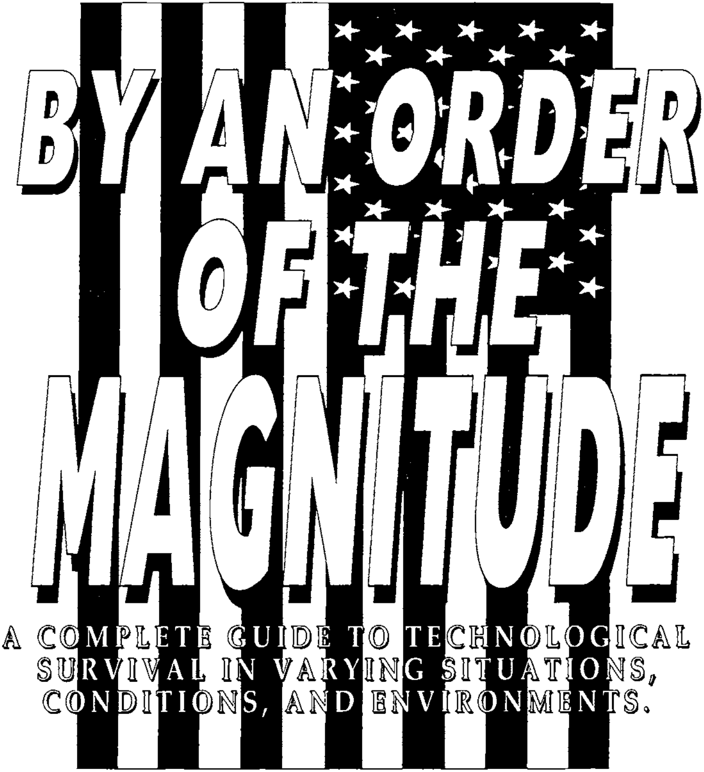


BY AN ORDER OF THE MAGNITUDE

A COMPLETE GUIDE TO TECHNOLOGICAL SURVIVAL IN VARYING SITUATIONS, CONDITIONS, AND ENVIRONMENTS.

Thomas Icom; OCL/Magnitude: Cybertek
John J. Williams, MSEE; Consumertronics
Cliff Williams, Consumertronics

TABLE OF CONTENTS

INTRODUCTION 2
ITS NOT WHO'S RIGHT BUT WHO'S LEFT 3
SOLUTION #1: GO BERSERK! 6
RESISTING OPPRESSION 8
ALTERNATE NEWS GATHERING 11
PRIVACY 14
ALTERNATE IDS 18
THE ART OF CONCEALMENT 19
VOICE INVERTER CIRCUITS 20
SURVIVAL LOCKSMITHING 21
SURVIVAL COMPUTERS 22
CRYPTOGRAPHY 24
TELECOMMO TECHNIQUES 26
INTERCEPTION OF TELECOMMO 35
WHO'S LISTENING 37
"RADIO SHACK REALITY" 40
ELECTRONIC WARFARE 41
SURVIVAL PREPARATIONS 44
TYPICAL SURVIVAL SITUATIONS 46
NUCLEAR, BIO, AND CHEM WARFARE 51
URBAN SURVIVAL 51
SELF-DEFENSE/OFFENSE 53
HARASSMENT-REVENGE 62
VEHICLE MODIFICATIONS 64
BETTER LIVING THRU CHEMISTRY 64
EXPLOSIVES AND DEVICES 66
SHORT TOPICS 67-69
SURVIVAL INVESTMENTS 67
URBAN SURVIVAL RULES 67
HOW TO NEUTRALIZE BUREAUCRATS 68
IMPORTANT MATERIALS 68
WILLIAMS COMBAT PRINCIPLE 69

INTRODUCTION

This book is about "TECHNOLOGICAL SURVIVAL" (also metimes known as "*Cyberpunk*"). The term was originally and turistically coined by John Williams in the early-1970s during the set of the first Energy Crisis. Note that his was all before home mputers and advanced telecommo came onto the scene. People ere interested in how to survive the skyrocketing prices and fuel ortages and outright rip-offs. CONSUMERTRONICS came out ith their publications on energy, and with that, started to use Technological Survival" - the use of technology to better one's life d to survive varying uncertain situations ranging from shortages rip-offs. Later, when CONSUMERTRONICS wrote such assics as "Tone Deaf" (a secure phone commo manual that got im threatened by Bell South Security goons and the goons hysically tossed out of his home), "**Stopping Power Meters**" which got him on CBS "**60 Minutes**" and a visit by the power ompany).

Meanwhile in 1984, William Gibson wrote "**Neuromancer**". his book about computer hackers and other high-tech people in e distant future, created the term "*Cyberpunk*", which basically as an attitude that people should grab onto technology with both ands and hang on. This culture was embraced by a small group of omputer hackers a few years later, who adopted the name. These re people who learned about the practical aspects of all types of echnology to better their lives.

That is the purpose of this book, to teach you how technology an help you out both today and in the future. William Gibson, ohn Williams and other Cyberpunk authors wrote of a dark uture: How people with high-tech skills and equipment improved heir lives and maintained their humanity during those roublesome times. Much is still wrong today and are getting even vorse. With the information in this book you can use technology o effectively - often fantastically - defend yourself and loved ones gainst attack or invasion, see through the media smoke screen to ind out the REAL news, obtain privacy against interlopers ranging rom big business to common snoops, live the way you want without interference, stay hidden from view yet still keep in touch, nd get justice when all other measures have failed. In short, this ook will help you get freedom, prosperity and security, and the neans to keep it.

One last thing, with knowledge comes responsibility. Please don't give technological survivalists and Cyberpunks a bad name by using these techniques indiscriminately and-or to harm innocent people. If you want to harm anybody, harm those whose put us in this mess to begin with: The energy, banking and insurance bigshots. Use common sense and try alternative methods before you resort to anything extreme. That's how this country was founded, and for the most part still works. GOD helps only those who help themselves.

---- **Thomas Icom**

People have always been fascinated with the unusual, the forbidden, the hard-to-get, the controversial and the thought-provoking. And people have always been interested in gadgets that will give them some advantage, whether it be for their pleasure or to succeed in a very competitive world. We are a materialistic people. We surround ourselves with far more material things then we absolutely need. The interest in knowledge and gadgets have a profound effect upon survivability. You can bet that the first person who made a spear and remotely killed a stronger enemy or difficult game became very popular and successful in his tribe (or the big-shot who stole his invention). And his tribe prospered. Soon, you had entire regions conquered by or in the control of the Spear-Making People.

Of course, the "government" of the Spear-Making People didn't want the knowledge of making spears indiscriminately distributed among the people. It was branded as knowledge forbidden to certain members of the tribe (ex: the middle and lower class, slaves, women, etc.), as a "military secret". And those who were not "cleared" to possess this knowledge/gadget and found with it were summarily executed.

The spear-making knowledge was so heavily guarded, even the CAPABILITY to possess the knowledge/gadget was denied. The bigshots of the Spear-Making-People would condemn anyone who just HAPPENED TO HAVE a straight stick lying around, or a sharp piece of flint that MIGHT be used to shape a stick. Or who happened to DISCUSS with an informant on how spears were made.

Still, in spite of the great risks, survivalists of that time recognized that it was far better to take the chance to gain the knowledge of spear-making than to go on with a bleak future without it. Fortunately for mankind but unfortunately for the bigshots of the tribe, the knowledge of making spears eventually did get wide circulation, and it wasn't long before other peoples were making spears - even improved versions - and by doing so could assure their own survivals.

Clearly, the only thing that has really changed since the days of the Spear-Making People is that the body of the forbidden knowledge has vastly increased. The bigshots are still there saying, 'you can't read this and you can't use that.' Even the capability to read has been denied of certain people in recent history. And you can be arrested by simply possessing the parts to certain forbidden things.

It's now clear to most people (it took some time for most people to realize this) that we are living in times of great upheaval and danger. The danger dominates every level of our lives. You can't walk thru a park at night, you are routinely robbed and surveilled by financial institutions, you can't get decent medical care, the educational system sucks, the Government is crooked as hell, foreign "investors" are taking everything over, and a total economic collapse will probably occur before the millennium.

And you now realize that this upcoming "depression" will be so great as to make the Great Depression look like a Sunday picnic in comparison! And that because of the erosion, destruction and sell-out of our economic and industrial bases, the probability of recovering from it as a united and prosperous country is bleak! Today's very high level of homelessness of families is just a small precursor of what's coming up!

More and more, people are realizing that they better prepare to survive or expect to perish. They're will be little mercy for those who can't or won't come up to speed. And surviving today and these upcoming catastrophes have nothing to do with what is fairest or what is best for the people or who is most deserving. Even the world's finest violinist can be killed by 250 pounds of pig slop with an AK-47 and a room-temperature IQ! The only thing that will matter will be who is the best prepared to survive the situation of the moment - nothing else!

Survival of the fittest does not exclude everyone who doesn't have an 18" bicep. More important than physical strength will be mental strength and sound preparations. When the "shit hits the fan", those who are highest up on the learning curve will be, on the average, far more successful at surviving and prevailing than all other people!

BY AN ORDER OF THE MAGNITUDE was created for the purpose of providing you much of the information you will require to not only survive the upcoming catastrophes but today's increasingly hard times. It is published only by CONSUMERTRONICS. It is written by "ICM" and JOHN J. WILLIAMS (of CBS "60 Minutes, National Enquirer, New York Times, and Forbes Magazine fame), and is contributed to, illustrated, and edited by CLIFF WILLIAMS.

BY AN ORDER OF THE MAGNITUDE is sold by CONSUMERTRONICS *for educational purposes only.* Altho illegal devices and methods are described, we do not recommend or imply any illegal applications whatsoever.

----- John J. Williams

IT'S NOT WHO'S RIGHT BUT WHO'S LEFT!

Survival has ALWAYS depended upon one's ability and capability to survive. It has nothing to do with who is right or wrong. And one's ability to survive is becoming more crucial every day.

I feel very fortunate to have grown up in the 50s and 60s, and I feel very sorry for my many young readers who weren't around during those times. Because our freedoms and life-styles are being eroded gradually on a daily basis, the losses are sometimes hard to recognize over short periods of time. However, since the 50s and 60s, the cumulative losses are now enormous.

Consider how things were back then and how they are now:

(1) THEN, you were a much-freer person. NOW, every phase of your life is controlled. Perhaps this area alone makes me feel the greatest amount of sorrow for the young people of today. Only few of them will experience what it is really like to be FREE. I can think of the countless hours I spent as a teenager and young adult hunting just about anywhere I wanted to with any weapon I could afford, shooting off the most powerful fireworks and homemade rockets, drinking Coors down by the Colorado River, swimming nude in spots set-aside for young adults, and running wild and having just a good 'ol time. NOW, you can't fart without a permit! You can be arrested for possessing a sparkler. There is almost nothing you can do without either breaking a law, endangering your life because somebody will mess with you, or paying a huge user-fee, tax or insurance premium.

Every second of your life is now surveilled by big Government and big business. If you don't believe me, get a hold of your credit report from your local Credit Bureau and learn just how much you are really being spied upon. (Don't pay for the report; instead, apply for an outrageous loan or Credit Card and then demand a free copy after being turned down).

I consider the loss of our freedoms to keep and bear arms to be the most offensive and dangerous of all of our losses of freedoms. The intent of the Second Amendment is crystal clear: Our Founding Fathers intended for every fit adult male (as females did not serve in the militia at that time) to possess, train in the proper use of, and to use as required to defend freedom, not only guns but rockets, explosives and artillery (as these are all classified as "arms" that existed at that time). And for over 100 years, that's how the Second Amendment was largely interpreted to mean. (see our ROCKET'S RED GLARE manual for more info)

However, our judiciary is now so corrupt and controlled that I doubt if you will find a Federal judge anywhere that will admit to the truth when in comes to Second Amendment issues. Now, even single-shot hunting rifles are threatened. You won't even be able to hunt with lawn darts - because they're illegal too! Your right to keep and bear arms is that thin blue line that protects every other right defined by the UNITED STATES CONSTITUTION.

And if you think that you have true First Amendment rights - think again. As publishers of very controversial works, I can tell you that the extent of your First Amendment rights largely depends upon whether or not you own a press. And even then, it only barely exists. For example, since first publishing AUTOMATIC TELLER MACHINES in 1978, (updated annually) my life was threatened by a banking/ATM newsletter publishing out of the Twin Towers in New York, efforts have been made to strong-arm the AG of New Mexico to put us out of business, banks have refused us loans and have cancelled accounts on us based upon lame excuses, and at least one major banking and ATM organization, Security Pacific (worth $77 Billion), has been snooping into our Credit Bureau records. The only First Amendment rights you now have are those accorded to you by bigshots.

WHO TO BLAME: We have progressively been moving into a slave state. The people behind this movement are just about everyone in a position of power. By controlling you, they can better force you to do THEIR wills - and destroy those they don't feel are sucking-up enough. And once they've got your guns, the only thing you are going to be able to use your hands for is to try to cover up your genitals when the bigshots get around to herding you into the "showers."

At first blush, it seems ironic that while officials everywhere are publicly applauding the crumbling of the communist dictatorships of the Soviet Union and Eastern Europe and the fresh breath of freedom now blowing thru those lands, while at the same time, doing everything within their power to erode and destroy freedom in the "Free World." But the truth is that the multinational big-shot capitalists just can't wait to subject their youths to flipping burgers for a living, paying thousands of rubles in car insurance for the "privilege" of driving, and getting ripped-off by the credit card companies.

(2) THEN, it was, *"Ask not what your country could do for you but what you could do for your country."* NOW, it's, *"I've got mine, so up yours!"* Now, there are no rules. Whatever you can get away with - by hook or by crook - is 100% OK. The end justifies the means. You are only wrong if you get caught, prosecuted and imprisoned without being able to buy, bullshit or muscle yourself out of the situation.

WHO TO BLAME (or to credit): This has always been the attitude of the rich and powerful. They have always demanded that ordinary people keep on the straight and narrow, while at the same time they have robbed, cheated, gouged and lied to anyone and everyone they could to gain enormous wealth and power. Nothing makes a big-shot bolt-up in bed in the middle of the night soaked in a cold sweat faster than the fear that the people will find out that they are being ripped-off and will take the law into their own hands.

