Issue #10 - March/April 1995

Cybertek

Technology, Security, Self-Reliance

Published by OCL/Magnitude, P.O. Box 64, Brewster, NY 10509

Editorial:
Looking Back: The Past Five Years

This month Cybertek celebrates it's Fifth Anniversary. I'd like to thank (in no particular order) my subscribers, my writers, Necross Sinister, John Williams of Consumertronics, "A.W.J.", Charlie, my parents, Benny Gillette, The Black Manta, Hanover Fist, The Datamaster, Peter Pulse, Glen Roberts of Full Disclosure, Malcolm Tent of Trash American Style, The Other Bookstore, Ignatious T. Foobar of Uncensored BBS, Rev Xidexx Unisexx, Wildfire Longstride, Wildflower, Bleach, S.V.M., Brian Oblivion, Count Zero (both of them), RL/RDT/L0pht Heavy Industries, Mercenary, Anubis, Ionizer, The IIRG, Nick Halflinger, Brain Donor, GarbageHeap, Demogorgon, Mike Gunderloy, Jerod Pore, WIRED Magazine, Factsheet Five, Emmanuel Goldstein and everyone else at 2600 Magazine, Kurt Saxon, The U.S. Postal Service, and those who I accidentally missed or wished to remain anonymous. Everyone who've helped Cybertek out, from writers to envelope stuffers, were instrumental in keeping it going over the years.

Cybertek was started as a quest for a 'zine in the flavor of TAP (Technology Assistance Program), a four page newsletter that ran in it's first incarnation from 1971 to 1984. TAP covered all kinds of technology from crossbows to computers. At the time of Cybertek's inception, there was no regularly published 'zine which had practical hands-on articles on technology, security, and self-reliance; a libertarian/constitutionalist viewpoint, and yet with a minimum of political raving.

Over the past five years, I've tried to fill in what I perceived to be a gap in this wide-ranging community. This community encompasses hackers (of all disciplines), techies, freethinkers, techno-libertarians, self-reliance and preparedness hobbyists (who used to be called "survivalists" before the term was slandered by the establishment media), and many others who are cut from the same bolt of cloth.

As strange and unlikely as it seems, we are all brethren. No matter what field of specialization, we all share a love of knowledge; the urge to expand our horizons; the capability to think for ourselves; a willingness to teach those who have a willingness to learn; and a fierce love of freedom. These characteristics bind us together, and are what distinguishes us. Although we all may seem different at first glance, we are all still fellow travelers.

One cold winter day five years ago; I wrote that the times were changing, and that the changes weren't for the better. Since then a lot has happened which unfortunately has now marked those words as a harbinger of what was to come. The socialists and totalitarians have been engaged in a systematic attack against what we stand for.

The propaganda that has been directed against the

Second Amendment of the Constitution has been continuing with increasing intensity, and it appears that we may be soon losing the teeth of liberty that has maintained this country's freedoms for over 200 years. With our right to self-defense and preservation almost out of the way, they are now attacking the First Amendment.

Recent media attacks against the Internet are stressing how the government should institute more control over the last major bastion of free speech in this country. The totalitarian organization, Handgun Control Inc., has come out and stated that there are certain types of "dangerous literature" which should be banned. They apparently consider information that would help people defend themselves "dangerous". One can guess what type of society those people want where the information to preserve liberty would be banned.

The last time an attack against knowledge and learning occurred, the result was the dark ages. Shall we let them doom us to repeat history? And as if things weren't bad enough, we still have problems with the rising crime rate and the declining economy. At a time when the knowledge of self-preservation is needed the most, the attacks against it have stepped up in intensity.

There is still hope for the future however. The attacks against "anarchy on the Internet" indicate it's effectiveness against totalitarianism. Should those who use the internet decide to "go tactical" it will be one of the most effective tools for freedom we can bring up to bear against the enemy. Citizen's have been joining the "militia" in increasing numbers (the last figure I received indicated an estimated membership of Five Million), and the performance of the militia units that appeared on the Phil Donahue show recently have shown that they are equipped to deal with the rigors of information warfare.

Things could be worse, but unless we continue fighting, they will be. Any person who studies the histories of Ottoman Turkey (1915-1917), the Soviet Union, Nazi Germany, China, Guatemala (1960-1981), Uganda (1971-1979), and Cambodia (1975-1979) will be able to clearly see what happens in a totalitarian state. We still need to put in a lot of work before we can, if ever, consider things safe.

- **Thomas Icom**, Senior Editor

Ψ

Terrorism in a New World

by **Atreides**
Managing Director, The Nemesis Group

In a time when a greater peace appears to be breaking out, smaller conflicts appear to be on the upswing. There are two major causes for this--the death of the superpowers and the stability they brought, and a severe reduction in the minimum means necessary to engage in conflict. The preferred method?
Terror.

Terrorism has been correctly identified as being media driven. In its guerrilla warfare form, terrorism is intended to bring attention to a conflict when the media is perceived to be controlled by the opposition or when it has no wish to cover the conflict otherwise. Organizations such as the Provisional Irish Republican Army (PIRA) or the Palestinian Intifada fall into this category--PIRA against British rule and control of the media, the Intifada against Israeli occupation, with a media bias in favor of Israel. Other terrorism is for the purpose of distraction, slight of hand, or revenge. Syria, Iraq, and Iran, following their belief that the ability to destroy is the ability to control, have used terror acts to control the Palestinian peace process terms and timing; the Syrian-backed Al Saiqa attack in Austria just prior to the October War distracted Israel from the impending threat; and attacks such as Black September's Munich Olympic operation, were purely reprisal.

Over time, terrorism has changed its form. The first generation of 'modern' terrorism, post-World War II, was based on a theory of attrition, a strategy of exhaustion. Target profiles were 'no retreat,' such as airplane hijackings and Embassy takeovers. Counter-terror tactics caught up at Entebbe, showing that police

methods and commando strikes worked against this threat. Second generation terrorist attacks stemmed from a reactive evolution and focused on a strategy of recognition, almost a coercive propaganda. These methods were adopted, in different forms, by the PIRA and Palestinian groups. 'No contact' targets were adopted, primarily through the use of explosive devices. Attack on this strategy was made by criminalizing the action, with complete removal of the political context in media coverage of the event or group carrying out the operation.

The next step in terrorism, which is happening even now, applies technology to overcome these problems. While nations' military and intelligence services re-tool themselves to deal with the fall of the Eastern bloc and worry about nuclear proliferation, a different genie has come out of the bottle, one that can't be put back in, and for which there is no infrastructural control possible.

