniques

6-14. This step will direct the EA system in the particular techniques to use. There are four basic techniques: **deception**, **jamming**, **masking**, and **DE**.

6-15. **Deception.** EM deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information to an enemy or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. There are three primary types of EM deception:

- Manipulative EM deception, which involves actions to eliminate revealing or to convey misleading EM telltale indicators that may be used by hostile forces.
- Simulative EM deception, which involves actions to simulate friendly, notional, or actual capabilities to mislead enemy forces.
- Imitative EM deception, which introduces EM energy into enemy systems that imitate enemy emissions.

6-16. **Jamming**. EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the purpose of preventing or reducing an enemy's effective use of the EM spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. Jamming falls into two categories, voice and digital (analog) data. Communications jamming is targeted against hostile voice systems for multiple purposes:

- To introduce delays into the enemy's C_2 system that allows the friendly commander to fully exploit his options.
- To delay hostile time-sensitive information until it is no longer useful.
- To force the enemy (in conjunction with ES) into actions that are useful to friendly operations. An example of EA forcing the enemy into action useful to friendly operations out of encrypted communications through jamming allows ES to gather intelligence from this otherwise secure net and further develops an intelligence baseline.

There are three primary types of EM jamming:

- Spot Jamming. Spot jamming may be directed at a single frequency or multiple frequency through sequential spot jamming and involves jamming various frequencies one at a time in sequence. Simultaneous multispot jamming involves jamming several frequencies at the same time. In both spot and sequential spot jamming, the full power of the jammer is directed against one frequency at a time, increasing the effectiveness and range of jammer. Spot jamming is less likely to interfere with friendly communications because receivers and transmitters can easily avoid it by slightly changing (detuning) the frequency they are receiving.

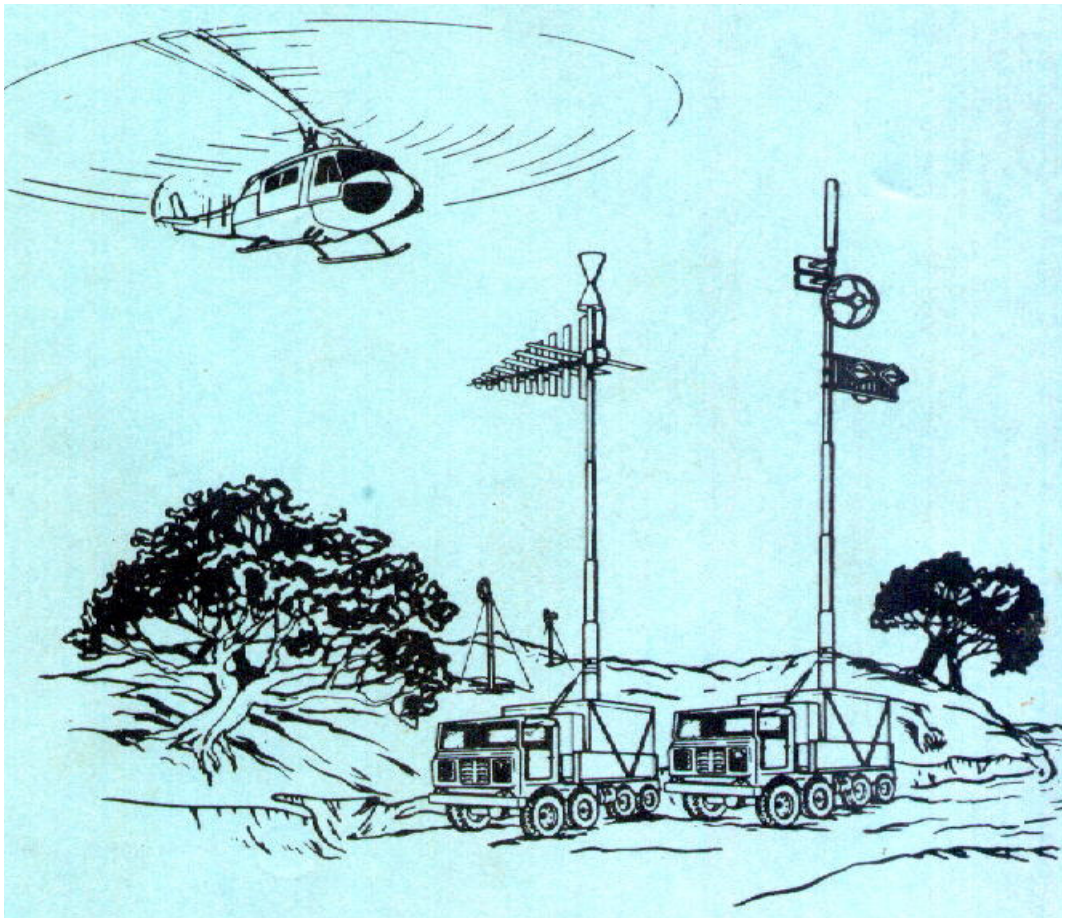
- Sweep Jamming. In sweep jamming, the jammer goes through a frequency range, then repeats the sweep continuously. All frequencies in the range are jammed. Friendly frequencies may be affected unless protected by the Joint Restricted Frequency List (JRFL).
- Barrage Jamming. Barrage jamming, unlike spot jamming, simultaneously spreads the jammer's power over a larger portion of the frequency spectrum, thereby reducing radiated power directed at any single target frequency. Barrage jamming is similar to sweep jamming, since all frequencies are jammed within the targeted portion of the spectrum.