(3) THEN, altho the "justice system" has always favored the rich, there were many honest and decent police officers, prosecutors and judges, and your prospects of getting a fair trial or justice if you or a loved one were the victim of a vicious crime, were much higher. NOW, most prosecutors and judges are bought off. Even horrendous white collar crimes are treated with kid gloves - if not ignored altogether. Rob $ Millions from an S&L, bank, Pentagon contractor or government agency, and the police, prosecutor, judge and you will grin and wink back and forth at each other until the charges are dropped or reduced to something ridiculous. And if you are convicted by some rare fluke, you will be fined a small percentage of the rip-off and required to do something really punitive like, "community service."

WHO TO BLAME: Enforcers of the legal system are bought and sold like condoms over the counter. Now, police commissioners, prosecutors and judges, and dope dealers all live in the same neighborhoods, fart at the same uptown parties, belong to the same clubs, move in the same social circles and send their kids to the same schools. They spend so much time sucking up to each other it's a wonder they can get anything done! If you are part of the clique, no crime is too great to get you punished. If not, no crime is too small to get you harassed. And if you are young-and-on-your-own, have an unacceptable hair style or a beard, are poor or lower middle class, and- or are non-Anglo, they don't even bother to unscrew the lid from the jar of Vaseline!

(4) THEN, you could get out of high school or college, find a decent job, get married, buy a home, and experience the AMERICAN DREAM. NOW, the probability is very high that you've got to set- up household with a minimum of one other full-time worker, you don't have a prayer of becoming self-sufficient trying to "earn" a living, and the only house you will live in is one owned either by your folks or the landlord. Over the last 8 years, while the costs of food, energy, insurance, medical care, etc. have each doubled, tripled and quadrupled, minimum wage has barely increased! Altho most people don't earn minimum wage, most people get paid based upon a scale related to minimum wage. Because minimum wage is so pathetically low millions of young people in particular have been robbed of their futures. During these same 8 years, the wealthiest 10% of our society have made off like bandits.

WHO TO BLAME: The blame here is clearly the huge political influence of bigshots in the business community. They outright own just about everyone who's job can be defined as political. If they need a blow job, they get on the phone and ring a State Senator and five minutes later he is at their door salivating like mad. If they need a 25% auto insurance rate boost - it's as automatic and as evil.

(5) THEN, you could easily find a decent, full-time, permanent position with decent benefits. NOW, you're lucky if you can even find a job. And if you can, it's probably part-time and-or temporary with miserable pay and-or few or no benefits. And if you can, it's probably because you've got a relative or friend who got you in, or you spread your legs for somebody. Getting a good job these days has a lot more to do with who you blow than what you know. And even if you do find a "good job" with good benefits, your employer can now LEGALLY rob every dime of your retirement fund - leaving you homeless and destitute - thanks to a Federal law passed by Congress. (see our ULTIMATE SUCCESS MANUAL on how to lie, cheat, and steal your way to the top of the corporate ladder.)

WHO TO BLAME: Again, the captains of our industries and institutions, and their kiss-asses in the Chamber of Commerce, who are not going to be happy until 90% of the population is literally enslaved.

(6) THEN, you could drive a car for a few dollars per week. Gas was cheap and you didn't have to buy insurance. NOW, gas cost you a fortune and the insurance companies have fixed it so you can't drive a mile per year without paying $1,000+ in premiums. Their system is very simple: They bribe state legislators requiring you to buy car insurance. The police powers of the state then become Mafia-style enforcers to force the collection of the insurance. They then jack up the insurance rates at least 2-3 times the inflation rate every year. For providing millions of people absolutely nothing except a box-full of worthless receipts, they steal $ Billions from them - totally legally without you having a single recourse under the law to stop them and still be able to drive.

The insurance industry is now so powerful that they can even deprive you of your say at the ballot box. California is an ample example of that, where the insurance industry has virtually defeated any referendum to reduce insurance costs. If the California referendum authors had been smart, they would have written the referendum to read, "No State law can be passed or enforced that requires or compels a resident to purchase auto insurance without the State itself providing that insurance at no greater than 1% of the resident's annual net income." Then, the insurance industry would not even have a legal leg to sue on. As a matter of principle and just plain fairness and decency, no law should ever require you to obtain something unless the state provides that product or service to the public at a reasonable cost.

WHO TO BLAME: The insurance companies. Oh, sure they blame the lawyers (another group of swindlers). And the lawyers are partially to blame. But it is the insurance bigshots who bribe politicians to pass laws requiring you to get insurance - not the tort lawyers. They also blame the car crash victims, so you known how much to believe them. The truth is that insurance companies are parasites, and they suck a greater percentage of your blood every year.

What I can never understand is that the same underpaid and underappreciated middle-class police officer - who is equally victimized by the insurance bigshots - initiates the process by ticketing drivers for not being insured. The insurance bigshots must surely be slapping their knees and horse-laughing up at the country club over the fact that they can get some big, burly police officer, who will risk his life to bring down a drug dealer with an Uzi or rescue a child from a burning building, to do their dirty work for them like some whimpering dog who has been beaten into submission!

(7) THEN, you could swim in a river that was clean, breathe fresh air, and eat wholesome foods. NOW, most things have turned into garbage. Everything is purposely polluted or poisoned. Birth defects and illnesses are at epidemic levels and increasing daily. Where there used to be wide-open virgin forests and clean and pure bodies of water, you find fences, mining operations, erosions, chemical spills and trash.

WHO TO BLAME: Virtually all of us must share the blame here, but some of us much more heavily then others. These are the captains of our industries and institutions and the bigshots who protect their interests. It is up to us to protect our environment in our day-to-day activities, and to insist that big-business and government also protect the environment. I don't care how big of a big-shot you are, you and your loved ones live on this planet too - and you are never going to escape from that fact. What goes around comes around.

(8) THEN, you could find an attractive person, have sex with her/him with the only fears of the girl getting pregnant - with a much less concern about venereal disease. And even if you got VD, it was virtually always curable. NOW, have sex with the wrong person, and two years later you might be down by 50 pounds, with sores all over your body, and nothing to look forward to except death!

WHO TO BLAME: My view is that AIDS (and probably a couple of other newer VDs and versions) resulted from government biologic warfare experimentation. The question is which government? I doubt if we will ever know. Probably several have done this to us.

(9) THEN, 90+% of all American businesses were owned by Americans. NOW, most of our big businesses (and many smaller ones) are owned and controlled by foreigners. For example, nearly one-third of all U.S. banking assets are now foreign-owned. That means, every time you make a credit card payment, a substantial portion of it is sucked off by some billionaire foreigner sitting on his fat ass in London, Bonn, Tokyo, Montreal or elsewhere.

WHO TO BLAME: Our Government. Political bribes have produced legislation and regulations that allow foreign bigshots to sodomize every American man, woman and child.

The solution is simple:

(A) Confiscate all foreign-owned properties.

(B) Disavow and cancel all U.S. debt owed to foreigners.

(C) Make it a capital crime for anyone or corporation to make any kind of interest, dividend or similar payment to a foreign entity.

(D) Cancel all passports owned by foreign businessmen and lobbyists.

(E) Make it a capital crime to accept any donation, contribution or gratuity from a foreign source.

Our great nation is in an emergency situation. If we don't act very soon on this matter, we will end up like India, where you have millions of half-starved people turning out trinkets in their back yards.

WHAT TO DO

I don't mean to imply that America is totally rotten. Or to imply that the solution is to destroy it or even to overthrow its Government. Most of our major corporations and institutions are rotten to the core and MUST be replaced or destroyed. However, by and large, the average American citizen is still a good, decent human being. And our CONSTITUTION is the best that has ever been written anywhere. And the framework of our Government is a solid basis to build upon.

I've asked myself, "What would our Founding Fathers do if they suddenly returned?" Heros like George Washington, Sam Adams, Pat Henry, Tom Jefferson and Ben Franklin. First of all, they would be highly pissed. Second, they would kick a hell of a lot of ass. Do you think that if Sam Adams lived today, he would be saying, "Yo dude, don't bother me about that. I've got to get up at six to get those fries going."?

I like the ways that the great Mexican revolutionaries Porfirio Diaz and Emiliano Zapata expressed it, "It is far better to die on your feet than to live on your knees," and "Go not to a tyrant with your hat in your hand, but with a rifle in your fist." Call me old-fashioned if you will, but it is my belief that the DECLARATION OF INDEPENDENCE fully legitimizes ANY action that the American people choose to take to change their Government or to correct the abuses of power.

As one person or as a small group, you are virtually powerless to do anything within the law to effect reasonable changes in our society. How about the vote? Sure. You get the choice between two or more crooks - if even the incumbent crook is challenged at the polls. That doesn't mean that you shouldn't vote. Always vote - even if you have to choose a significantly lesser evil - or write in your vote. I am a big believer that evil must be challenged in every direction - even if your chances of success are small or the expected gain is small. The vote has occasionally worked. Better yet, organize political forces and candidates that represent YOUR views. Hopefully, those views will include the absolute critical need to preserve the BILL OF RIGHTS - including the implied right to privacy.

Get even. If somebody rips you off or someone you love, get even with them. I make a practice of carrying around certain items that I can use to get even with somebody who's done an injustice against me or against a family member or friend. You would be surprised how handy Crazy Glue, DMSO gel laced with certain substances, razor blades, ice picks, toothpicks, piano wire, etc. can come in handy when you have to deal with a real shithead. Your bank ripped you off? That could be so disturbing to you that you might accidentally reach for a slice of processed cheese instead of your ATM card.

One really neat method (I found in a newspaper called, FULL DISCLOSURE consists of wetting a sponge (natural one preferred), squeezing it dry, and while still moist, tightly binding it with a string. After it has thoroughly dried, you cut off the string. The result is a real tight sponge ball. Be careful not to flush it down any toilets as it could expand and lock itself into position, resulting in a very messy situation and expensive repair. Another really neat toilet method of dealing with a shithead (see our ULTIMATE SUCCESS manual) is to lift up the toilet seat, stretch a piece of Saran wrap across the toilet bowl and close the seat. This trick is so nasty, don't even try it on your worse enemy.

In carrying out your mission, if I may, I have some suggestions:

(1) HONOR IS IMPORTANT. While there are many who will rip-off or vandalize anyone, if you want to accomplish a noble goal, you must select only those most deserving of your attention and leave innocent people alone. For example, if a person robs a bank to get rich, to me he's just a common crook that should be locked up. But if he destroys a bank that's largely foreign-owned or that's stealing homes, businesses or farms, to me he's a hero.

(2) NEVER TAKE CREDIT FOR WHAT YOU'VE DONE. Defending freedom is not a humorous matter or something that you brag about. If you want to brag, brag about your bowling scores. In fact, when it comes to personal type actions, it is almost

always far better to act alone or in small groups and to never tell anyone.

(3) DON'T BICKER OVER PHILOSOPHY. If you have a common enemy, the first thing you must do is unite and destroy that enemy. Then afterwards, sort out the particulars. That's basically what the freedom fighters did in Romania. And in Nicaragua. They saved their country first, and now they are going thru the re-birthing process, painful as it always is. That's why I repeatedly state that, "It's not who's right but who's left." You can go literally nuts - not to mention miss the entire point - trying to figure out what has the greatest claim to righteousness. Or on how many angels can fit on the head of a pin.

And always keep in mind that your enemy is very clever. He will plant among you spies and provocateurs. A classic example of how well they did this was during the Vietnam War. The truth is, that most of the blame for the Vietnam War belongs to the oil companies that had rigs off of the coast of Vietnam, pumping oil like mad during most of the war.

You didn't know? No mystery to that. It was kept out of the media. And the oil companies continuously paid off the communists to leave their operations alone (it has also been reported that they provided the communists with intelligence). The communists then used these bribes to buy Soviet and Chinese weapons to kill our heroes. This may come as a shock to you, but Valdez was not our first experience at being ripped-off at the sign of the double-cross.

But who was actually blamed for the war? Why it was the American fighting men and women who served in that war. Why were they blamed? Our fighting men and women were blamed primarily to take the pressure off of the politicians, military brass, defense contractors and oil companies. They were also blamed to cheat them out of jobs and VA benefits upon their return home. The widespread belief was that they were doped-up, infected, baby-killers - thus undeserving of decent employment and VA benefits.

Who carried out the execution? That job largely fell into the hands of those "freedom-loving hippies" that protested the war. Altho many Vietnam War protesters were sincere in their beliefs, the movement itself was largely dominated by rich, spoiled, yellower-than-fresh-manure, draft-dodging slimebags whose real agenda was to dishonor and destroy the decent men and women who served in that war. The only thing I can blame on our heroes was that they were entirely too naive and trusting in their Government. As was I then.

The Vietnam War should have taught everyone first of all not to trust your Government (for that matter, not to trust ANY Government). Second, it should have taught you to see thru the bullshit and read between the lines, and to never to lose the sight of who the real enemy is.

(4) SUPPORT THOSE WHO ARE LOYAL OR HELPFUL TO THE CAUSE. I hate to sound like I'm tooting my own horn, but it is very important to support those entities important to the cause. Not just us, but others like CYBERTEC MAGAZINE, 2600, HACKER'S QUARTERLY, FULL DISCLOSURE, etc. There aren't that many of us around, and the risks and pressure we take are enormous.

THE AUTHOR & CONSUMERTRONICS

The information provided herein is provided for educational and entertainment purposes only. Views expressed are those of the author, John J. Williams. John is the founder and proprietor of CONSUMERTRONICS, in business since 1971. CONSUMERTRONICS offers 200+ books, manuals, software packages, hardware items and services. Order our new Top Secret Catalog today for more info!

CONSUMERTRONICS best known works include:
CELLULAR AND CORDLESS PHREAKING, COMPUTER PHREAKING, BEYOND VAN ECK PHREAKING, BEYOND PHONE COLOR BOXES, SECRET & SURVIVAL RADIO, AUTOMATIC TELLER MACHINES, CREDIT CARD SCAMS, HIGH VOLTAGE DEVICES, ELECTROMAGNETIC BRAINBLASTER, ROCKET'S RED GLARE, STEALTH TECHNOLOGY, POLYGRAPH DEFEATS, STOPPING POWER METERS, LIBERATE GAS & WATER, GAS FOR' ALL!, RADIONICS MANUAL.