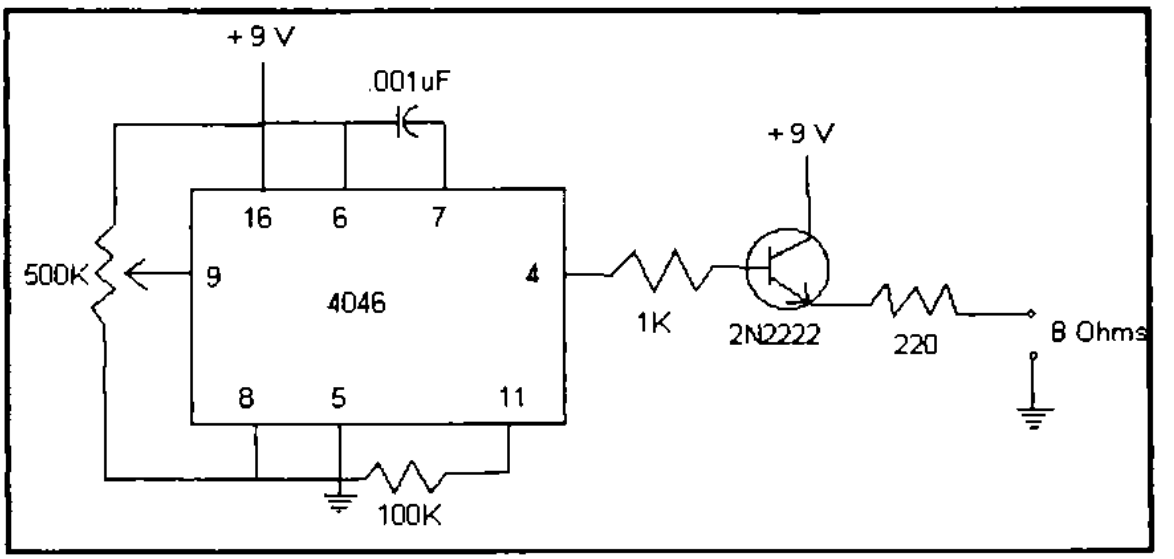
Communications technology has revolutionized the way the average man lives, works, thinks, and plays. The popularization of this technological infrastructure will provide a ready tool for the future terrorist--a global arena and a way to leverage limited resource. Soon to be gone (in most parts of the world) will be the cut-outs, drops, forwards and other elements of tradecraft in the Cold War period.

The telephone system, with its anonymous payphones, reprogrammed cellular phones that allow one to roam, facsimile machines, alphanumeric pagers, and voicemail are only the beginning. In and of themselves, they can act as a digital replacement for most items of tradecraft, but they provide even better services. They also allow computer networks, private and public, with numerous anonymous entrypoints, to move information around without worry; information as simple as a scanned image altered in a creative fashion to be distributed, laser printed, copied, and distributed for propaganda purposes; or information as potent as a continuing evolutionary design of explosive devices. Distribution through the electronic mail, mailing lists, anonymous remailers, newsgroups, or whatever, can now act as a 'community memory', keeping all parties informed of all evolution in tactic, technique, and technology.

Digital cryptography for the masses has provided another powerful tool. Messages

Audio Tone Generator Schematics

This device is capable of operation from .5 Hz to 18.5 Khz by adjusting the 500K pot. It's handy for various tone signalling and remote control functions. The heart of the unit is a 4046 PLL IC, boosted by your basic 2N2222 transistor amp. Due to the fact that it uses a handful of parts, it can be implmented in a very small physical package.



can be secured using public-key cryptographic technology, among other methods, for authenticated distribution, internal to a 'virtual organization' for things such as operational plans; or external, to media organizations to provide propaganda statements to negate counter-terror efforts to 'close the lid' on issues. Even this technology is rapidly evolving and will provide even greater capabilities--voice encryption using a normal computer, providing security and authentication for dynamic, real-time communication; the ability to disguise secure information as signal 'noise' inside of other data, innocuous or not, such as the large pornographic subculture on the public computer networks. This technology is being given away free to any who want it, even making the 'source code' available, to allow the user to be certain it isn't gimmicked; this allows a more sophisticated user to make alterations, or use certain techniques for other purposes (such as the creation of a cryptographic computer virus, which infect a system and encrypt data with a public key technique for blackmail purposes, since capturing the virus doesn't provide a mechanism for retrieving the data). Rising interest in such technology have also made available the resources for attacking such systems, which secure personal, corporate, and government computers worldwide.

Technology is making direct alterations in the way every organization operates; terrorist groups, or for that matter, any organization with the wherewithal to, can drop the hierarchical or 'cell' structure that is out of date. Such structures, other than being inefficient, have also become negated through contract tracing, traffic analysis, or 'gateway' style checkpoints on members which make the entire organization vulnerable. Heterarchies, with localized independent action are the next wave, with authority being roll-based and functional, and structures only being one level deep, allowing direct control or supervision but providing complete isolation from the other elements of the network.

Recruiting is effected--members who are voluntarists can be thoroughly investigated before trust is given. Collateral networks can be established as never before--vulnerable elements on the computer networks such as women or homosexuals can be exploited; tracing back dependent behavior such as drugs, sexual, or other deviant behavior can provide blackmail leverage; mules can be recruited among the population who are still legal 'minors.' Legends for members of the organization can be made quite thorough and backdated.

Funding for the organization can come from industrial espionage, which requires essentially the same virtual infrastructure, computer crime, or blackmail. The needs of the organization won't be extreme, however, as the technology provides leverage, and the infrastructural costs are practically negligible, carried mainly by the legitimate use by the populous at large.

Operations gain considerably, and intelligence and research, the backbone of any organization, profit most, targets can be isolated and an in-depth background brief and schedule developed through penetration of computers and communications (including contact tracing, purchasing habits, travel, etc.), and all in a fashion that doesn't alert the target or any security protection they may have.

Training, planning, and debriefing can benefit from virtual walk-throughs, models of anything important to the operation built entirely in advance, which can be used together by team members who need never meet to use them, working over networks. Post operation 'spin control' can benefit from massive monitoring of media channels and real-time propaganda or manipulation. Operations may even become fully digital--information warfare attacks are highly leveraged, low cost, can be done at any distance, take whatever time needed yet be synchronized, have complete surprise, and move faster than the opposition can respond to.

There is very little in the world of intelligence that is not now available to most anyone with technology and the will. More so than any 'dual use' technology, computers and communications are an equalizer, in a world where whomever makes the first move, wins.

The Riddle of Steel

Long Knives, Swords, and Machetes

by **Jim Teff**

Most people fear knives more than guns. The reason for this is that while few have any concept of a gunshot wound, almost everyone has experienced a serious cut at some time in their life and the memory of this injury makes them squeamish at the sight of a menacing blade.

Long knives and swords were the primary weapons of the middle ages and are just as useful today. My advice to the contemporary Viking or Ninja is to consider the machete. Machetes are more useful tools for clearing trails, constructing shelter, chopping firewood, etc. They are also far more economical. Smoky Mountain Knife Works offers 2 styles for $3.99 each (The most expensive are under $20.) These come without sheaths, but a serviceable scabbard can be made by sandwiching the blade between 2 slabs of cardboard and wrapping with duct tape. At this price, you should keep a spare or two. Besides its versatility, the machete is easier to explain to "the authorities" if carried with camping gear, tools, or fishing tackle. Try explaining a broadsword or Ninja-to to the police. Machetes can be blued if desired, for camouflage and rust prevention. Even if you choose another type of sword or long knife as your main weapon, I recommend a machete as a backup or spare.

If you desire a more exotic blade, Smoky Mountain Knife Works offers a variety of steel at reasonable prices. A few of their blades are:

Gurkha Military (Kukri)
ORDER# GT368 - 11" blade - $8.99
ORDER# GT365 - 24" blade - $14.99
These come unsharpened; so you will have to put an edge on it yourself.