6-17. **Masking**. Electronic masking is the controlled radiation of EM energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy ES without significantly degrading the operation of friendly systems.

6-18. **Directed Energy.** DE is an umbrella term covering technologies that relate to the production of a beam of concentrated EM energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to damage or destroy enemy equipment facilities and personnel. Directed energy warfare (DEW) is military action involving the use of DE weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel; or to determine, exploit, reduce, or prevent hostile use of EM spectrum through damage, destruction, and disruption.

Report Inability to Locate Target

6-19. The operator reports the inability to locate the target and therefore to queue ES assets to search for the target or to pass targets to other EA assets.



On the topic of intercepting frequency-hopping signals, Joe Loritz (GBPPR) writes on the LCWN list http://groups.yahoo.com/group/lcwn/:

> *I found another interesting piece of RF test gear:*
>
> *2-Way FM Radio Tester (FC5001)*
>
> *The FC5001 is a two-way FM radio tester that has the ability to automatically and almost instantly lock on to any FM signal within its frequency range. FM signals are demodulated and output through its internal speaker or external earphone. The high sensitivity to nearfield signals makes it ideal for RF security, counter-surveillance and radio communication testing applications. Supplied complete with internal NiCd pack, AC wall charger, VHF/UHF flexible antenna and audio earphone.*
>
> *It's available from Circuit Specialists for only $99.*
>
> http://www.circuitspecialists.com/prod.itml/icOid/8095
>
> *I'd love to slap an old MMDS downconverter on it to see if will follow frequency hopping 2.4 GHz cordless phones.*

A quick nod goes to the individual from the U.S. Army Material Command Army Research Laboratory http://www.arl.army.mil/ who was checking out the 'zine. Someone originating from that organization's IP discovered Ticom 'Zine while doing a Google search on "survivalist articles". I spent some time down at APG, and it made me appreciate New England even more. It's just too bad we don't have the Waffle House up north. While on the subject of places down in that direction, if you ever find yourself in New Castle, Delaware by the airport, go check out the Air Transport Command Restaurant. You won't be disappointed, unless you're a vegehead. "Vegetarian: Old Indian word for "bad hunter."

As a reminder for those readers who live in New England, Hosstraders is coming up. Hosstraders is one of the best hamfests in the Northeast, and one of the 'fests I attend regularly to find neat shit. The next Hosstraders is going to be May 6th & 7th in Hopkinton, NH. Their website is at http://www.qsl.net/k1rqg/ for those of you who want more information. Hamfests are an important source of inexpensive used equipment for hackers. Hackers in New England can keep informed about upcoming 'fests via the **New England Area Ham - Electronic Flea Market List** available at the following websites:

http://flealist.senie.com/
http://mit.edu/w1gsl/Public/ne-fleas
http://www.k1ttt.net/flea.html
http://www.connix.com/~wz1v/ne-fleas.html
http://www.k1dwu.net/flealist.html
http://www.mmra.org/~mmra/flealist.htm
http://www.qsl.net/vhfnews/ne-fleas.html
http://uhavax.hartford.edu/~newsvhf/ne-fleas.html