SOLUTION #1: GO BERSERK!!

If you were to pinpoint the single biggest root cause of everything that is wrong in America today, you would be pointing to the fact that the vast majority of Americans are complacent, compliant, apathetic and stupefied when it comes to wrongdoings. Because of the lack of public outcry when even serious wrongdoings occur, wrongdoers increasingly get away with it, and the general level of wrongdoing in a society increases.

An excellent example of how wrongdoers now get away with even major crimes is the S&L crisis and bailouts. Big-shot crooks running the S&Ls lined their pockets with Hundreds of Billions of Dollars that the taxpayers will be soaked for over the next 30+ years. Yet, the outcry over this astronomical scandal was minimal.

Gone are the 60s when militant young people eagerly protested just about every wrongdoing they perceived. Now, we are a nation anethesized by our entertainment electronics. We sit down in front of our electronics - fat, dumb and happy with the expectation of experiencing one or more new and exciting contrived sensations every day.

We have become a nation of mental paraplegics! We are now at or near the point that, if told to do so, the majority of Americans would compliantly strip down naked and march into the gas chambers.

We have become a nation of sheep, and shepherds are one-by-one leading us into the barn to nail our hooves to the floor, and do whatever they want to us. Afterwards, we stagger back to the herd with a shit-eating grin on our faces, as if nothing happened, only to be singled out again when the next shepherd gets a hard-on.

Every day I hear or read about just how incredibly wimpy we have become as a nation. The last story I heard was of the businessman and his wife who were persecuted by the IRS for an assessment of $70,000. Nine years later, the IRS, thru their outrageous system of interest and penalty rip-offs, jacked up their alleged $70,000 debt to $300,000. And the fight against the IRS had cost them $70,000 in legal fees, their home and all of their other property. The businessman became so desperate that he committed suicide to leave his wife $250,000 in insurance benefits to pay for the court battle. Shortly thereafter, the judge ruled that they didn't owe the IRS a dime. The "legal system" prevents the widow from recovering a single dime from the IRS for the outrage they had committed against her family!

I'm talking about the AVERAGE American. Fortunately, there are still a few very courageous people who vigorously complain about and fight wrongdoing. Unfortunately, because they lack the mass of public support that their efforts are usually so deserving of, they are usually ignored, harassed and persecuted with impunity by the Government or by big business.

And unfortunately, because of the Byzantine, extremely expensive and corrupted legal system we are now saddled with, only a small percentage of wronged people can ever hope to obtain justice or redress their grievances thru the legal system. Our legal system is supposed to work on the principles that there are, "Justice for All," and that, "Justice is Blind." Both of these principles are absolutely critical to a fair and just legal system. Unfortunately, both are largely and routinely ignored or subverted in virtually all jurisdictions. Just try to get an attorney to handle your case pro bono.

I can find no statement in the U.S. CONSTITUTION that states that if you cannot afford LEGAL justice, you must quietly suffer with any injustice dealt to you. The fact is that in many cases and for many people, the only reasonable way to obtain justice in this society is to obtain it thru EXTRA LEGAL or ILLEGAL means! Clearly, if society intended to relegate justice solely to the legal system, then it would require and provide a legal system in which all justice could be reasonably obtained from it by everybody.

In many cases, by applying principles of creative vengeance, you can obtain a semblance of justice for wrongdoings committed against you. Our society now is so complex, controlled by information stored about you and everyone else in databases, so inflexible and so out-of-control that you can, if you really put your mind to it, mess up a wrongdoer royally just by spreading the wrong information about him.

A classic example of how to do this is the ploy used by tax protestors and others to get back at those who they have perceived wronged them. They get their revenge by filing a Form 1099 with the IRS against the perceived wrongdoers. They use this form to report to the IRS that they have given their targets large sums of money (sometimes in the millions of dollars). The Form 1099 automatically flags the targets' tax filings with the IRS, usually resulting in one or more audits. Since the targets will be unaware of this money if false and unlikely to report it anyhow if true, they will not have likely reported this unusual income to the IRS in their filings. Consequently, when they are audited, they'll have a lot of explaining to do. And since the IRS loves to compound things whenever they can, they'll closely scrutinize the targets' filings for ALL mistakes and wrongdoings, probably over several years.

The best way I know of to royally mess somebody up is to give him cash (particularly over a couple of years) which you can prove you gave him and which you are sure he won't report on his taxes, and then file Form 1099s on him. In fact, you are LEGALLY obligated to file the Form 1099s because the IRS requires an absolutely complete and accurate accounting of your income and expenses.

Paying a wrongdoer difficult-to-explain money can be done without him even knowing it. If you feel that he is forcing you to pay him bribes, and you can find a banking account number for one of his accounts, you can conveniently pay him the expected bribes by depositing them directly into his account. You then keep the deposit receipts. Since he won't have this INCOME on his regular books, by later (about 3 years later) filing a Form 1099 and turning over your receipts to the IRS, he's going to have a dickens of a time explaining why he was forcing you to bribe him and then not reporting the bribes to the IRS. Even if he is not criminally prosecuted, still it's unreported income he SHOULD HAVE known about, and will very likely have to pay taxes, interest and penalties on it.

Even if the wrongdoer does discover the mystery income, he is still going to have a dickens of a time explaining the source of this income on his tax forms (and if he takes that tact then you will have proof that he knew about the bribes all along and accepted them). This will likely get his filings flagged and audited. Not to mention the nightmares it will cause his accountant and tax preparers - all with their meters eagerly running.

Finding a bank account number is usually no sweat - particularly if he owns a business. You simply go to the business and buy something with a check. When the cancelled check is returned to you with your statement, you find his account number on its reverse. If he is a private person and you are a business, you can send him a "refund" check, which he will probably deposit. If you are concerned about him knowing about you (and thus becoming suspicious), use a Postal Money Order (write on the back, "For Deposit Only"). Then later report it lost or stolen and ask the Post Office to provide you a copy of it.

Another method is to use outright sabotage against the wrongdoer. Krazy-Glue applied to locks, and toilet wreckers are typical methods here.

Other methods are limited only by one's imagination. There are many good ideas found in the current collection of revenge books. Methods used to ruin a wrongdoer's reputation and to get him into big trouble with various important people like the police, banks, insurance companies, creditors, his neighbors, etc., again limited by one's imagination.

Some of the best forms of revenge require in-depth personal knowledge about the person. Ideally, to start with, you should have a person's Social Security Number (SSN), his birthdate, and his first, middle and last names. From this information, you can go to any "information company" (a company that sells its access to various databases, they advertise in the Yellow Pages under "Computer", "Data Processing," "Security," "Credit" and "Investigative" Services headings) to find the wrongdoer's current and previous home address(es), place(s) of work, position(s), criminal record, financial condition and spouse(s) and other family members. These services can run you anywhere from about $100 to $1,000.

On a practical basis, if you know the person's first and last name and middle initial, and either their birthdate or SSN, you can usually get the rest of the information for very little or no extra cost. The only time that this doesn't work is if the person has a common name, then the middle name is usually also required. Also, if you know the make and model of the vehicle the target drives and its license number, in most states, you can obtain a copy of the target's auto registration (which provides his full name, address and other information), for about $5 from DMV.

Using the information gained, you can raise royal hell with the wrongdoer, in most cases. You would be surprised to find what lurks in a person's closet by even doing a minimal investigative effort. And once you know a lot about the wrongdoer, you can "become" that person for the sake of obtaining justice for a serious wrongdoing.

However, there are many occasions in which a wrongdoing will be committed against you by someone whom you either don't know who the actual person wrongdoer(s) is (are) or by a known wrongdoer that is remotely located or so highly positioned and protected that you can't use most of the normal methods of obtaining justice. For example, if a top executive of XYZ MEGA CORP causes an action or policy that rips you off, who at the giant conglomerate do you get back at when you know nothing of that person?

Or what if the wrongdoing against you and your loved ones is so vile that any malicious mischief you cause against him does not provide a comparable measure of justice?

For whatever the reason, you may find yourself in a situation so extraordinary that you must, as the BIBLE says, "gird up your loins" and take THE ULTIMATE STEP. Nothing new here. Basically, this is what you do when you are in a combat situation. The objective of your enemy is to destroy you, your loved ones and your way of life. You don't think twice about using a weapon to kill that enemy. Your Government even trains and rewards you for doing so. Or a criminal breaks into your home, again to destroy you, your loved ones and your way of life. You don't think twice about picking up a weapon to kill the source of the threat, and you are fully justified in doing so.

In some states, in fact (ex: Texas), you can gun down a murderer whose crime you witnessed, in the street in broad daylight in front of many witnesses - even if he is of no threat to you, your loved ones or your property - and go scott-free! Clearly, the legal principle is well- established that you can react very violently to wrongdoings that directly affect you and, in fact, to those that don't directly affect you!

And clearly, it is occasionally necessary to react to a situation in such an extremely violent manner that the lesson taught will have a very long-staying power. Other similar wrongdoers will then think twice about messing with others in your situation. It is my belief that the occasional act of someone going berserk has a much greater benefit to the general public than all of the usually wasted efforts of trying to use legal and political methods to resolve wrongdoings.

To destroy any wrongdoer who is trying to destroy you, your loved ones and your way of life is 100% justified. *Just as for any important other decision you make, certain guidelines should be observed:*

(1) The wrongdoing must be so serious that it justifies the ultimate step. And the wrongdoing against you and yours is not something that is justified, or is way out of proportion to what would be justified for any wrongdoing you may have caused the wrongdoer.

(2) You have done everything reasonably possible to convince the wrongdoer to leave you and yours alone and to compensate you for any outstanding wrongdoing.

(3) You have unsuccessfully tried every LEGAL method that is reasonably at your disposal to prevent the harmful effects of the wrongdoer and to obtain justice for those harmful effects that have

already occurred.

(4) As in (3), you have tried every EXTRA LEGAL method to no avail. Note that I am not a big believer in peaceful resistance. It's nothing but a crock. Ten people going independently and randomly berserk will accomplish far more ultimate good than 10,000 peaceful demonstrators, 1,000 speeches and 100 demonstrations.

(5) Your back is completely against the wall. You feel desperate and like a trapped animal. You may be even contemplating suicide. You should never allow a situation to get so far out of hand that suicide appears to be a rational alternative to any other solution - including the solution of going berserk.

Mexican revolutionaries of the last century and early part of this one had two expressions that clearly state how I strongly feel.

- *"It is far better to die on your feet than to live on your knees!"*
- *"Go not to a tyrant with your hat in your hand but with a rifle in your fist!"*

Just as there are guidelines for your reasons for going berserk, there are guidelines for the way in which you go berserk. *Consider:*

(1) Direct your wrath towards those most likely to be guilty of the wrongdoing against you and yours. Spare innocent people. In any major organization, the lower-level people are seldom to blame for anything significant even though they are usually the people a chicken- shit upper management uses to carry out their oppressive policies and actions. And of course, people not associated with the wrongdoer in any kind of direct sense are innocent people. For example, don't take it out on the postman because some giant corporation is persecuting you. And of course never take it out on children or non-feral animals. Use the principle that responsibility for any action increases with one's rank in the organization.

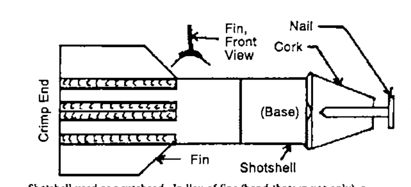
(2) When it comes to lower-level implementers of an oppressive action or policy, altho they may not be ultimately responsible for the action or policy, they are still responsible for the implementation of it. By knowingly implementing a patently oppressive action or policy it is then clear that whatever spills over onto them is a risk that they have assumed. Therefore, you should make it clear with the implementers that what they are doing is an oppressive wrongdoing against you and yours.

(3) Carefully plan your action, and tell no one - not even those closest to you. To be a most effective lesson, going berserk must be done on a random and unexpected fashion, done by an individual or a couple of individuals at most and involving no direct knowledge by anyone else. Whatever assistance anyone else provides you must be done so in an unwitting or unwilling fashion.

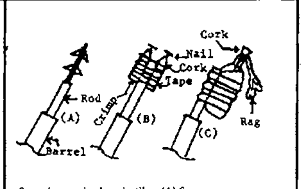
(4) Take no prisoners! The ultimate step requires the ultimate commitment and perhaps even the ultimate sacrifice. Just as the soldier in combat must be prepared to die in combat for his country, prepare yourself to die for your cause. Everyone eventually dies. And there are many situations in which it is far better to die accomplishing an important goal than it is to live and thereby ultimately accept a major wrongdoing. It is always far better to die for a cause (and in the process take some deserving bastards with you) than to live to a "ripe" old age and die soaked in your own urine in a nursing home.

RESISTING OPPRESSION

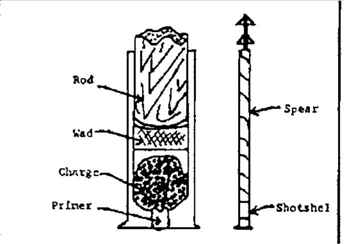
It was Ben Franklin who said, "An ounce of prevention is worth a pound of cure". Today, our freedoms are being ripped-off at an alarming rate - all supposedly in the interest of our own well being, safety and efficiency. One of Thomas Jefferson's many famous sayings was, "If you take away a little bit of freedom for a little bit

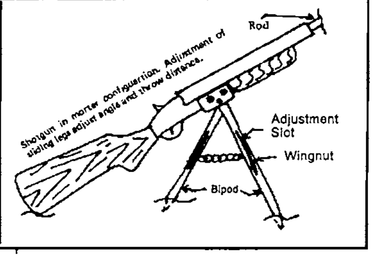


Shotshell used as a warhead. In lieu of fins (hand-thrown use only), a streamer can be taped onto the crimp end. Without a fin or streamer, only about 5% of those thrown landed on the nail first.



Some improvised projectiles: (A) Spear or arrow. (B) Shotshell warhead(s). (C) Molotov Cocktail (MC)




Rod
Shotgun in mortar configuration. Adjustment of sliding legs adjust angle and throw distance.
Adjustment Slot
Wingnut
Bipod

of security, soon you will have neither." Just by comparing the Founding Fathers to the current crop of snakes and buzzards we've been voting into office in recent years, clearly, this country has departed a great deal from the principles set back in the beginning of our country. What's even more disturbing is that the majority of Americans don't care, are too afraid, or even believe and assist our elected low-lifes in destroying our freedoms in exchange for a few drachmas or trinkets.