Giant Bowie
ORDER#PM1170 9 3/" blade, 14 3/4" overall - $12.99
A good copy of the Western Cutlery bowie at 1/3 the price

Texas Bowie
ORDER# HK2730 - 15" blade, 2- 3/4" overall - $19.99
A heavy chopper with a sawback blade and knuckle bow.

Texas Pigsticker
ORDER# HKT2 - 15 3/8" blade, 21 1/2" overall - $19.99
Double edge - sawteeth on both edges near handguard

These last three are made in Pakistan, but have surprisingly good steel for the price. They come sharp but could, and will, take a better edge.

25" Machete (Tramontina - Brazil)
ORDER# MA076 - 20" blade - $3.99
19 1/2" Bolo Machete (Brazil)
ORDER# MA074 - 14 1/2" blade - $3.99

These two machetes are of excellent quality. They measure right up to the $20 ones.

I also recommend their carbide sharpener. This will put a razor edge on a donut!
ORDER# SI1 - $5.99

All of these are available from:

Smoky Mountain Knife Works
P.O. Box 4430
Sevierville, TN 37864
1-800-251-9306

Ψ

Echinacea: An Indian Tea

by **Bleach**

The winter that we are in now has not only come with cold temperatures and icy conditions, but also has come with colds and flus.

A couple of months ago people were scurrying to their personal physicians to receive a flu shot. Well, I was learning in class about flu shots and it seems that

doctors need to see what the flu type is this year, since the flu virus itself is different every year. So, doctors have to use a control to test the virus. If the doctor receives 30 patients wanting a flu shot, it is possible that the doctor gives 15 patients the real shot, while he gives the other 15 water in the form of an injection. I am not trying to say your doctor does this, but it is proven fact that some doctors do.

I have been sick with the flu once and had about four colds already this winter, and my brother told me something his friend said about Echinacea Tea. My brother's friend has not been sick yet so my brother bought the tea. I was reading the history about the tea and this is what I found:

"Used as a remedy by the Plains Indians more than any other plant, Echinacea is a perennial plant native to the United States. As early American settlers moved west in the 1800's, they discovered Native Americans used Echinacea for a variety of both internal and external health benefits. Also known as the purple coneflower, Echinacea has delicate, daisy-like pastel petals and narrow leaves. The name Echinacea is derived from the Greek 'echinos' meaning sea urchin or hedgehog in reference to its sharp spiny projections on the cone-shaped seed heads. To this day, herbalists continue to grow and use Echinacea for its beneficial properties." (Alvita)

So, it seems that the Native Americans have shown us another good way to keep ourselves happy and healthy without going to doctors or spending too much money on prescriptions and loss of pay from work.

You can get Echinacea Tea Bags at General Nutrition Centers (GNC) for $5.15 a box. It comes with 24 Tea bags and I recommend to put some honey into it. It says on the directions to do it to sweeten it, but I say it just tastes better all together with honey in it.

In conclusion, I would just like to say that looking for alternative ways to heal yourself and/or prevent diseases through safer methods such as Echinacea Tea is the best way to survive on your own. Surviving in the wilderness is something that present day people are not thinking about anymore. You need to be one with the earth and then you will be able to survive anything.

"Ignorance is the death of a society."
-Bleach

References:

Alvita Co. (Div. of Twin Lab Co.) product literature

Ψ

A Guide to Computer Operational Security (OPSEC)

by **Bleach**

1.0 Introduction

The Higher Entities in the world today are becoming more active in the world of computers, or as referred to by the media, "The Information SuperHighway." The past decade proves that OPSEC is important for anyone in the computer world, even though you might not be in an organized computer "group". Such incidents as the Jackson Games situation in Texas and the Craig Neidorf trial proves that certain bad seeds in law enforcement will blatantly throw the Bill of Rights out the window and try to stop the information being spread over computers.

The reasoning behind this article is that I have seen many articles that cover certain aspects of security on computers, but not always a full compilation of OPSEC on computers.

I would also like to state that the views in this article are my views only and should not be looked upon as the views of the editor or any other writer at CYBERTEK.

2.0 Basic Security for the Computer User

The Computer User who is looking for security from strangers and the higher entities would want to use certain personal security measures off and on the

computer before even using a modem. This may not apply to the basic user, but more likely to a computer hacker, pirate or someone who the general public would not look upon as a friendly user.

2.1 Keeping a Low Profile Off The Computer

This is probably the most simple, but probably the hardest measure to keep for some people. The only thing that you have to do is keep your mouth shut.

I believe every computer hacker or just an average person has told someone else something that they regret saying for some reason. You must always believe that the person you are speaking to is your worst enemy when it comes to certain security aspects. You would not want to tell anyone about what you have done that was illegal (not that I am promoting illegal activity) or whom you are not positive is 100% trustworthy. The fall of many hackers in the past was saying something to someone who was not trustworthy. The person you told could either be an informant or just another person who might get busted and sing like a bird to the authorities

Also, do not say anything incriminating over the phone. It would be the safest bet to assume that your phone is always tapped. The phone system today is not secure enough to feel safe and an average person could have the ability to tap a phone after reading one book. It is a frightening thought, but also a very true one.

2.2 The PC's Basic Security

A computer user should take the basic precautions before even starting to get into anything the public would find questionable. It seems that everyone has different suggestions, but these are the basic necessities:

(1) A Password Protection Program: This item is usually not on people's list due to it not being very secure to the intelligent computer user, but it is good for protection against people who pass through your residence and you do not want them just screwing around on your computer

(2) More than one Virus Scanner: Virus Scanners receive bad media in the computer world for not being very accurate, but they have saved me from certain virus programs that could have done large amounts of damage. The reason I recommend using more than one because using one will limit you to the virus programs that the one scanner looks for. When you use multiple scanners, you are less likely going to have a virus get past you. I recommend having one of your scanners made by McAfee, they have never given me any trouble.

(3) Some Sort Of Cryptography: It is safe to say that the government does not look too kindly on Cryptography because it makes their life harder. I will get more into the Cryptography topic later on, but just for starters I recommend getting PGP (Pretty Good Privacy) Encryption (c) by Phillp Zimmerman. Encrypt everything that you would not enjoy having someone, who you are not acquainted with, to look at. Always encrypt your personal e-mail that you would not like System Administrators reading.

(4) Backups: It is definitely recommended to backup your computer several times, preferably on floppy disks and tape backups. Backup your computer every month to two months to keep recent acquisitions safe from drive crashes and viral attacks.

Once you have your own personal computer secure, you then are prepared to enter a world that simple backups and Password Protection, won't save you from. This is the online world.

3.0 Online Introduction

The online world is full of many sorts of people. The main reason many people sign up for online services, or receive Internet access is to meet other people, as well as gaining further knowledge in other subjects. In this online world, a person can meet all types of people, good and evil. It sounds like an old medieval story of the dark warriors being fought off but the heroic knights, but it is not as "simple" as the good vs. evil story The reason for this is that certain groups of

people consider one group evil, while another group of people may consider the same group heroes. The online world is a never ending battle ground and that is why security is so important.

The three main categories of the online world are Online Services, the Internet, and Bulletin Board Systems (BBS).

4.0 Online Services

Online Services have been around for the past decade but have really bloomed into something rather large within the last five years. With Services such as The Prodigy Online Service, The America Online Service, CompuServe, and Genie, almost any person in North America with a modem can connect and talk to other people. The people on these services are not always the brightest people in the world, but there are many who you can speak to on a normal basis. Even though Online Services stress security by telling its customers to change their passwords often, you are really not safe from anyone on such services.

I will give a brief explanation of the Prodigy Online Service and the America Online Service. Those are the only two Online Services I frequent, but if I get enough requests to investigate the CompuServe Service and/or the Genie service, I will due so promptly.

SideNote: I do not consider the CRIS service or Delphi service as online services. I consider them as Internet Providers

4.1 Prodigy

When I received my own personal computer two years ago, when the community that I participate now in was unknown, all I wanted to do was get on Prodigy. When I entered the land of Prodigy, I thought it was a great place to communicate with other people across the country. This was until a few months later when I started meeting certain people in "clubs" that used to bash people for fun and set up fake accounts using fraudulent credit cards. I of course finding this interesting so I joined one of these "clubs" The Prodigy service did not take too kindly to those groups though and they later disbanded without a trace. There are still such organizations now full of people who think they are the greatest people to ever live and want to harass you and prove they are the "best". What I am stating is fact, they will stop at nothing to rip you off or just harass you away from their "club".

The best way to keep secure on the Prodigy Online service is stay out of the way of certain clubs. Let the Board Managers do their job and take care of them. Secondly, do not post anything too radical that would gain too much attention from the wrong people If you are interested in hacking or any type of Underground "scene", don't post on Prodigy about it. You would probably just be called a "lamer" and targeted for their next attack. I also recommend setting up the account in your name, but then go to the personal info section and changing your name to something else Prodigy will not get upset unless you change it all the time, which is not recommended. The final major factor in for the Prodigy Online service as well as all of computer security is DO NOT TRUST ANYONE. If you do change your name, do not tell anyone anything about yourself, because it can all catch up to you at the end, even if you do not do anything illegal In my own personal opinion, there are many people there with severe emotional problems that you would not want to get tangled up in.

4.2 America Online

The America Online service is different security wise than Prodigy. AOL has a lot more determined people who claim to be hackers, but really are not. These types of people will stop at nothing to rip anyone off blindly, especially the service itself. These "wannabe hackers" use means of ripping people off by posing as a worker for AOL and ask for passwords for security reasons. Now many people reading this will probably think, "how stupid are the people handing out their passwords?". The answer to that question is not stupid at all. The "wannabe hackers" on AOL aim for the people in the "New Member Lounge" looking for

someone who is not familiar with the system, and then uses certain techniques to trick the victim.

My recommendations for the America Online System is to change your password monthly, as well as when you create your profile, put a lot of false information. You can keep your same occupation or something like that and even your first name, just do not put the real place you are from so they can track you down. The people on AOL love making harassing Telephone calls, and if some of them are reading this now, I am expecting to receive a few myself. Don't go looking for trouble either. On AOL, no one likes someone who talks a lot of shit. If you say something that upsets them, they will try to find you. Most of the time if you are secure, they will fail miserably, or just get bored and give up. The Trust factor plays a larger role on AOL. I recommend that even if you think you trust a person, still do not hand out anything that is too personal, because a lot of your "friends" will tell someone anything about you if they get something out of it

4.3 Online Service Conclusion

My personal opinion is if you must choose between these two online services, pick the Prodigy Online Service A year ago I would not have said that, but Prodigy really cleaned up their act and are now providing a nice service. If you do subscribe to Prodigy though, receive the Prodigy software for Windows instead of DOS due to the fact that the Windows Version is the one that gives you most of the Internet Access Also, if you run into anyone on Online Services that claims to be a hacker, they probably are not. In my research, I asked the so called hackers many technical questions which are easy in the eyes of hackers. They claim to be hackers because they can card (use of a fraudulent credit card) an account and that is NOT hacking.

5.0 The INTERNET

The Internet is now becoming larger by the day and even though security specialists brag about their new methods of making it "safe" from hackers (even though that really isn't true), you are not safe from anyone. Since the Internet is so vast, the people on it are open for attacks. Even if the System Administrators claim that the system you are running off of is safe, you still may want to do some investigating.

5.1 The Legit User Seeking Operational Security

A person seeking an account, in his name, for his own personal use, and wants enough privacy and security to not be hassled, then he should look into this. If you are a cracker, then you might not care about this section, but it is still information in which you may want to know anyways.

5.1.1 The Finger Command and Password Files

The Finger Command is one of the least secure things about the Internet. If your system is not secure enough, the Finger command could give valuable information about you, such as your name, address, and phone number. If a system even has one that gives your address or phone number, stay away from it.

Password Files however are different. Many Password Files have your real name and sometimes your phone number. On several University Systems, if you are a worker there, the password file states the person's name, phone number, and Department the person works at. You are more secure as a student though, since from what I have seen at those systems, the students have random accounts, such as s154862. These are more secure, but also possibly has your full name.

A person needs to investigate these two aspects of any system running UNIX.

5.1.2 Commercial Internet Services

One part of the Internet that is growing rapidly is the Commercial Internet Services, such as Delphi, CRIS, and Netcom. I have had my own personal interactions with such services and they were not too pleasant.

Many legit users will be happy with these types of

systems, as I was in the beginning, but there seems to be catches (NOTE: This is not true with all services, so I do not want to receive complaint letters explaining to me how I am just someone with a grudge. I also do not want to receive any libel suits.)

The first thing you would want to do with these services is to find a nice commercial service with a nice, low cost, flat fee with suitable features. If you find one of these services, you may like to keep everything you receive about the service before you sign up (data or hard copy) It may seem to be a pain, but in the end you would like to show that it was a flat rate in the beginning so they do not change it without notifying you.

The second thing is not to say or do anything suspicious, incriminating or just plain out odd (NOTE: This should go for all legit users.) My own personal case shows that even being on #hack often was suspicious, which is ridiculous, but that is how some System Administrators are Also, keep in your head that the service you are on is not a nice system that lets you maintain your privacy. Many services log your IRC sessions or just your sessions period. I was called once from that certain service I was a member of and they said that I was doing suspicious activity and they read off everything I did from login to when I logged off. The suspicious activity turned out to be me being on IRC in #hack, #Phreak, #2600, and #virus all at the same time and then doing some FTPing. I still cannot believe what was so suspicious as that I was chatting (no illegal subjects), and downloaded a back issue of Phrack Magazine (c), if I remember correctly.

Another tip is if your service goes through a Packet Switch Network, which many don't anymore, only call the same number everytime. There are many 1-800 packet switch networks, but if you call several different ones, every time you log in to your system, it shows a different Network address. Many of the addresses start off with the area code of the state it is located, but on the 1-800 networks, they are all different. The system believes that people are logging into that account from different states, which makes them believe it is hacked and then deletes it. So if you just stick with one number, it will save you a lot of hassles.

5.2 The Hacker Seeking OPSEC On The Internet

Being a hacker on the Internet seems to be safer than being a legit user in recent times. Some hackers do get caught for Internet Hacking, but the fact is out of the thousands of "hackers" out there, few busts are made, and even fewer convictions. My major recommendation in the beginning is if you think you are going to hack the Internet or anything in general, do not direct dial from your house. A laptop computer comes in handy often. (***IMPORTANT NOTE***: Using the term "Hacker" in my case does not mean computer criminal. The media seems to be using the term in a wrongful manner which is not fair to the real hackers. The "Dark Side" hackers, who just use their skills to rip off other people are not hackers, they are criminals.)