This chapter is for the perhaps 10% of you who intend to do something about it, and those who want to know how to hit the ground running when the shit hits the fan.

SCENARIOS

There are two main scenarios which would create the conditions necessary to justify resistance operations by the people. The first and most obvious is foreign power invasion. While this has been relegated to the world of science fiction, as you will see that it is still a distinct possibility - now even more so due to misleading recent happenings. The second, and a more immediate threat today, is the accession of a totalitarian government in this country.

THE SOVIETS

According to the Government and the media, communism is dead, the Berlin Wall is gone and democracy is returning to the Eastern Bloc nations. Or is it? Any survivalist worth his salt knows that there are three things in this country which you should distrust the most. These are the **media**, the **Government** and **Big Business**. As one who believes in freedom and self-reliance, they simply don't like you, want to take you for all you're worth and want to destroy or enslave you. Because of this, take everything they say with a grain of salt and learn to read between the lines.

A totalitarian communist government is still firmly entrenched in the Russia, they haven't significantly cut back on their military (only a few highly-publicized token efforts), and all of the good news coming out of there is manipulated and highly choreographed by the media.

On the contrary, massive U.S. military reductions as part of the "peace dividend" have left an even wider gap between the two countries. Also, when the Soviet Union made its threatening stance against the Soviet Republics after they declared their freedoms, we were sternly warned to stay out of their affairs.

Considering what's really going on today, a Soviet invasion could take place the following way: Over a period of a couple years, the Soviet Union seeks "better relations" with the United States. Token gestures are made and the borders are opened up. Hundreds of thousands of people cross over what was once the Iron Curtain, a great many staying in the West. Over these years the West greatly reduces it's military forces, but the Soviet Union doesn't. Thus we enter a short period of mutual peace and harmony with an even greater difference between the two super powers. After 5 or so years of this, with the help of our politicians and media, the Soviet's could launch a surprise attack with a 90+% chance of success. They could do it right now if they wanted to with perhaps a 60% chance of success.

They would start by mobilizing **Spetsnatz** (Soviet Special Forces) which have infiltrated into the NATO countries over the last years as refugees. They could also bring them in under the guise of cultural exchanges. Most Soviet artists and performers are KGB agents, and military service is compulsory there. Further, military forces could also be smuggled in under the guise of commercial transportation, something sure to occur with greater frequency between the U.S. and U.S.S.R. in the future.

The initial attack would be a mass targeting of strategic points in the U.S. using either low yield tactical nuclear weapons or conventional explosives such as Astrolite. These could either be smuggled into the areas or fired from cruise missiles just off the coast. Both types of at tack cannot be stopped by any defense system in use by the U.S. today! Cruise missiles come in at sea-level doing mach 2, under defense radar. Smuggled devices wouldn't be detected until they went off.

According to nonclassified sources, there are nuclear warheads which fit into a briefcase. One of those placed between the White House and Capital building would effectively take out the U.S. seat of government. Or a boat carrying one of these could get real close to DC by sailing up the Potomac and then launching. A "terrorist" group could steal an armored truck, load it with such a device and drive balls-to-the-walls into a missile silo site. The detonator could be set to go off when they reach the center of the base or via a dead-man's switch. One could even be a mile off target and still be effective. A large city could be hit by an Astrolite warhead, simulating a nuclear blast and causing widespread panic the police and national guard would be hard-pressed to control the people. They have a hard enough time as it is!

Drug runners smuggle in thousands of tons of drugs each day. How hard could it then be for the Soviet Union to smuggle in a couple of nuclear warheads via their Cuban connections? A moderate-sized Spetsnatz unit could fight their way into the Capital and-or White House and capture and kill Government leaders.

Killing can be by means other than the bullet. What about poison gas into the ventilation system? Or how about vaporizing a couple of gallons of a inflammable chemical while Congress is in session, and then detonating it? How about the water supply? All they'd have to do is get access. You can just walk into many of these places as the security is usually minimal.

Once an initial attack was made, mopping up would be relatively easy. The resulting civilian panic, combined with the fact that the heads of Government would be mostly wiped out, would leave whatever armed forces we have remaining stunned and in disarray. Combine that with the fact that most of the citizens would probably not do anything except panic, an external enemy has the almost perfect opportunity to invade our country and take over our Government.

Of course, there are a few hitches. The U.S. is a large country so that initial control will be relegated to high population areas. They would have the disadvantage of operating in unknown terrain. And out of the minority that would fight back, many are well-trained and heavily armed with small arms, and would be able to give the Soviets a very hard time. There is also a large technological base that would assist freedom fighters greatly.

Further, by freeing Americans from the choking hold put on it by our own current Washington Government, the people would certainly be able to function more freely and independently in their own defense. Actually, a takeover of Washington, DC by a foreign power might be the only means of clearing out the entrenched crooks and incompetents now there, and might rejuvenate the people to recapture Washington to install a fresh, new and representative Government.

Freedom-fighting is never the easy or safe thing to do. Unlike the resistance movements in the past that were supported by the U.S., we will have little support from the outside. Also, with our freedoms being taken away more each day, our capability to defend ourselves against a foreign invader is now severely limited and diminishing daily.

DICTATOR TAKEOVER

As high as the risk is for a foreign invasion, there is a much greater probability of an internal takeover by a dictator than by an invasion by a foreign power.

The disruption of the Iran-Contra conspiracy did not adversely affect the larger ongoing conspiracies to overthrow our Government (notice the plural). For example, consider the inroads made in recent years by a bunch of anti-gun nuts to get guns banned and confiscated. They originally started with handguns, and have now progressed up to semi-autos (as they say, "All firearms capable of being rapidly discharged"). They are also working to ban hunting, which would destroy what many people believe is a great need to use firearms (sporting purposes). On one end, they are working against your right to self-defense, and on the other they are working against the "sporting purposes" of guns. And then you have the nut cases who are burning the flag. The real intent behind the flagburning is to enrage the American public to call for a Constitutional Convention. Once a Constitutional Convention is called, any part of the Constitution can be changed - in fact, the entire Bill of Rights could be scrapped! You don't have to be a rocket scientist to figure out what's REALLY going on here!

One of the things that has kept this country free is the true meaning of the Second Amendment. No number of BS rulings from the courts on the Second Amendment will ever remove one iota of its meaning to the majority of the American people. Everyone of us are the "Militia", and no court can diminish one iota from our grave responsibilities as members of the militia. The Second Amendment is the "thin blue line" that guarantees the rest of the Constitution. It is the key that keeps the tyrants locked out.

It is what stopped the Japanese from invading us in World War II. Their intelligence revealed a heavily armed and highly pissed-off American people willing and ready to wipe them off the planet if, in a moment of insanity, they decided to invade us. The advantages of disarming a populace is easy to see - just like the disarmed rape victim - we can be raped and sodomized all an enemy wants.

There has also been attempts to control the one aspect of free speech that isn't yet completely controlled in this country: Electronic media and computer networking (the Internet). Independent BBSs run by computer hobbyists are a safe, convenient and efficient means to assemble and to distribute information instantly and at low cost. Furthermore, there exists advanced computer hobbyists known as "hackers" who collect information as a serious hobby. These people maintain databases on all sorts of info from security, to explosives, to advanced programming information, and for many different systems.

Their special knowledge and skills make them excellent potential freedom fighters, and because of this, also excellent targets for any conspiracy to destroy or neutralize. Clearly, the *hacker witchhunt* is well under way. The hackers aren't the only ones that major efforts are being made to destroy. The survivalists is another major group. Have you ever noticed that just about every nut involved in a mass-murder is described in the media as a "survivalist". All they need to find in his closet is a camo jacket. Clearly, the purpose is to defame the survival movement and to conduct witchhunts against survivalists. The Second Amendment, the survivalists and the computer hackers are the greatest threat to the rise of a dictatorship in this country and that's why they are the ones being so viciously attacked.

A dictatorial accession would start and proceed very slowly, as it is doing now. But one day an incident will occur which will give the Government reason to declare martial law. If someone big doesn't get assassinated, then they'll blame it on the drug dealers or something else. So far, in California and New Jersey, laws have been passed restricting the possession of semi-auto firearms. And the courts in many different places have ruled illegal search and seizure to be within the law if drugs or guns are being searched for. And the FBI has recently been given full legal authority to shoot fleeing suspects in the back!

Even more recently, BBSs are being taken down for no reason whatsoever except that, *"It might aid in an investigation"*. Thus to detect such an occurrence, one will have to be very alert and use wise judgement for determining when the time comes. The difference between a freedom fighter and an insurgent is what side your on. Once you decide to fight a ruling Government in open warfare, no matter how bad it may be, you've taken the final step as the Government will do every thing in its power to stop you and will show no mercy whatsoever. There will be no due process.

ISSUES TO CONSIDER

Ok, now that you've decided to resist, there are a few things you have to ask yourself in order to judge the best way you'll be most effective.

(1) Should I work in a group or alone?
(2) Should I head for the hills or stay where I am?
(3) How should I prepare?
(4) What should I do to be most effective.

(1) While it is man's nature to form groups, in certain situations it might be wise not to. Remember, "Three can keep a secret, if two are dead". By operating alone no one can compromise you if they get caught. You also cannot harm anyone if you get caught. And if you go it alone you do everything alone. Some actions are much more difficult and-or dangerous if attempted alone as compared to with a group. On the other hand, it's almost always better to make decisions alone than via a committee of which you may not even be a member. However, if you have little knowledge of freedom-fighting and its related topics, your best chance of survival is to join up with people who do.

What is the optimum number of people for your group? It depends upon many factors: Your physical environment, group organization, mission, equipment, threat, required skills, available quality personnel, etc., are all important factors. The range for a highly mobile group consists of 2-10 people. If you have a concealed and little-known retreat and are organizing by families, the range is 7-25 members. If you are travelling by caravan as a refugee group to permanently relocate somewhere and are a very visible group, then the range is 100-1000 members.

Should you decide to be involved with a group, you are faced with the profound task of picking the other members of the group. You must be able to pick people not only that you can trust your life with, but who will both contribute to your survival and have their survival contributed to by you. And once you pick a group - regardless of the group - you will lose some independence and decision-making power. For example, you might pick a group that contains Guy B, who you admire for his great survival skills. However, unknown to you, Guy B insists that his beloved Aunt Mildred also belong to the group (as he just can't abandon her), altho Mildred is a heavy burden to everyone.

Once you pick a group and that group is finalized, then completely reevaluate the group and its leadership, and carefully and objectively compare its benefits and risks to those you have on your own. If you don't come out SUBSTANTIALLY ahead, back out of the group. The reason why I say, "substantially", is that the predictability of group behavior is much more uncertain than individual behavior. And it is never a good policy to reveal your cards to group members until you are CERTAIN that you are going to stick with the group.

(2) If you are in the military, a political activist or some other way remotely represent a danger to the regime, then it might be best to go into hiding as soon as possible. If not, just stay where you are for now and keep a low profile while you go about trashing them.

(3) As a freedom fighter, you will need a wide variety of knowledge. Some important topics are:

(A) GUNSMITHING/WEAPONRY: Useful specialties include full- automatic weapon conversions, improvised weaponry, black powder guns, rocketry, explosives and ammo reloading. Basically, you want to keep your weaponry up to standards, keep them operating even if you have to make your own replacement parts and ammo, and be able to improvise a wide variety of weaponry as the needs arise.

(B) CHEMISTRY: is very handy - particularly regarding the fields of poisons and explosives. And for improvising all kinds of useful and necessary materials. And for being able to properly identify them.

(C) COMPUTERS: A computer is a useful data storage, analysis, and commo tool. Fields you want to definitely get into are modems, desktop publishing, probability theory, and statics and dynamics analysis. A high level of computer programming skills is a major plus.

(D) COMMO: Particularly, radio and phones.

(E) OUTDOOR LIVING: Emphasize camping, hunting, wild plants (edible, poisonous, & medicinal) and trapping.

(F) MILITARY TRAINING: If you can afford to go into the reserves or national guard and feel that you an handle it, then I advise by all means to do it. The training and contacts you obtain will be invaluable.

(G) UNARMED COMBAT: The best approach is solid martial arts training. Else, get someone experienced to teach you the basic techniques and tricks.

(H) AREA KNOWLEDGE: It's well known that Americans do poorest at geography than just about any other academic subject. What a pity! Very useful for when you go into hiding and when you plan operations. This is something an invader will not have in the beginning, so you should initially have the edge. I would suggest learning about hideouts (abandoned buildings, good camping sites and the amount of cover and concealment offered by them), prominent building layouts (particularly those used by the government), sewer layouts, roads/trails/ paths (including their conditions and side roads), foot, pack animal, 4-wheel drive, bikes and motorcycles (and the amounts of concealment available when using them), hiding places for supplies (including their accessibilities), and indigenous animal and plant life (habitats and habits).

(I) PRINTING AND PUBLISHING: Useful for generating propaganda. And to provide messages or newsletters for larger or disconnected groups.

(J) MEDICAL: Especially from an improvised standpoint.

(K) PHYSICAL FITNESS & GOOD HEALTH: Usually of life and death importance - especially if you're going to be running around all over the place.

(L) OTHER TECHNICAL SKILLS: Survival situations call on all kinds of technical skills. Others that are very important are vehicle repair, radio repair and power station set-up and repair. And a good general knowledge and capability to get into, troubleshoot and repair equipment of all types using basic tools and available parts and materials.

(4) The primary thing to remember when planning your operations is that civilian support is essential, therefore do not target innocent civilians! When innocent people get hurt by your actions, you will lose their support, and you will usually hurt yourself in the end. The only times that it may be worthwhile to attack civilians are:

(i) If you will only be in the area for a short time or just passing thru, or

(ii) The civilians are distinctly and universally against you or in favor of your enemy over you.

Also, work on a scale that you'll be comfortable with. *Your operations will probably fall into one of these categories:*

(A) EQUIPMENT & SUPPLY PROCURE: Obviously, it pays to get what you can now. But after a while you will need to replenish. Getting weapons and supplies from your enemies makes things a lot easier. These operations could be as simple as taking out a lone guard and stealing his equipment. It could also be on the scale of raiding a supply dump or camp. You want to take only what you need, and destroy the rest. And don't load yourself down.