5.2.1 Targeting Systems

A solo hacker or a group of hackers looking for a system for their own personal use should look for a UNIX system with the major security holes, ie. defaults, holes, few users or administrators on often, and of course have all the services you want in an Internet Provider. If a person dedicated enough wants to find a system with little security, that will provide for them a suitable place to explore and use, they should find services with unpassworded accounts. Looking around for myself, more foreign computer systems have unpassworded accounts. The one flaw with having unpassworded accounts is that they may not have a home directory, which would not be good for the hacker looking for an address where he can keep stuff online, such as texts, scripts, tools, etc..

5.2.2 Spoofing

Spoofing is an excellent way of keeping yourself and your group secure. Basically Spoofing is just covering up your tracks. If a hacker wanted to use basic spoofing, he would just Telnet to several hacked accounts ending at the account he wanted to play

around with. Spoofing gives System Administrators large headaches since if they really want to try to catch you they have to try to get back to the original account you were on, and if your first account was not legit, then the worse that could happen is that you lose most of the accounts that you were using for that hack. It could be a hassle for you, but things could be worse.

5.2.3 Cryptography

Cryptography is a major resource for a group on the Internet due to possibly being watched. Unlike the legit user, I would not recommend using PGP(c) or another sort of a shareware or freeware cryptography. If your group of hackers should have at least one programmer in the group, and if you do, then you should program your own type of Cryptography in which only the members of your group know. That should cut back on the surveillance of your group's interaction with each other. If you are a solo hacker or if you or any other member of your group wishes to have outside contact with other people in the community and do not want to be read by the System Administrators, I recommend also having a copy of PGP or another type of cryptography.

5.2.4 Outdials

Many hackers love playing around with outdials. Outdials are used by hackers to call out via modem and not pay for it. They telnet to a remote sight owned by a company to use their modem. Many hackers use these to call boards that are long distance to them. That is not a smart idea due to company computers logging everything that happens on them, including what happens on the outdial. If they log an Underground BBS number, they could have the feds investigate and possibly shut down the BBS. You would not like your favorite BBS being brought down due to your own stupidity.

Outdials are fun to fool around with, but they are against the law so I would not recommend using them.

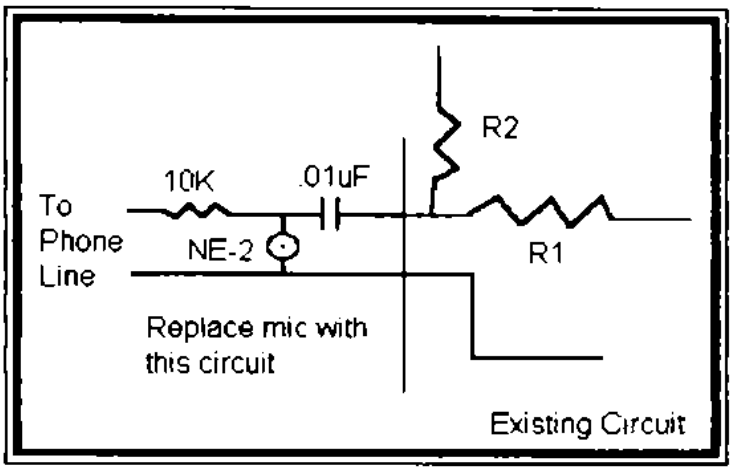
6.0 Bulletin Board Systems (BBS)

BBSes are the glue that holds the Modeming Community together. Almost every person who owns a modem is on at least one Bulletin Board. Many users have a false sense of security about BBSes. A good example of what could happen is a BBS that used to be local to me was raided by the FBI for child pornography. The Sysop's computer, which included all of the logs and User data files on it, was confiscated. All of the Users' e-mail and file transfers were on the logs and read by the Feds. Any user who had anything suspicious written on it could have been watched by the feds.

My recommendations for BBSes are as follows:
(1) Sysop is Not Your Best Friend: Sysops are normal people, but they all have different personalities. I have met some of the coolest Sysops and some real asshole ones. I cannot really judge any of them due to the fact that I don't know them personally, although I feel that it is admirable of them to take the time to set up a nice board.
(2) Encrypt Your E-mail: I sound like a broken record, but you need to know how important that one concept is. It will save you from a lot of hassles, and that is what every computer user is looking for.
(3) Watch What You Say: Since there is no tone of voice or body language, people can interpret what you say on BBSes any way they want it. That is just a way for people to dislike you which could lead to things not in your best interest. Also, do not talk about what you have done that is not law abiding on the message bases or in e-mail. (NOTE: This is not always the case on H/P boards, since the spreading of hacks and other information goes on there.).

7.0 Language

This only really pertains to H/P groups or any type of Underground Group. If your group is participating in activities that you wish to talk about between each other but do not want anyone else to know what you are talking about, then I suggest you make your own personal type of language. I do not mean make another



Modifying the Radio Shack Wireless Microphone Kit for Telephone Surveillance.

(Before implementing this device, check the applicable laws regarding telecommunications surveillance in your locale, and ensure compliance with same.)

Spanish or Latin or something of that sort, just take your homeland language words and change the definition to something else that only you and your group knows. It may sound childish, but in the end it may save you from Outside Interaction. You can speak freely over the phones without anyone knowing what you are talking about. To them it could be a common discussion of gardening, when you are actually speaking of cellular phreaking, it is just that simple.

8.0 Conclusion

Operational Security seems to be the only means to protect yourself from the bad seeds of our country or strangers invading the privacy of you or your group. If you follow my recommendations, I believe that you should not have any problems. Once again, I am not promoting illegal activity, just the means of making you feel more secure.

I hope this file helps get you started on your Computer and Operational Security. I would be happy to hear any suggestions or questions on OPSEC.

The Ten Dollar Bug

by Thomas Icom

For those whose surveillance budget is less than that of a third world nation and don't care about sophistication, this little gem will do the job at the bargain price of $9.99 plus tax.

The device is the Radio Shack FM wireless mike kit (28-4030). Soldering will be required. It operates on the FM band between 80 and 106 Mhz, and according to Tandy's catalog will run about 40 hours on a 1.5 volt "N" cell. The instruction sheet states that it's range is 45 feet.

My Observations

All things considered, it's a decent unit for the price. The mike sensitivity is a bit lacking, but it lends itself to some interesting modifications.

The circuit design is capable of running off of more voltage than 1.5 volts. Doing so will also increase your transmitting range. I ran one off of a 9 volt battery without any problems. At 13.5 volts the unit still held together, but what stability the unit had went to hell.

The heart of this unit is a 2SC1923 transistor (a/k/a ECG107). This transistor is usable to 800 Mhz. By changing the component values for capacitor "C4" and coil "L", you'll be able to move the unit off of the FM broadcast band for increased security.

Even Cheaper

If you're so destitute that even ten bucks is too much, the Radio Shack kit is comprised of about eight dollars worth of parts. The design is such that you'd get away with constructing it using point to point wiring, provided you stay on the lower frequencies. Personally, I think that when one takes into account the time of waiting to get the parts from a mail order house, the typical $20 or so minimum order that most mail-order parts dealers require, and the time and the fact that the

Radio Shack kit has a nicely laid-out PC board all ready to go for you; that you'd probably be just as well off spending the extra two bucks and getting their kit.