(B) HARASSMENT: This is all the nonlethal stuff you do to annoy them, and wear them down. Personally, I'd do something heavy duty instead if you are going to take risks, but sometimes the only opportunity you might get is for harassment, and if it's at very little risk to yourself, go for it.

(C) INFRASTRUCTURE TERMINATION: Also known as assassination. Taking out key people will do a lot of good. We did this with the Phoenix Project in Vietnam and it was very effective. Good intelligence is essential.

(D) DENIAL OPERATIONS: When you run into useful equipment and supplies during an operation, destroy everything you don't/can't take along. It'll make life more difficult for them.

(E) PROPAGANDA: Gaining support of the people is essential. So educate them and keep them informed of abuses by the regime. Use radio, print and include how-to-sessions to turn them all into potential freedom fighters.

(F) AMBUSHES: Nailing the enemy in remote areas keeps them out of your country. Ambushes are also ideal for getting supplies.

(G) REMOTE CONTROL: Timed explosives and boobytraps are useful as they work without you being there. However, they are nonselective and must be used with care.

(H) INTELLIGENCE: Always try to get info on the enemy.

SELECTED PRINTED MATERIAL:

"GREEN BERETS GUIDE TO OUTDOOR SURVIVAL SERIES" By: Don Paul This is an excellent series on defense, survival and outdoor living writ ten by the Green Berets. Excellent information:

PATHFINDER PUBLICATIONS
Hamakua Center / Suite 401
150 Hamakua Rd.
Kailua, Oahu, Hawaii, 96734

"SECRET FREEDOM FIGHTER: FIGHTING TYRANNY WITHOUT TERRORIZING THE INNOCENT", by Jefferson Mack

PALADIN PRESS
P.O. Box 1307
Boulder, CO 80306

"THE ANARCHIST COOKBOOK" By: William Powell

ALTERNATE NEWS GATHERING TECHNIQUES

"You shall know the truth, and the truth shall make you free" - John 8:32

Back in the "good old days", the newsmedia actually did fulfill it's purpose, which was giving the public news in a fairly unbiased manner. However, things have changed since the days when Ben Franklin and Alexander Hamilton were running newspapers. Today, it appears that the purpose of the media is to brainwash, rather than to inform. Few real news stories in regards to the status of our nation are seen; with most of the news being some sensational scandal of some kind or another, or being some attempt at brainwashing the public into accepting the media's views. Very rarely do you see a real news story, and when you do, it is usually perverted to serve one of the two above purposes.

Think of just some of these outrageous injustices and misinterpretations caused by the media and their coverage: The current movement to ban fire arms. All I've heard is how bad guns are, not any factual information regarding this topic, other than information from antigun groups. About the only reason I've heard is that they are "dangerous", and that "they must be taken out of the hands of the people". When pressed for more factual information, the antigun media starts beating around the bush, and rarely is any factual information or data seen in media articles regarding the Second Amendment. And how about the O.J. Simpson trial? That will always be a prime example of how the media fucks things up by always searching for the next sizzling headline, or the "inside scoop" on a case, when much of the information they report isn't accurate!

Besides these two recent examples, there have been, and will be, many others. I suggest you watch either the ABC, NBC, or CBS TV networks, or read any major metropolitan newspaper too find some examples, then read some of the sources that I will give later in this chapter. I guarantee you'll see the difference.

So where do I go for real news?

To start with, the one thing you should always keep in mind is that ALL news is biased to some extent. Some may be more biased than others, but it is still biased. The most biased news comes from the major TV networks: ABC, NBC, CBS, and CNN; and from the major U.S. city newspapers such as the New York Times, and Washington Post. Typically, these media sources are liberal/left-wing biased. Altho any type of bias is bad, the liberals are the worst when it comes to matters most concerning the survivalist/freedom fighter, due to the liberal hatred of self-defense and of Government nonintervention in people's lives.

The idea with getting news is to sample as many sources as possible, and then actively make your own conclusions as to what's going on. Particularly in regards to survivalists and freedom fighters, news gathering is an active process, and not the passive process as many people today treat it. You can't learn about what's going on from sitting in front of the TV for an hour each night, or by reading a newspaper.

The first place you can go for mostly unbiased news, is ironically enough your TV - provided you have cable or satellite TV. There are two networks which offer decent news reporting. The first and best is C-SPAN. This is a "public-affairs" station, which is a direct feed straight from capital hill, and is offered without comment. While not news per-se, you can get a first-hand look at the U.S. Congress in action - debating, passing laws, resolutions, etc. You may not like what you see, but at least it's directly from the source. You local cable TV station may also have a similar channel for local legislative sessions that might be worth checking out. The second source is CNN news, which is a division of the Turner Broadcasting Network (TBN). While this is becoming more biased than it used to be, it is a more honest news station as it's now as biased as the three major TV networks. However, don't use CNN as your sole source of news.

Regarding news in your local area, the best thing I've seen is a Police scanner radio. With one of these tuned to your police and fire frequencies, you'll get a firsthand report of events in your local area. While some places are beginning to scramble their radio transmissions, the practice isn't widespread, and most scrambling schemes are easily cracked. Attacking scrambled audio is discussed in another chapter of this book. It might also pay to attend your local town-board meetings, as this will also give you a firsthand look at how well, or poorly your community leaders are doing.

One very effective technique for getting news, or at least an alternative viewpoint is to check out shortwave radio broadcasters. The broadcasters from Western Europe, Australia and Mexico offer news abut the United States that in some cases isn't mentioned by the domestic media. It also gives you a more objective and less self-serving view, as these broadcasters aren't living here. The best station to listen to is the BBC (British Broadcasting Corporation). However, the other Western European stations are satisfactory as well, when you can get an English language broadcast from them. Some suggested radio freqs (KHZ):

5950 - 6200 9500 - 9775 7100 - 7300 11700 - 11975
15100 - 15450 17700 - 17900 21450 - 21750 25600 - 26100

The entire shortwave frequency spectrum (1 MHZ - 30 MHZ), as well as the AM and FM broadcast bands, will become very useful in the event of a hostile takeover of the United States Government, whether it's from an internal problem, or an external power trying to take over. In such a case, freedom fighters with the background and the equipment could set up underground broadcast stations to help the resistance effort. This will be more prominent on the shortwave bands because the equipment is easier to obtain, and due to the nature of the band, it is more difficult to use radio direction finding techniques to track down an "illegal" transmitter. Homebrew broadcasting will be discussed in another chapter.

Also of interest to survivalists is the Emergency Broadcast System (EBS). The EBS is run by the nearly extinct Civil Defense/ "Emergency Management" Authorities to provide official news and instructions in the event of a national emergency. It is one of the holdovers from the 1960s Civil Defense Program, and unless you live near a place such as a dam, or nuclear power plant, there isn't much to the EBS other than it exists. However, if you have a spare AM/FM radio or TV it's worth the effort to listen to just to see what little the Government informs you of or instructs you to do. In the event of an actual emergency, I suggest programming the areas public safety frequencies in your scanner, as you will probably hear more information over them.

You should also tune around the ham radio bands in the event of a nation wide emergency. Many hams are involved in Disaster Relief Services such as Red Cross, and RACES (Radio Amateur Civil Emergency Services). Being a ham operator myself, I can tell you that a lot of info goes over these frequencies - both official and unofficial. Common freqs are (KHZ):

3500 - 4000 7000 - 7300 14000-14350 21000 - 21450
25600-26100 28000 - 29700 144000 - 148000

All but the last rage are shortwave frequencies, and offer worldwide coverage. The 3500 KHZ (80 Meters), and 7000 KHZ (40 Meters) bands offer better coverage at night. The 14000 KHZ (20 Meters) band offers decent coverage around the clock. The 21000 KHZ (15 Meters), and 28000 KHZ (10 Meters) bands are best during the day. The 144 MHZ (2 Meters) band is a local coverage band useful for finding out news regarding your local area. Also potentially useful to listen to is the CB band. Most people have a CB, so at the very least you might pick up something substantial in the event of an emergency.

The above list is just a small sampling of radio frequencies that might yield useful information. For much more info on the field of Radio Monitoring and Communications see our "Secret and Survival Radio" manual for a comprehensive listing of freqs, plans (including schematics) and techniques.

The last way one can get news from a different angle is from the network of underground newspapers known as "The Free Press" or "Alternative Press". Unfortunately, in it's role of informing the public, it falls rather short. Most of the "underground newspapers" I have seen are bitch-rags run by aging hippies with very narrow interests and focus, and are of an extreme left-wing orientation, and because of that have an antitechnology and anti-self defense orientation. This makes them unsuitable for the needs of the survivalist/freedom fighter. While most of the underground newspapers are virtually worthless, there are two examples of "alternative press" which I feel stand out, and are worth subscribing too.

The first is Blacklisted 411 Magazine. A good hacker mag, with info similar to 2600 (below). Lots of high-tech tips on hacking many types of hi-tech related systems.

The second is 2600 Magazine. 2600 Magazine is primarily designed at the computer hacker market; providing tips and techniques, but their telecommo/computer news section is comprehensive, and minus bullshit. If one wanted to keep up with that section of the news, 2600 is the best way to go. Of limited value for those who concentrate on hard-core survivalism, 2600 is a must for the hacker and techno-phreak.

Keep an open mind and sample others (report to us your findings). You might find one that suits your requirements.

Finally, to toot my own horn, there's Cybertek - the "cyberpunk technical journal". It's published by Thomas Icom, and delves into the full range of technological topics.

Blacklisted 411, P.O. Box 2506, Cypress, CA 90630
(714)899-8853. See comments above.

2600 Magazine, P.O. Box 752, Middle Island, NY 11953,
(516)-751-2600. See comments above.

CYBERTEK, P.O. Box 64, Brewster, NY 10509. See comments above.

TOP SECRET CONSUMERTRONICS. Not a newsletter but the ultimate source for technological survival manuals, software, hardware and service. Used to publish REBEL and Survive and Win newsletters. Three catalogs ($2 each or $4 for all three). Technology Survival Catalog: Mostly computers and electronics. Super Survival Catalog: Mostly weaponry, energy, rocketry, etc. Radionics Manual: Electronic medical plans/devices.

The First Amendment Made Easy: How to Become Media

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech or of the press; or the right of the people peaceably to assemble and to petition the Government for a redress of grievances" - The United States Constitution, First Amendment

Freedom of speech and thought is the most important of our freedoms. If it were otherwise, the Founding Fathers wouldn't have made it the First Amendment. However, in practice today it is quite a different story. Certainly we have the media to inform the people and to provide news. But if your views are different from those of media bigshots (reporters, editors, publishers, producers) then your side of the story may be twisted or outright ignored.

Until recently, it was widely believed that to deal with the media one had to have an excessive amount of money to start publishing or broadcasting. With the advent of computerized desktop publishing systems, it is a fact that even people with modest incomes can become media. For about the cost of a TV and VCR, or of a stereo system, you can start your own newsletter, or even broadcast station, and say whatever you feel like.

Unfortunately, the traditional media still exercises some censorship power over the self-publisher. If he wants to become very well known, he must often advertise in the traditional media, and they can and have certainly been known to, arbitrarily and capriciously cancel ads not to their likings. However, even this undue influence is limited because there are many magazines out there when one can advertise in, not to mention Internet webpages, special- interest and grassroots newsletters, and the old standby when all else fails - word-of-mouth.

Once you become known as a survivalist publisher, certainly the media will try to label you as a "survivalist", "right-winger", "left- winger", "kook", and perhaps even "terrorist". Soldier of Fortune is a classic example of that kind of treatment, having been systematically abused by the traditional media for decades. However, even this can play to your advantage. First, it makes you out as an underdog. And in most cases (but not all), bad publicity results in greater success. Particularly for anything countercultural, bad publicity is often preferred over good publicity and certainly much better than non-publicity. For example, I was interviewed on CBS "60 Minutes" regarding our "Stopping Power Meters" manual. Essentially, I was portrayed as an energy crook. The result was $12,000 gross sales for the first month after the segment was aired for the sale of "Stopping Power Meters" alone.

However, in a few cases, bad publicity can harm you - sometimes very seriously and permanently. *Examples: If you are accused of:*

(1) Robbing or cheating your subscribers or supporters.
(2) Having any connection with child abuse or pornography.
(3) Having any connection with drugs - or worse, drug cartels.
(4) Being an informant or sting for a law enforcement entity.
(5) Being incompetent, stupid, foolish or mentally ill.

Carefully read between the lines of any publicity you receive. If you find yourself receiving bad publicity in respect to any of these categories, you must react vigorously and loudly against the source. A good example was a news article that appeared in one of New York's largest news papers (The Daily News) about T. ICOM. This article implied that ICOM was so stupid and incompetent that he didn't know how to hail a cab in New York - as if to say that his well-established credentials as a high tech security expert must be fraudulent because obviously he must be some kind of mental retard. And to hold him up to ridicule and derision. Media bigshots are famous for cleverly using techniques like to this tear you apart while at the same time giving the semblance of balance and fairness.

Often, you can be ripped-off in the media because of something they fail to say or broadcast about you. By selectively eliminating certain things about you - for example, statements you made during an interview or background information - they call that "editing" - they can distort the truth so much as to make you look very bad. And often what they include is either negative and-or irrelevant, or purposely distorted to make the interviewee look bad. And because it is virtually impossible to win a lawsuit against a powerful media entity, short of taking the law into your own hands, there is no remedy to such an injustice.

An even more infamous and sinister trick is for them to change the context of your responses - particularly with TV interviews. They'll show a shot of the interviewer asking the interviewee a question. Then they'll show a shot of the interviewee answering a question. The implication is that he is answering The Question just asked by the interviewer. In many cases, the question actually being answered by the interviewee is a different one than the televised one from the interviewer. Sometimes, they'll shoot the questions asked by the interviewer AFTER the actual interview took place, and use a stand-in with a similar-looking back shot (often using a wig) to appear as the interviewee during the questioning. By later crafting the new questions based upon the actual answers given to the different old questions, they can make the interviewee appear to be just about any kind of character the TV media bigshots want to make him out to be.