Final Analysis

It's no crystal controlled Deco unit. Then again it doesn't cost $70 a pop either. At $10 it definitely falls into the throw-away category. I use mine for a few internal applications where security isn't a concern, like wiring it to the speaker jack of one my scanners, so I can use an FM radio to listen in while working around the house The unit is easy to put together, and lends itself to experimentation.

Ψ

Room Bug

by S.V.M.

Take any old baby monitor and place the transmitting device in any room or anywhere you want to hear somebody talking Plug transmitter into wall (Ed Note: Some of the newer ones run off of DC power so you can substitute a battery for the unit's power supply. The current Radio Shack unit (43-487) uses 9V DC.) - hide it as much as possible! Leave it on and Shazzamm!! You have a room monitor. Just turn on your receiving device and listen in. The only downfall of this is you will have to be within 500', maybe 1000', of the transmitter device. I have picked them up at garage sales for $5-$10 a unit.

Ψ

Survival Notes (#2)

by Wildflower

Just got done filling another coffee jar with desoldered electronic parts, to be sorted into other jars for reuse or future barter later on. No matter what kind of board, machine, or other item; I always look for salvageable parts & hardware for my shop. Some are used now, some later; all stored in various marked jars or coffee cans as to contents for later retrieval. And if I never use any, still it is sort of a GOLDMINE for the next generation to tap into. I mean, in fifty years, if one wants to restore one of today's TV's or RADIOS, parts will be damn near impossible to find for such sets! Also think if you wrapped up that obsolete computer or radio, in fifty years it may fetch thousands of dollars if still operational or not, as a collectors "item"

Or if the world truly goes to hell, such parts, hardware, even working obsolete computers, will be all worth their weight many times over in whatever currency is used for barter. Even a ZX81 (TIMEX 1000) Sinclair with 16K RAM is going to be of more value than a dead, rotting mainframe.

And hardware; kept dry and free from dirt & corrosion, will be worth $??? over rusted, deteriorated nails, screws, ectra. What will be more incredible is that such items are found "FREE" in most dumpster bins or trashcans! Yes, by crafty salvaging, I have over several thousands of dollars worth of parts, hardware, ectra; all accumulated slowly over a ten year time period; with more than half of it already reused in other projects!

Of course, not all discards are worth salvaging even one part from, but one should think twice before discarding any JUNK if there is anything recoverable before throwing it away, next time!

Took apart a hair dryer the other day as its element had parted apart of old age. Needless to say, did recover the remaining element wire, switches, the power cord, and its fan. Incidentally, a few years ago was delighted to find that a hair dryer fan motor, rigged with diodes to run in one direction only, also minus element, ran off a six, then twelve volt battery! This gave rise to another home project: a simple "BLAST FURNACE". This was built utilizing a #10 can (39 oz coffee can) with a piece of auto exhaust pipe coming up into the bottom of the can; then cover the inside bottom with 1/2" metal mesh circle (same dia. as inside bottom). With foil & wire, hooked up a fan motor unit. Supported on bricks, the furnace was filled with common store brand charcoal,

lit, then topped with an old circular saw blade.

With the fan running off an old auto battery, it pushed enough air through the burning charcoal to bring that old coffee can "CHERRY RED" within a few minutes. It only takes slightly more to "BRIGHT RED" iron rod (1 inch dia.) section.

Steam Power Resources

Building steam boilers and steam engines takes having the necessary information, parts, and plans to craft, run, and maintain them. A good "steam primer" can be found in Kurt's (Saxon) _Survivor_ books; after which one can look to other sources for more information.

Some sources are.

Lindsay Publications
P.O. Box 538
Bradley, IL 60915-0538
Catalog. $1.00
A lot of old time reprinted books, on various topics.

The Steam Outlet
P.O. Box 1426
Thonotassassa, FL 33592
Catalog: $5.00
Building plans & parts

Campbell Tools Company
2100-P Selma Road
Springfield, OH 45505
Catalog: $1.00
Various books & kits.

Blue Ridge Machinery and Tools Inc.
Box 536-PS
Hurricane, WV 25526
Catalog. FREE
Various books & kits.

Do remember "live steam" can be dangerous if improperly contained in boiler/engine; resulting in injuries or death! Do not try to use inferior materials as a substitute to what is recommended in constriction of boiler/engine.

However, steam technology will be useful for those who want power to run their machines. Those who don't can suffer all the way to hell!

As batteries fail (unless you create new ones); storing your excess energy could be found in: uphill water reservoirs, pressurized air, hydrogen gas, large capacitors, flywheels, superconducting storage loops, and possibly superhot metals (or glass) in superinsulation containment.

Sounds "too exotic", then why are you using: computers, automobiles, microwave ovens, etc...? And after the collapse of civilization, does that mean you will give it all up, including "TO CONTROL THE LIGHTNING!"? Give it all up to live in a cave, whispering strange stories about the fire about "WHEN MEN WERE GODS"? ARE YOU NUTS!?!

In the "post-collapse years", we will be trying to survive as best possible as we can. However, afterwards, we will want to reconstruct our basic industrial basics to start tackling many areas, including any hazardous areas to recover useful materials for our needs. (also to neutralize hazardous sites that could ruin local ecological zones, trying to recover!)

Those wishing to correspond with me can send inquiries to:

WILDFLOWER
PO BOX 1745
New London, CT 06320

Please include a self-addressed/stamped envelope (or a stamp)
Please no bombs, drugs, or radioactives .....

LAST: As undoubtedly direct neural interfaces (implants) could hookup a person directly to their computer, remember as you may program a machine, you may get reprogrammed by it! Also a computer

virus will create ultimate horrors if it gets into your natural neural networks, indeed! Do heed this futuristic warning!

LIVE LONG & FREE!
Wildflower*95

Ψ

Editor's Choice: Hobbyist's Guide to COMINT Collection and Analysis by Thomas Roach

review by **Thomas Icom**

This book is an excellent how-to introduction to the world of communications intelligence (COMINT). This self-published work goes into detail on the equipment needed, where, when and how to listen; data analysis, and using a personal computer for COMINT analysis.

COMINT is the practice of gathering information of interest to you by monitoring radio communications and analyzing their content so you can apply it to your situation. Depending on your requirements, the signals can range from international shortwave broadcasts to your local public safety agencies.

The book's focus is more on strategic intelligence, rather than tactical intelligence. The book is heavy on HF ("shortwave") communications interception, particularly those originating from Russia and the former Soviet republics, although it does talk about COMINT activities focused towards local VHF/UHF public safety communications.

This book is geared to the beginner and intermediate radio hobbyist, and is a very easy read; especially considering the complex nature of COMINT analysis. I strongly recommend this book for anyone whose shortwave radio or scanner usage goes beyond casual listening, and especially for those who are looking to take full advantage of alternative news gathering techniques.

94 pp, 8.5" x 11", $26 (with Priority Mail Shipping)
Tom Roach
1330 Copper Peak Lane
San Jose, CA 95120-4271

Prologue to the Hobbyist's Guide to COMINT Collection and Analysis
(reprinted with permission from the author)

This book was written so that anyone with normal intelligence, and the inclination to do so, can engage in the esoteric and "hush hush" art of communications intelligence or COMINT. Communications intelligence is considered by most governments as the most sensitive and secret of all their intelligence activities. Most governments conclude that if details of such activity, or even the existence of COMINT operations were to become public knowledge, cataclysmic damage will result to their "national security". It is always concluded that if the "target" became aware of the existence, success, or extent of COMINT activities, they would change their security procedures and deny the listening party(s) any further intelligence. History is witness to the fact that even when governments are informed of failed security measures, they often fail to believe the facts, or are constrained by cost or circumstance from correcting their failures.

There are also "ethical" pressures which cause governments to wince at public admission of COMINT programs. The haughty American statesman Henry L. Stimson is quoted as having said "Gentlemen do not read each other's mail." It should hardly be a secret that almost any government larger than Monaco's almost certainly is monitoring the diplomatic and military transmissions of both friends, and foes, alike. Fears of "Big Brother" in the United States are not so easily dismissed when citizens discover that the United States Army used COMINT during the 1968 Democratic Party Convention to spy on private citizens within our own borders.

For many people there exists a strong fascination with listening to, or reading another person's or country's private communications. You will be surprised to

discover the degree of success that a hobbyist can expect to attain by a personal intercept and analysis operation of the sort described in this book. At a minimum, you will be able to intercept an astonishing number of foreign communications from the comfort of your home. Certainly you will encounter private communications; some personal, some administrative, and some diplomatic. With the incredible computer power available today at remarkably low cost, it is not impossible that a very clever hobbyist might achieve some success in penetrating some country's cipher system. Perhaps a gifted amateur could even equal the success of Yardley, who personally broke not only America's top level codes, but those of numerous other nation's as well. Yardley did this with nothing but his wits, intercepted communications, and hard work. This book will place in your hands the techniques required to routinely examine information that governments, corporations, and even your next door neighbor, would just as soon you didn't have.

Some of the messages I have personally intercepted may surprise you. In his remarkable study "Soviet Naval Power in the Pacific" Derek Da Cunha quotes an Australian MP "... supposed non-military [Soviet] fishing vessels have been logged sending messages in highly complex codes, far more complex than warranted by a report on fish tonnage caught." I have personally intercepted many of these messages, which the Russians refer to as "KRIPTOGRAMMA". A February 1994 news story revealed that the Soviets used just such messages to cover up the fact that they were butchering twice the number of whales than they had agreed to! One section of the book deals with these messages and gives clues as to how they might be generated by the Russians or decrypted by interested hobbyists. Then there are those very rare instances when somebody makes a mistake and sends a classified message in the clear. Not too long ago I monitored a four page classified message sent by radioteletype by a branch of the United States military. I provided the unfortunate radio station with a copy of the message in hopes that such slips could be avoided, and as a reminder that someone is listening when you least suspect it. In return, I received a letter saying that the matter was under investigation. The point is that you don't know what you will encounter unless you listen.

I have also intercepted a Russian "research" vessel's reports classified as "upper air" weather data. This vessel was located just a few miles offshore from Vandenberg Air Force Base during American test missile firings from Vandenberg Air Force Base to Kwajelein Island. Weather data of this sort was of significant intelligence value to Russian intelligence analysts wanting a better understanding of the success of American "Star Wars" weapons testing. It is easy to see that even the most amateur of collection efforts can catch intelligence plums. While not of such compelling security interests, but equally interesting, was an intercepted message to the captain of one Russian fishing trawler whose crew had accidentally spilled toxic waste on the catch. The captain was directed to process and can the catch anyway! Other messages heard by hobbyists included a message from a Russian ship's captain discussing the activities of a "mutinous" crew which was forming an illegal labor union because of "unfair" promotion exam testing. While the cold war is considered over, the Russians continue to operate gigantic listening post located at Lourdes in Cuba. An agreement between the Russians and the Cubans, renewed in November of 1992, ensured that this listening post, targeted on the United States, would not end its mission. The recent headlines surrounding the Ames case provide further proof that the Russians have not stopped spying on the United States.

Between the covers of this book are the details on exactly how to snoop on sensitive, but easily accessible communications. The communications you can easily monitor range from top level diplomatic communications between a government and its embassies, messages to and from spies, cellular phones, and "baby monitors". The content of this information ranges from the serious (government diplomatic material and police channels) to the farcical (e.g. the chit chat, lovemaking habits, and gossip of your next door neighbor). I will leave the moral posturing regarding the ethics of this hobby for the reader's own resolution. Nevertheless, there are certainly socially

acceptable and useful ways of using certain types of information. I have a friend who started out listening to the Russians and ended up working hand in hand with the local police. After the fall of the "evil empire" he started using a scanner to monitor the local police's radio transmissions. He converted the information given in the police radio calls into maps and databases. These are now distributed to both the police, and his neighbors. His reports reveal what is being stolen, where it's being stolen, and descriptions of suspects to watch for. The beleaguered police welcome his efforts since budget cuts prevented them from buying their own computer to do the job. Besides, this is exactly the neighborhood involvement the police need to keep the vermin on the run.

While this book mostly deals with methods used for intercepting radio communications, the book also details methods which will allow the reader to gather, and recall with ease, newspaper stories which are unlikely to ever be found in local, or for that matter, even the major national newspapers. In some cases the news stories will provide a rational explanation for changes observed in the radio messages. Equally important, trumpeted declarations of reform or change may be revealed as illusory by the absence of such changes which would/should have been reflected in radio messages

On a personal level I have found the hobby to be a source of intellectual pleasure and delight. I like to think of this hobby as the means by which I can extract a realistic portion of truth with which to balance the silly lies so often told by governments and foisted upon the public by an unsuspecting and all too often servile and lazy news media. I personally believe a careful analysis of the news to be the duty of any citizen who wishes to maintain a democratic form of government.

The book is divided into three parts. The first part of the book is devoted to the specifics of the equipment you need to monitor radio messages, and details on how to put the equipment together to form an integrated and powerful collection and analysis system. The second part of the book deals with how to analyze the material collected. The last part of the book explains how to contact and exchange information with other hobbyists, thus sharing your knowledge and widening your expertise.

Good luck and good listening!
troach@netcom.com

Ψ

Cybertek Reviews

by The Cybertek Staff

The Ultimate Potato-Bazooka
Hair Spray Powered Vegetable Guns

What are commonly known as "spud shooters" or "potato guns" are quickly climbing in popularity. These devices are made out of PVC pipe, use hair spray as the propellant, and will launch a 3 ounce potato 200 years. They are inexpensively made from materials at your local hardware store and are great fun.

M&M Engineering's book goes into easy to understand detail on the construction of five different potato gun variations, and provides valuable information on theory, design, construction, propellant types, and safety measures.

This book is geared towards the beginner/non-techie. Those of you who have already built one will probably find the information old-hat, but if you've never built one this book offers some valuable information.

If you're a parent looking for something to keep your kid(s) away from the TV and video game console, this would fit the bill, and is safer than some other things your kid could get into. If you're a statist, you'll read this book, think that both the author and I should be institutionalized for suggesting such a thing, and also probably go off on a crusade to ban PVC pipe and hair spray. Du-ma-nhieu. (TI)

36pp, 5.5" x 8.5", $9.95 + $4 s/h.

available from M&M Engineering

1995 Police Call Radio Guide

Police Call is a beginners guide to the world of VHF/UHF radio monitoring and a list of public safety license information for your region of the country; derived directly from the FCC database. It also contains "unofficial" lists of aeronautical, railroad, and "non-sensitive" U.S. Government frequencies, and an allocation list which tells you what service (both public safety and non-public safety) is assigned to each frequency.