For example, you might be asked, *"Do you enjoy being with your wife?"* Your response might be, *"Yes, I very much look forward to that."* However, the new televised question that precedes your answer might be, *"Do you enjoy beating your wife?"*

Many TV media bigshots engage in this crooked practice. To minimize the probability of being victimized:

(1) Answer questions as specifically as possible. For example, in the above case, you might have answered, "Yes, I very much look forward to being with my wife." You may sound a bit dopey answering questions by rephrasing them, but most in your audience will read between the lines that the traditional media can't be trusted and you are simply protecting yourself.

(2) Pay attention to the reputation of the media. If you can, con tact previous interviewees. Ask their colleagues and other media and TV insiders. If they are scum, avoid them, because they are sure to give you a type of bad publicity that will harm you.

(3) Wear an outfit that has an unusual style, texture and-or color to make it difficult for them to use a stand-in. If you are a woman, wear an unusual necklace, scarf, ribbon or pin visible in back shots (make sure that it's also visible in front shots). If they insist that you change your back shot appearance without justification, insist that you don't, and be prepared to walk out on them. But before you walk out on them, make sure that you identify the people you are talking to and clearly tell as many of them as possible why you are walking out on them. This helps you later on if you have to sue or discredit them if they accuse you on the air of, 'refusing to talk to them'.

Underground Publishing

The easiest method of homebrew media is to start your own underground newspaper/publishing setup. While you may not look as sophisticated as Time Magazine, it'll still be effective. To accomplish this, you need three basic things. The first is a means to mass produce the manuscript you are writing. The second is a way of producing consistent writing. The third, which is somewhat optional, is a means of producing graphics and pictures.

Stepping up from a basic set-up requires using computers for what is known as "desktop publishing". Using a computer to design material saves considerable time, effort and aggravation, and makes your piece look more "professional".

"Conventional" desktop publishing software, and the necessary support equipment costs $$$ though, or at least that's the impression you might get from reading desktop publishing articles. The truth is that the "conventional" desktop publishing set-up usually consists of an IBM PC 386, Mac SE or better system, "true" desktop publishing software, and a laser printer.

While this setup works well, it's expensive. For someone starting out in desktop publishing, one can get by much cheaper and still do a pretty good job. All you need is any late model home computer, a good printer, some wordprocessing software, and optionally some graphics software. This el cheapo desktop publishing setup will serve quite adequately, and even excellently to design any type of printed matter you want with a pretty high quality end product.

AM and FM Broadcasting

To start with, what this chapter won't tell you to do is how to set up your own version of WFAN for only $19.95 in parts. The reason FM broad casters get out so well is that they use Megawatts of power, and have large high-gain antenna arrays that are up real high. They also have their own electric company substation to run the whole thing, and pay more for electricity in a month than you do in a year. If you have that kind of money, and want to setup a broadcast station then you don't need to be reading this.

In any event, most community and pirate stations have a substantively less amount of money than a corporation, and manage to have a decent station. There are even some individuals who are running small broad cast stations on a shoestring budget. What they did was use the techniques in this section. Basically, all you need are three things to set up your own broadcast station: some type of transmitter, a decent antenna, and some type of stereo setup if you want to play music.

The transmitter is the hardest to get of the three, and even that's easier than you might think. For starters, anyone can set up their own legal AM or FM broadcast station. This is due to a section of the FCC regulations called Part 15, which deals with "low power" devices such as cordless phones, and wireless mikes. The catch is that the power is limited to 100 milliwatts, and the antenna length must be less than 3 feet long. This equates to a maximum range of about one mile. In urban areas, a mile encompasses much, and you can go even further higher off the ground.

Of course, there are several ways in which one can get greater power. The first is to use a more resonant antenna. By doing this one's range can be increased by a factor of 2 to 3. The second is to use an amplifier. Both of these techniques are illegal, and if caught you face a fine, and confiscation of your equipment. Of course, the FCC has to find you, and they have better things to do.

There are several advantages to both AM and FM broadcasting. FM offers better fidelity, and the equipment is more easily available. It's disadvantage is that range is limited. In the city, expect your range to be 5 miles tops. In a rural area, you can get 10 miles if you're lucky. AM, on the other hand, can offer up to 50+ miles on a clear channel with a decent amount of power, say 50-100 watts. It also lacks the fidelity that FM has, requires a much larger antenna, and the equipment is harder to get.

There are several ways to get AM and FM broadcast equipment. The most obvious are those wireless mikes sold by Radio Shack and others. Hooked-up to a better antenna, they provide a better range, but lack means to connect stereo equipment. Another choice is to mailorder *"broadcast experimenter"* equipment. These are basically wireless mikes that have simple audio mixers attached. All this equipment is legal, FCC Part 15 type stuff, until you add the resonant antenna that you need.

The third way is to build your own. FM Wireless mike plans are available from various sources, and a great deal of them offer more than Part 15 power levels. There are also several RF amplifier transistors available which make nice FM Amplifiers. The most noted are the Motorola "MRF" line. For other schematics of Radio Transmitters also see our "Secret & Survival Radio".

Shortwave broadcasting is perhaps the easiest method to set up a broad cast station. However it is also the most expensive, but offers the greatest range. Just about all pirate broadcasters operate in the range between 7100 KHZ and 7500 KHZ. This area is shared by American ham radio operators, and by European broadcasters. As a result commonly available ham radio equipment can be used to transmit, as well as commonly available antenna equipment, and technical information. For about $500 one can by a used ham radio and antenna, hook up one's stereo, and get broadcasting. For those wanting to really put out there are also 1 Kilowatt ham amplifiers that already cover that frequency range. Schematics for homebrew equipment are also readily available through ham radio organizations such as the ARRL. Just tell them you are interested in ham radio, and they'll tell you everything you need to know.

TV is an interesting realm of pirate broadcasting. To set up a basic pirate TV station, all one needs is a VCR, Video Camera, and antenna. With VCRs, you either have a choice of Channels 2 and 3, or 3 and 4. One of the two transmit channels on your VCR should be clear in your area. Just hook up the VCR according to the instructions, except that the antenna goes to the "Out to TV" F-connector. With this set-up, a range of 1 to 5 miles is expected. Also available on the market are TV transmitters for other channels that are designed to be hooked into a cable or master antenna TV system. These put out a little more power than a VCR does, but are expensive.

Computer BBS and the Internet

The future wave of underground media is, of course, the Internet, and the BBSs associated with the Net. BBS fall into two categories. Most are private and the rest are public. The biggest BBS are public. Place a message on the right BBS, and in a few hours it'll be seen all over the country.

The grandaddy of public networks is America Online. This is the Internet networking system which is connected to several hundred BBS systems all over the country where topics ranging from computers to cars are discussed, and e-mail can be sent to the west coast in 24 hours for the cost a local phone call. There are also smaller networks set up by hobbyists which link a few BBS systems together, and larger pay- networks such as Compu-Serve which can provide real-time networking connections all over the country with such features as their "CB Simulator" computer conferencing system. However, with public networks, privacy is often a big question as they are often owned by major corporations.

Various groups of technological survivalists could set up their own private network of BBS to exchange ideas and information, as well as serve a coordinating role amongst the technological survival movement, as they now do for some very specialized political organizations. BBSs are a non-attention getting, legal method way of maintaining a "public forum" on survivalism, and with some modifications be shifted over to radio commo mode using packet radio (see "Secret & Survival Radio") in the event of a telecommo disruption. Remember that many Internet Service Providers (ISP) often monitor what is being put on their system. America Online is particularly conservative about what types of webpages can be posted, and what can be said on them. They consider themselves a "family oriented" provider.

See our INTERNET CONS & SCAMS, and INTERNET TRACKING AND TRACING manuals for much more information about the Internet!

PRIVACY

"And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name." - REVELATION 13:16

We now live in an age where that End-Times Biblical Prophesy is now being fulfilled. Thruout our lives, one of our main goals is to accumulate little scraps of paper that prove we are who we say we are, and if you don't have a Social Security Number (SSN), drivers license, checking account and credit card, then you don't exist. Already there are certain things you can't do without having a credit card! And concerning drivers licenses, well what's the first thing people always ask you for? The fact is that unless you have all this paper issued to you by the bigshots, you will be persecuted, and as The BIBLE says, unable to buy or sell.

The reasons for this are simple. By knowing who you are, what you do, and other sundry detail of your life, they can better control you, and keep you in line by having the power to strip you of your identity. Lets face it, the only reason you are accepted as who you are is because of those little pieces of paper that the bigshots issued to you. They are in the process of giving you the, "Mark of the Beast"!

Already several times in this century we had a dictator round up millions of people, put them in concentration camps and use them as slaves or have them exterminated. Hitler did it. Stalin did it. Saddam Hussein tried to do it. And no matter where you look in the world, people are being controlled enmasse. In South Africa, blacks are controlled. In Israel, Arabs and Moslems are controlled. Whenever you have two or more groups competing for land and economic resources, you'll find the strongest one severely repressing the weaker one(s).

In the United States today we live on the edge of a totalitarian state. Have the wrong mark in your file, and you can be persecuted, harassed, and denied credit and often your freedom. And with the advent of powerful computer database systems, keeping information about you is as easy as hitting a few keys. Imagine what Hitler or Stalin could have done if they had even a fraction of the computer power and database controlled by TRW! Millions more would have certainly perished! With the advent of information system technology, all it will take is one little spark to start a remake of another *"Final Solution"* which would make Hitler's mass persecution, rounding up and exterminations of millions of Jews, Germans, Gypsies and Eastern Europeans look like a Sunday school picnic in comparison!

TECHNIQUES OF PRIVACY INVASION

OPINION SURVEYS: One of the most insidious and effective methods of invading your privacy is by the "opinion survey". This is based on the premise that one of the most effective means of gathering intelligence is to ask the target. You will either be called or sent a questionnaire with anywhere from 50 to 100 questions on it, designed for easy data entry into a computer. The stated objective of this questionnaire is "market research", or some thing similar. Often, you will offered either free samples, coupons, a prize, or entry in some type of sweepstakes or contest as an inducement to sell out your privacy.

About half the questions consist of inquiries about what particular consumer goods and food products you buy and use. The other half are questions about your job, hobbies, political contributions and life-style. In other words, standard intelligence information that, in the wrong hands, could be used against you. The questions are also worded and arranged to indicate any discrepancies to detect lying or an unusual condition, such as a blue collar worker having a sailboat and cellular phone, or an upper-level white collar worker making $15K a year.

And some questions are designed as possible alerters to indicate individuals who might prove to be trouble during an internal takeover, or invasion of this country, such as people who are knowledgeable in out door activities like camping and hunting, veterans, and people with technical knowledge and equipment such as computer, electronic and commo hobbyists. When the "shit hits the fan", these are the first people to be "neutralized" (ie: exterminated).

Incredible? Just take a look at some of the actual surveys which you receive thru the mail. Similar "surveys" were also sent to vets containing irrelevant, but revealing questions to, "determine how to improve VA service". The apparent real purpose of these surveys had nothing to do with improving VA services (as they consistently get worse) but for singling out disgruntled veterans.

Any one of these surveys, truthfully filled out, will at least give any intelligence gatherer a good start at completing a dossier on you. The information could also give some good indicators as to what they should watch you for in the event of an "emergency". You could fill out one of these and possibly be audited for taxes next year due to a life-style vs. income "discrepancy", or even be "detained" for being "potentially subversive". Don't laugh, the United States Government did it to thousands of Japanese Americans living on the West Coast during World War II! And privacy rights are routinely violated today with innocent people as the victims, using the "war on drugs" as an excuse!

The way around this is simple, don't fill out any of those questionnaires that get sent to you, and don't answer any questions when you are called for a "survey". If you really want to do your part, get a hold of one of those letter surveys, and fill it out with false information. You could also use the name of an enemy, for added fun.

SOCIAL SECURITY NUMBERS: Originally started as a means to implement a Government supplemental retirement fund as defined by the Social Security Act, the SSN has turned into a national ID number. If the bigshots need a number for you, they go for your 9-digit SSN. This is used for military ID purposes, bank accounts, employment and just about anything else.

The bigshots have also decreed that all children starting at age 5 are required to have a SSN to keep track of them at an early age! The joke about all of this is that at the current funding rate, the Social Security Administration will run out of money long before the current batch of people just entering the work force have retired. Thus for it's originally intended purpose, the SSN is probably useless. Unfortunately for the millions who really need SSN benefits, the program was designed as one enormous Ponzi scheme that mathematically must collapse!

The real purpose of the SSN is to allow giant information moguls, such as TRW, Equifax and Trans Union, to compile gigantic databases consisting of information they sell about you and everyone else to virtually anyone with about $15 of spare change. This information consists of your financial history, medical history, family history, criminal history, and your political, religious and sexual preferences. On an average day, a computer transfer is made of *YOUR FILE* three times! For much more information on this topic, see our "CREDIT REPORTING AGENCIES - Number One Source of Domestic Espionage!".

You better be sitting down when you read this manual! You'll learn such things as: Why the Government of Japan has a database on 313 Million people who are NOT Japanese citizens. You'll learn why every time you submit a change-of-address form to the Post Office that data is entered into a computer and immediately wired to TRW headquarters. You'll learn how swindlers use city directories and even Census Bureau data to single out potential victims. And you'll learn how to combat these many outrages.

Getting around this form of privacy invasion isn't all that easy. One thing to remember though is that many places that ask you for your SSN aren't required to have it. In this category are many government entities and businesses that ask you for it as a matter of course. This is all put forth in the Privacy act of 1974, which details which government entities are legally entitled to ask you for your SSN and when they can (the Privacy Act does NOT apply to the private sector). Read up on this law and know it. What you can then do is demand that the government entity supply you a valid reason, as supported by the Privacy Act, why it requires your SSN, and what specifically you will be deprived of if you refuse to give it to them. This will trip up any government flunky who routinely asks for people's SSNs.

Since most agencies and corporations don't ask to see your SS card when they ask your number, it's easy enough to give a fake one. However, don't make it too obvious, as the credit reporting entities flag numbers which have been known to be fake. A fake SSN will totally protect you from credit reporting, as their inquiry system is based upon SSNs. How ever, the only problem is accidentally choosing one which someone is already using. Just by giving a fake SSN to companies who ask for it, but are not required to have it, you can effectively hide yourself in their files, as the SSN is usually the key in their database system.