When it comes to information on who is licensed to what frequency, I've found Police Call to be extremely accurate. They have even started adding specific information about frequency use. They lack the in-depth information that frequency directories like Scanner Master provide, but it appears that they are trying to catch-up. Recent editions have been including 10-code information and precinct/troop coverage maps, and the 1995 edition has more auxiliary information than previous editions

Police Call is solely public safety listings (environmental conservation, fire, local government, medical, police, highway maintenance, and special emergency). The allocation list will however tell you what type of service is assigned to a non-public safety frequency.

Police Call is great for doing a quick check on a frequency to see what locality and agency is licensed to it. It's also great for compiling quick lists of frequencies used by public safety agencies in your area. Police Call doesn't list unlicensed frequencies that are used for surveillance or other covert activities, but by knowing what frequencies are already taken one can then search through the "unused" ones to find more interesting activity.

At $9.95, it costs a lot less than most other frequency directories. For VHF/UHF enthusiasts who are into public safety monitoring, it's an excellent buy. Beginners will find the information in the first chapter particularly valuable. (TI)

Bootleg's DMV CD-ROMs

DMV records are, in most states, publicly available information. The entire database however, is usually expensive to acquire and only available on arcane media.

A well-known hacker from the old days who goes under the handle "Bootleg" has decided to make the information more readily available on CD-ROM. So far he is offering the driver's license and registration records of Oregon, and the registration records of Texas and Florida, with other states planned in the future.

The data is presented in delimited ASCII format, making it easy to implement with the database software of your choice. These CDs would be invaluable for mailing list generation or as an investigative aid. Considering how much it would cost to purchase the information from the state's DMV and the hardware to read the media; these CDs are a bargain. (TI)

Oregon CD: $219, Texas & Florida CDs: $495 each
Mike Beketic
9520 SE Mt. Scott Blvd.
Portland, OR 97266
503-777-2910

How to Live Well on Practically Nothing

The cheapskates' bible! A treasure trove of ideas to make you more self-sufficient and cut your living costs. Recipes, building plans, tips on clothing, camping, budgeting, etc. for today's depressed economy. (JT)

153 pp., 8 1/2" x 11", $19.95
Available via M&M Engineering, Loompanics, Paladin, and others.

How to Get Anything on Anybody Book II
Hands on Countermeasures
Hands on Electronic Surveillance

These three are excellent guides to surveillance and investigative techniques and technology; geared towards the beginner to intermediate. How to Get Anything on Anybody Book II is a general guide on techniques and technology. Hands on Electronic Surveillance and Hands on Countermeasures specifically deal with operational techniques on their respective topics. As with Lee's earlier works, all three of these superlative texts are a must for the bookshelf of anyone who is interested in surveillance, investigative, or intelligence gathering techniques. (TI)

How To Get Anything on Anybody Book II - $34.95
Hands-On Electronic Surveillance - $24.95
Hands-On Countermeasures - $24.95
(If ordering from Intelligence Inc., add $5 s/h per order)
Available from Intelligence Inc. and other sources.

The Art of Throwing Weapons

An excellent manual showing the fundamentals of throwing and making spears, spear throwers, knives, shaken, and boomerangs. This is a must for your primitive weapons library. (JT)

102 pp., 5 1/2" x 8 1/2", $8.95
available from M&M Engineering

The Sling

State of the art stone throwing! Here is a weapon that is cheap, easy to make, and uses free ammo. Everything you need to know about the sling is in this book. Every warrior should have a sling in his/her kit. (JT)

72 pp., 5 1/2" x 8 1/2", $7.95
available from M&M Engineering, Loompanics and others

Slash & Thrust, Flexible Weapons

These books give you designs of several weapons in the knife/flex class; as well as construction of practice weapons and practice sparring tips. Two more for the warrior's library. (JT)

Slash & Thrust: 72 pp., 5 1/2" x 8 1/2", $8.00
Flexible Weapons: 80 pp., 5 1/2" x 8 1/2", $8.00
available from Loompanics

Bloody Iron (a/k/a Prison's Bloody Iron)

THE book on knife fighting. 'NUFF SAID! (JT)

121 pp., 5 1/2" x 8 1/2", $10.95
available from Loompanics

Publishers' addresses:

M&M Engineering
RR1, Box 2630
Arlington, VT 05250
802-375-9484
Loompanics
P.O. Box 1197
Port Townsend, WA 98368
Catalog: $5 (and worth it!)
Paladin Press
P.O. Box 1307
Boulder, CO 80306
303-443-7250
800-392-2400
Catalog: $2.00
Intelligence Inc.
2228 S. El Camino Real
San Mateo, CA 94403
Catalog $15 (and is also interesting)

Reviewers:
JT - Jim Teff
TI - Thomas Icom

Ψ

Classifieds

Hacking / Phreaking / Cracking / Electronics Information/ Viruses / Anarchy / Internet information now available by computer disks, books, manuals or membership. Send $1 for catalog to: **SotMESC, Box 573, Long Beach, MS 3956**

UNDERGROUND INFORMATION: Computer Security, Hacking, Phones, Survivalism, Cryptography, and more. Catalog $2. **SHP, 862 Farmington Avenue, Suite 306, Bristol, CT 06010**

CONSULTING SERVICES NOW AVAILABLE: The staff of OCL/Magnitude: Cybertek are now available for consulting on information and electronic security, disaster preparedness, personal security/self-reliance, and specialized communications systems for individuals and businesses. **For more information call OCL/Magnitude Consulting Services at 203-225-1OCL (1625)**

WANTED: Articles for Cybertek #12. We are seeking high-quality, practical, how-to articles on various aspects of technology, security, and self-reliance. Write us or call RuneStone BBS for topics of interest, writers' guidelines, and compensation information, or to submit an article

Classified Ad Fee: 5 cents/word, 20 Word minimum.
SPECIAL OFFER: Place an add for 5 issues, get 6th issue free.
Deadline for May/June '95 Issue: April 15, 1995.
Send ads to: Cybertek, P.O. Box 64, Brewster, NY 10509 ATTN: Classifieds

Ψ

Masthead

Publisher
Thomas Filecco
OCL/Magnitude
P.O. Box 64, Brewster, NY 10509

Senior Editor
Thomas Icom/IIRG
thomas.icom@iirg.com

BBS Sysops
Mercenary/IIRG
mercenary@iirg.com
Brian Oblivion/RDT/L0pht Heavy Industries
oblivion@l0pht.com

Writers
Atreides, Nick Halflinger, Wildflower,
Bleach, S.V.M., Jim Teff

Dial-In BBS
The RuneStone BBS
IIRG WHQ
1-(203)-832-8441
(10288)-0700-THE IIRG
New User Password: *Cyberdeck*

Internet BBS
L0pht Heavy Industries
Telnet: l0pht.com
FTP: ftp.l0pht.com

Subscription Information
Individual: $15/year (published bimonthly)
Corporate: $80/year
Canadian: US $25/year
Overseas: US $30/year

Equivalent trades of similar periodicals, interesting electronic equipment, office supplies, envelopes, and 32 or 55 cent stamps accepted in lieu of monetary payment.