TELEPHONES: If you're like most other people, you can get tracked down by your phone. By having an idea of your name, and where you live, anyone can track you down by simply checking the phone book. And many phone numbers not listed in the standard phone directory, are listed in city directories. Many libraries carry city directories, as well as most banks and insurance companies. City directories not only reveal your name, address and phone number, but your occupation, age and marital status as well.

The simple way to protect your privacy is to get an unlisted phone number (which will cost you more). You might also try getting a phone listing under a fake name, someone else's name or a business name, which would also keep some professional snoops away. And don't answer any questions by anyone compiling a city directory - else provide them with fake data.

And stay away from cordless, mobile and cellular phones. Everything you say, and the number you dial is sent out over the airwaves which can be picked up with some common receivers as we detail in another chapter.

BANK & CREDIT ACCOUNTS: Banking account and credit card information is shared over TRW and other credit reporting entities, and your credit file is available to any one willing to make the effort. Also the information is available at a moments notice to the IRS and other government agencies. The way around this is to simply use cash, live as much by the underground economy, and stay away from the banks and credit issuing entities unless absolutely necessary and then only by using a false ID.

INCREASE YOUR PRIVACY

Today, much of what has to do with privacy relates directly to your credit report and the activities of those who prepare and handle these reports. For more information, see CONSUMERTRONICS "Credit Reporting Entities". To increase your privacy, you MUST contact several organizations IN WRITING to get you off of their mailing lists for at least part of their operations:

(1) **TRW TARGET MARKETING SERVICES DIVISION,** Suite 700, 600 City Parkway West, Orange, CA 92688.

(2) **MAIL PREFERENCE SERVICE,** Direct Marketing Assoc., 6 East 43rd. St., New York, NY 10017.

(3) **TELEPHONE PREFERENCE SERVICE,** Direct Marketing Assoc., 11 West 42nd. St., New York, NY 10163.

(4) There is a Federal Law that states that federally-insured savings banks and S&Ls must now notify you if they intend to sell your name and financial information, to give you the chance to nix this scam. Just in case your bank or S&L forgets to notify you, you should notify them.

(5) As well as regularly obtaining your credit report file, you should also periodically contact the: **MEDICAL INFORMATION BUREAU,** P.O. Box 105, Essex Station, Boston, MA 02112, for their file on you. After you receive your medical file, ask your doctor to review it with you. And then ask him to write up a report that contradicts errors. And then send this report back to them and demand that they correct the errors in their records.

ADDITIONAL INFORMATION

Some additional information:

(1) Many people don't realize that in most states, if you know the name of a person and-or the make, model and license of one of his vehicles, for a few dollars, DMV will sell you a copy of the registration and-or drivers license applications form, which usually includes the person's address. Businesses - particularly insurance companies - readily avail themselves of this invasions of privacy.

(2) The credit reporting industry is dominated by three industrial giants: TRW Credit Data Corp. (Orange, CA), Equifax (Atlanta, GA) and Trans Union Credit Information (Chicago, IL). First-ranked TRW recently purchased fifth-ranked Chilton.

TRW's Consumer Financial Database (CFD) provides mail and phone order companies with the identity of credit cards held by individuals that do business with them or appear on a mass mailing list they buy - as well as their outstanding balances and limits. TRW has also developed a computer model of persons most likely to not pay their bills. Regardless of how good of a bill-payer you may be, if you just happen to fall into their stereotype, it's tough titty!

TRW alone rakes in $355 Million every year from selling their services. Combined, they have 400 million credit files on 180 million people! Apparently, the big-three have carved off their own turfs.

(3) Equifax credit reports are now available to the 50,000+ companies that subscribe to Dun & Bradstreet, the major supplier of COMMERCIAL credit reports. Most of these companies extended credit only to unincorporated businesses and partnerships. Even so, this expansion represents an outrageous and unprecedented expansion of access to PERSONAL credit reports. Now, these businesses have another back door in which to invade YOUR privacy!

(4) Even the Vice-President of the United States is not protected from these vultures! BUSINESS WEEK reported that one of its reporters (Jeffrey Rothfeder), who described himself as an employer checking on prospective employees, paid a $500 fee, plus $15 each, for reports on J. Danforth Quayle and Rep. Richard J. Durbin (while they were in office!). He received detailed financial and life-style information on both people! For example, he was informed that the Quayle family frequents Sears and Brooks Brothers stores. Had this reporter been an assassin instead, both men would have been in jeopardy of their lives and the lives of their family members!

What it amounts to is that the life of a national or world leader is worth exactly 15 bucks to any credit reporting entity that has his file (and that's most of them!).

(5) TRW seems to be one of the favorite topics on hacker BBSs. From what I've been told by unidentifiable computer hackers, there is a tremendous amount of interest in TRW. Hopefully, this manual will increase that interest.

(6) If you find an error in a credit report, it is almost never enough to correct that one record as most businesses report to more than one credit reporting entity. To avoid being haunted by that error or seeing it mysteriously reappear again and again, you must find out from both the store and credit reporting entity the names of all of the other credit reporting entities that they share data with, and then you must INDIVIDUALLY contact each of these entities in writing to even have a shot at making all of the corrections.

In most cases, you will also have to find from these secondary credit reporting entities all of the bureaus that they share data with, and then do the same with the tertiary bureaus and so forth until you have contacted every credit reporting entity that could have that record. If you miss even one entity, it can (in its continuous data sharing and automatic updating activity) restore the erroneous data to the entire network of credit reporting entities!

And even if you get them all, there is still no guarantee, because most of them won't even bother to look (unless you recently purchased your credit report from them), and even if they did, they all won't make the change at the very same microsecond. In other words, after a credit bureau deletes an error, it can be automatically restored by another credit bureau within seconds, before the second credit bureau deletes its record.

There are people who have made major efforts in their lives to purge an erroneous credit record only to see it pop its ugly head up somewhere else, and they have been continually denied credit and-or jobs because of it! If you are such a victim, perhaps you should be reading our chapter, **"Solution #1: Go Berserk!"**

(7) What is there now to stop a convicted felon from tracking down those who put him away - the judge, the DA, the arresting officer(s), the witness(es) and the jurors? Even in the recent past, violent and vindictive criminals were faced with the major problem of tracking down those they hated. No sweat any more! The criminal can now, for as little as a few dollars (or free if he has a good contact in any entity that can access a credit entity database), instantly learn where his targets and their families live, and their buying habits, life-styles and family histories.

(8) TRW now has a service called Sherlock, which provides the names, addresses and SSNs of persons wanted by the police to the private sector. With the high error rate that TRW has with their "normal" credit reports, what's going to stop them from "accidentally" including innocent people in this file. Since the FCRA, in its current form, absolves all credit reporting entities of all responsibility for all errors (unless malice can be proved, which is virtually impossible), if innocent people were killed because of such errors or their lives or livelihoods totally destroyed, TRW (Equifax, etc.) would never be made to pay for their error!

(9) Another TRW database is the, "Highly Affluent Consumer Data base" of households with incomes over $100,000. This database is better known as the "Burglars and Swindlers Directory". And even "legit" businesses can structure their charges based upon your ability to pay! If you are rich, you'll be charged more for things like car repairs, home repairs, medical bills, etc. - all done 100% legally! And those who want to sue you, can now first determine just how deep your pockets are.

Most wealthy people I know of knee-jerk support anything that sounds like it promotes capitalism. I hope those that support what the credit reporting entities are doing to this great country have a knee-slapping laugh the next time they are burglarized or swindled! Or when a mistake on one of their credit reports destroys them financially or gets them jailed. Those who have the most money have the most money to lose to those who know how to use credit reporting databases to rob and cheat them.

(10) Now everyone has access YOUR personal information from the privacy of their home or business using their

microcomputer. Lotus now markets a 10 CD-ROM disk offer that contains detailed personal information on 120 million Americans (80 million households) for about $695 that runs on the MacIntosh computer. Another powerful tool for the burglar and swindler, as well as the rapist, pervert, baby snatcher, gossipy neighbor, and any other scum willing to spend $695!

GOOD FOR THE GOOSE

There are certain actions you can take as an individual which will make life a little bit more miserable for the credit reporting industry. Some are described in the K.V.A.R. file found herein. Others include:

(1) Credit bureaus are fond of telling you how disastrous it is to declare bankruptcy. They're not doing YOU any favor! It's all just self-serving snake spit! Their biggest clients are the credit card issuers, and they lose a fortune every year to bankruptcies.

If the credit bureaus already rate your credit bad, what good is it going to do you if you are in financial trouble and you don't declare bankruptcy? Even their industry brochure states, "...a poor credit history cannot be erased." and TRW literature states, "No one can 'repair' your credit history..."

Since you are already stuck with a poor credit record and there is absolutely nothing you can do to "repair" it that is acceptable to the arrogant bastards that run the credit reporting entities, you might as well go all the way!

(2) Whenever a credit issuer sends you an application form you should always dutifully complete it and return it with whatever information you find plausible. If you can't use the extra credit, how about your cat or dog? After all, they too have some human qualities.

In fact, there is at least one known case of this. A family decided that their cat named, Gayle R. Shamoo did a pretty good job as an accountant for their firm. They completed a credit application for her (American Express), she was able to pass the credit check (and why not), and they charged $80,000 worth of airline and cruise-ship tickets on her account.

(3) Actually, there are only three ways that you can effectively avoid having your privacy invaded by these vultures. The first way is to permanently leave the country. The second way is to move to a shack deep in the woods or mountains, post it with "No Trespassing" signs and react accordingly to trespassers. There are many such opportunities still available in the deep South.

The third way is to mostly or completely do your business in the underground economy. I am NOT suggesting that you do this to avoid taxes (always pay your fair share - at least it is believed that your 1040 is still reasonably private), but you MUST do it if you need to preserve your privacy!

(1) Do as much business and work as possible in cash or barter.

(2) Assume as many alternate and secret IDs as you can. See our "**Secret & Alternate IDs**" manual, the Paper Trip series of books and other sources on how to do this.

(3) Eliminate or at least minimize your credit accounts. For those credit accounts you feel that you need, acquire them under an alternate ID - never under your real ID.

If you have several IDs, it's going to be difficult to explain that on a 1040 to pay the right tax. A way of doing this (it's fair but may not be 100% legal) is to properly and individually complete and file tax forms under each of your IDs, and include payments for the proper taxes owed. Then complete a third set of forms, that you don't file, that shows your combined incomes and taxes. Then subtract the taxes you paid under the individual forms from the amount you owe under the third set of forms, and pay the difference in the form of a Postal MO anonymously contributed to the U.S. Treasury.

(4) To stop TRW from snooping into your private life, take out a Post Office box. If you move, don't immediately file a change-of-address with the Post Office. Instead, keep your P.O. Box active, and have a trusted friend or relative pick up your mail and send it to you. And if you do complete the change-of-address form, write on it, "Under my Privacy Act rights, all distributions of this change-of-address information to TRW and all other credit reporting entities is strictly forbidden." Then make a copy of the form, and if possible, personally hand it to the Post Master of your Post Office.

And you might consider completing a change-of-address form that changes your address to a mail drop. Today, many sophisticated people routinely use mail drops to insure their privacy. Unfortunately, some of the bigger mail drop firms routinely provide information to the credit reporting entities - whatever assurances they give you about your privacy are mostly BS! If you consider using them, be sure to first get a written statement that they won't distribute your name to anyone.

It is always much preferred to use either a small, local mail drop business or a trusted friend or relative for that service. An excellent alternative is for three or more close friends or relatives to provide a mail drop service to each other in a circular fashion. For example, Person A receives Person B's mail and forwards it to him. Person B receives and forwards Person C's mail. C receives and forwards A's mail. If anyone comes to the door and asks for your stand-in could say, *"Sure, he used to live here, but that was several years ago. I have no idea where he lives now."*

It may seem like a lot of trouble, but in the end it can save you and your loved ones a ton of grief. For example, if a credit reporting entity fouls up (with its usual pile of mistakes and outdated information) your credit report, with a few other changes to your ID, you can establish a virtually untraceable new ID and thus credit history file.

And for example, what if these credit reports that are so readily available to just about everybody fall into the hands of a dictator or other terrorist organization, and what if they have constructed a file of Americans meeting certain criteria. When they look for you, they'll discover that your address is wrong, and probably quit looking for you on grounds that it's too much trouble for them or your file record is full of errors.

Another great technique is to create a household full of people! For example, if you are living alone but like the idea of having ten other like spirits living with you. Then, submit a change-of-address form for each of these new friends of yours as they go out into the world. I bet that would make TRW's computers squeal like a pig in heat!

Since credit reporting entities routinely redline (ie: discriminate against people according to what side of town they live in), a neat double-revenge tactic is to turn in a change-of-address form for some bigshot scumbag, changing his address to the seediest part of town. You get your revenge against him and against TRW at the same time! And while you are at it, you might complete a few consumer surveys and opinion polls for him that reveal what his true character is.

(5) If you have trouble getting credit or a job because of a bad credit report, you might try using your spouse's SSN instead. There are reports that this method works. Or you might read the chapter, "**Solution #1: Go Berserk!**

SOCIAL SECURITY PREFIXES

Alternate ID cards can easily be fabricated to match whatever use you might want to make of them. For an alternate SS card to work, the SSN on it must, at the minimum, be a valid one. Ideally, the SSN prefix should correspond to where your alter-ego was theoretically living between ages 16 to 20. Valid SSN prefixes are listed below (as of Jan. 1, 1980):

Alabama	416-424	Alaska	547 only
Arizona	526-527	Arkansas	429-432
California	545-573	Colorado	521-524
Connecticut	040-049	Delaware	221-222
D. of Columbia	577-579	Florida	261-267
Georgia	252-260	Hawaii	575-576
Idaho	518-519	Illinois	318-361
Indiana	303-317	Iowa	478-485
Kansas	509-515	Kentucky	400-407
Louisiana	433-439	Maine	004-007

Maryland	212-220	Massachusetts	010-034
Michigan	362-386	Minnesota	468-477
Mississippi	425-428, 587	Missouri	468-500
Montana	516-517	Nebraska	505-508
Nevada	530 only	New Hampshire	001-003
New Jersey	135-158	New Mexico	525, 585
New York	050-134	North Carolina	237-246
North Dakota	501-502	Ohio	268-302
Oklahoma	440-448	Oregon	540-544
Pennsylvania	159-211	Rhode Island	035-039
South Carolina	247-251	Tennessee	408-415
Texas	449-467	Utah	528-529
Vermont	008-009	Virginia	223-231
Washington	531-539	West Virginia	232-236
Wisconsin	387-399	Wyoming	520 only

NOTE: Stick to this list, although there may be more recent assignments, as you don't want to use a prefix assigned more recently than the date of birth. Never use an alternate SS card for the purpose of fraud.

ALTERNATIVE IDS

Someday, the time will come when you'll have to abandon or set aside your current ID for a new one. Many say that this day is either already here or is very fast approaching. If you're a "character", that day will come sooner as the trend for strict compliances to certain behavioral standards are becoming more oppressively enforced. Or you may be just an ordinary citizen who is sick and tired of having his privacy routinely invaded and his life controlled by the credit reporting entities (see our CREDIT REPORTING ENTITIES - a real eye opener with a lot of how-to-protect-yourself information). And see our SECRET & ALTERNATIVE IDS for more information on acquiring new IDs.

ID Changes fall into two categories:

(1) The first is a quick and dirty short-term change, usually to accomplish a single objective or as a buffer between your real ID and a later long-term ID. You're not totally hiding, but just want to be someone else for a limited period of time or at a certain place, for whatever reasons. This type of ID can be used to fool your average John Dokes, but it will not stand up to a thorough examination.

(2) The second is a long-term or permanent alternative ID. This is designed to pass a relatively thorough scrutiny. However, if the guy checking you out does a very good job, he'll probably discover your little secret. But that doesn't usually happen unless you are arrested for a serious crime.

To be more effective at changing your ID, there are several handy tools and skills. First, you need to be a fairly good artist, or be close friends with one. Artistic ability is a definite plus when designing a "fake ID". You should also have sufficient material and equipment for a studio to work with paper media. Basically, you need various types and colors of writing implements, various types and colors of paper stock, a sharp X-acto knife, and some transfer lettering in various fonts, as well as a comfortable, private, secure and well-lit workplace. Another useful accessory is a computer with good graphics software, a good quality graphics printer or plotter (preferred), and possibly an image scanner. The idea is to put out as professional quality stuff as possible. Also, stock up on various company letterheads, business cards and other related stationery. This will give you some graphics to work with, and an idea as to styles being used. Also, acquiring company ID and business cards by whatever means is very useful.

For short-term IDs, the primary credentials are letterheads, ID cards, and business cards. Each of these are easy to make. And it is assumed that if you possess these, you are whom you say you are. Just look at your formats, and copy them. Since there are no set standards, this is easy. If you want to look "official", you can even have a real badge made up to say anything you want. The mailorder badge makers usually don't check to see if you're really a cop or not, and will of course make up a corporate security or private investigator badge with no questions asked. Again, send your ID order on "official" letterhead that you make yourself.

For long-term uses, you need a Social Security Number (SSN), Driver's License, and a Birth Certificate (BC) or Baptismal Certificate. Legit BCs are becoming harder to get. The old trick of getting the BC of someone who died at an early age no longer works in many areas, and will soon no longer work at all, due to birth and death record cross-referencing in most states.

And the old trick of copying a BC, whiting out the info, and recopying it also doesn't work IF the entity you present it to requires an original copy, because of anti-copying patterns printed on the paper. However, if a copy of your BC is OK, faking becomes much more easily done. Because losing an original is not that difficult to do, if you really fuss about it, many entities that ask for the original will settle for a copy. To fake a BC, first make a copy of it, fake the copy, then make a copy of the faked copy.

There are two other ways to go. The first is to make a phony BC from scratch either the old fashioned way (draw it up) or by using sophisticated computer graphics and desktop publishing software. The problem here is that each state has a standard format, which must be conformed with to avoid discovery as a fake. Fortunately, most DMV employees got their jobs politically and are both disinterested and marginally competent (the major reason why you stand in line for two hours to get a driver's license). A busy, dysfunctional and politically-secure DMV clerk is not likely to spot an out-of-state phony ID. However, you never can be certain that this won't happen to you.

However, it is better to say that you were adopted (or something similar) that would justify not having a BC, and use a Baptismal Certificate instead. While in the past adoption was relatively rare, today there are so many illegitimate and abandoned babies that about 1/5 of all children are now adopted or raised in foster homes. Baptismal Certificates are universally recognized as an acceptable alternative to Birth Certificates, and there is no set design to them as each church and religion that issues them has its own format. Also, the design is relatively straightforward, and there is effectively no way to really check it out, as churches vary widely in record keeping practices and, to date, very few churches that we know of share their records with any government entity (ie: verification is very unlikely). As long as it looks good, you will have no problem. Remember, your alter ego doesn't exist unless you can authenticate its existence with a piece of paper.

A SSN can be acquired once you have a BC, altho you should not have too much trouble guessing one if you must resort to guessing. Just remember to have a good story as to why you don't have a SSN at age 35. However, don't use an alternative ID to get a tax refund from Uncle Sam, or to collect Social Security benefits. If you feel that you are going to lose Social Security benefits because you can't collect off of an alternative SSN, unless you are now upper middle-age, the probably of you collecting meaningful SSN benefits even from your legit SSN is nil. Also consider that there have been numerous cases to date of two legit and identical SSNs issued to DIFFERENT people.

A better way to obtain a 100% legit SSN is to pick up the phone directory or city directory (preferred) of your nearest large city. Look for someone with a name that is as close to the name you choose to adopt on your BC or Baptismal Certificate (NOT YOUR REAL NAME!). Then, by using the services of a "super bureau" (a credit bureau that sells personal information to anyone and everyone), and the excuse that you are trying to track down a family member for inheritance or other purposes, run a credit check on the person. This does two things. First, you acquire a 100% legit SSN in YOUR NAME. What more can you ask for! Second, you can determine the credit worthiness and credit card accounts of your namesake for whatever later profitable use that might bring you! If you're careful and lucky, you can value from this experience over many years.

However, there is one major flaw using this method. The IRS increasingly uses matching techniques to matchup people's bank accounts, stock dividends and other sources of income to the people and then compare these with the reported income on their Form 1040s. The IRS has caught people "riding piggyback" because of more than one submitted 1040 or an audit of the legit person resulting from "unreported income". Therefore, people using this method must stay in the under ground economy as much as possible. And it is also the reason why this method is preferred for short-term alternative IDs only.

An even better method is to acquire your Birth Certificate and SSN from a person who has been mostly homeless and jobless for the last 5+ years. Since the vast majority of homeless people are never given enough chance by the system to recover from their state and most die as "John Does", this method is the safest and securest method. And after 7 years, the credit entities are "supposed to" drop any bad credit they may have.

Another very important ID is a driver's license. With a BC (some states also require an SSN) you'll be able to get a driver's license fairly easily. It's recommended to go thru the usual requirements as if you've never had a driver's license before. Avoid the "fake ID licenses" as they are a joke, and will not fool anyone.

Use of alternative identities is not illegal, unless fraud is involved (that's why it's always recommended to pay your taxes). Alternative Identities go back to English Common Law when a man could change his ID for any reason. Many Americans did this when they first immigrated to this country to provide them more opportunities and to escape a past criminal record. Many pioneers who moved out West changed their names for similar reasons. Alternative Identities are as American as apple pie, and in fact account for the large popularity of the "Smith" and "Jones" surnames in the U.S. However, ID changes -legit or otherwise - is something the bigshots hate as it lessens their control over you because it decreases their abilities to accurately keep track of you.

The best age to start an alternative ID is late teens. Altho SSNs are required at age 6, most people don't follow this requirement, and I don't see it being enforced yet. Late teens is still the age when most people start work, get a driver's license, and start establishing them selves. Chances are, the ID will mature to over 21 when you need it, which makes the person a legal adult in all aspects. So what if your second ID is a few years younger than you are, once you're over 21, nothing matters. If you want a real SSN, the best age is 19. This is old enough to be an adult, but still young enough to justify not having a SSN. If asked about your parents, either assert your adult status, or simply state that they died or you lived in foster homes. Most people won't question you any further about them.

When applying for any official paper under your fake ID, choose a location removed from where you actually live. This keeps you from being recognized.

For long-term alternative IDs, it is best to maintain a clean credit bureau record, because the poorer your credit is the more your records will be scrutinized. It takes about 6 months to establish "good credit." However, for short-term alternative IDs, as they say, "be as bad as you can be" and take advantage every way that you can. After all, one of the biggest reasons for obtaining an alternative ID in the first place is because credit reporting abuses are so blatant and oppressive that you are forced to do so.

IMPROVISED DISGUISES

Much can be done to alter your appearance by changing simple things. You can dye your hair a different color, and change it's style. If you wear glasses, switch to contact lenses, or even different color contacts. If you wear contacts, or don't need eye correction, wear glasses. You can thin out your hair, or put on a toupee if you're bald. If you're male, either grow a mustache and/or beard, or have it cut off. By taking 250 mg of Canthraxanthin, an organic food coloring, a day for two weeks, you can darken your skin color. You can also bleach your skin to make it lighter. Adopt new physical and speech mannerisms. Attempt to put on, or lose weight. Change your clothing style. Finally, look as plain and non- descript as possible, just another face in the crowd. It usually helps by using earth, dull and impure colors.

For example, I myself put on an extra 10 pounds, changed from contacts to glasses, and had my previously long hair cut real short. This was due to my new job, but these three simple changes rendered me unrecognizable to about 60% of my friends and acquaintances. There's nothing esoteric about these methods, in fact people do it every day in the name of vanity. They do work however, and require little effort. Most people pick up on the expected, and have a hard time when it isn't there. Wearing a hat, unless it's your personal trademark, always tends to disguise you.

For quicker and more drastic changes, you might obtain and use a movie makeup kit. These are available from movie and stage supply stores and stores that sell gimmicks and magic tricks.

THE ART OF CONCEALMENT

The ability to conceal objects is one of the most important and useful tools in a survivalist's/ freedom fighter's bag of tricks. Effectively using it is a big step forward in making sure one's equipment and other possessions are safe, thus ensuring that they will still be available when needed. In this respect, concealment is more important than tamper-proofing as if something is properly hidden, then tamper-proofing will more likely not be needed.

PERSONAL

There is no place on your body where you could hide something that would withstand being found in a good, thorough search; however, unless the searcher knows his stuff, and-or isn't bound by any legal restrictions, then there are a few places which will withstand a less than thorough search. Law enforcement and most civilian security officers have certain restrictions on how thoroughly they can search someone. As you've already guessed, these restrictions are routinely violated. If you've pissed off a cop, or are dealing with some major corporate security officers, you can expect the works.

There are several ways you can be searched. The first is a cursory inspection. This isn't really a search, but an examination of your person for anything abnormal, like an odd bulge where it shouldn't be, indicating an effort to conceal something. This technique is commonly used by store detectives to nail shoplifters, and by police when looking for probable cause in order to take things further.

The second is a "pat-down" search most commonly used by police officers making an arrest. In this case they feel for anything concealed, and in most cases avoid areas which "patting-down" may constitute a sexual-assault charge. A pat-down search will reveal just about any thing you may try to conceal.

The cursory inspections and pat-down searches are the usual legal limit on searching procedures, unless there are extenuating circumstances, or your searchers simply don't respect the law. In that case, more thorough methods will be used. The most common of the more thorough methods is a strip-search. As the name implies, they have you take off your clothes in order to discover anything you might be trying to hide on your person. A strip search will discover anything you are carrying unless it is small and is sewn in your clothing, or you got esoteric and hid it in your body.

If they believe that you are hiding something in your body, there are two things they can do, both of which are very effective. The first is a BCS, or "Body Cavity Search." This is a physical examination of the rectal cavity and vagina, which are common areas of internal concealment.

The second and more esoteric is an x-ray of the suspected area. Both of these will turn up concealed objects. Another common device is a metal detector, usually a handheld one called a "wand". The more sensitive ones will detect an object concealed within the body. They are also not regulated because no physical contact is made during the "search". Their disadvantage is that they can only detect metal. They are commonly used in areas where they don't allow weapons inside, or in stores where they don't want employees walking out with jewelry or other small expensive items.

With the above in mind we can now discuss personal concealment. This can be divided up into three categories: In clothing, on your person, in your person and in your clothing.

CONTINUED ON PAGE 21...

You can no longer trust ANYTHING you say over a phone or radio is private. You've got Government and corporate snoops all over the place. You've got telco employees listening in. And you've got all kinds of people from dedicated scanners to casual listeners tuning in. Even when you record your voice on a recorder (or some other critical or proprietary information), you leave yourself in great jeopardy. Even if what you say is completely innocent, with about $5,000 in computer equipment, anyone can real-time analyze, store, retrieve and-or synthesize your voice so that your own mother couldn't tell the difference. The mere fact that they have your voice sounds in their computer, they can get the computer - speaking in your voice - to say anything it is programmed to say. Try explaining that to a jury, your spouse or your boss!

Once you've considered the grave implications of this technology, you will assuredly want to disguise and-or scramble your voice. For voice disguising technology, CONSUMERTRONICS sells the very popular "*Voice Disguiser*" manual and module.

Both voice disguisers and scramblers have their places. If you want your message to be secure, but once descrambled, you want the listener to clearly identify you as the speaker, then you need a scrambler. Keep in mind that he'll need a descrambler to derive the message from the garble. However, if you want to conceal your identity as the speaker but are not particularly interested if someone is able to monitor and understand your conversation, you need a voice disguiser. They can be used together to provide both features.

There are two ways to invert a signal. The first is to invert the AMPLITUDE of the signal. The simple inverter circuit in (A) will do that. That does not offer much security because it's easy to defeat and with a keen ear you can pull the message from the garble. The second is to invert the FREQUENCY of the signal. This requires a much greater design effort, and it is virtually impossible to lift the message from the garble by ear. The schematic for this method is in (C), and its block diagram is in (B).

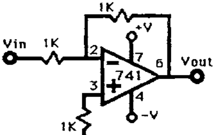
Essentially, a freq inverter transposes the high freqs to the low freq band and vice-versa. The two bands are separated by a center freq, which is not transposed). Freq inversion requires a bandpass filter, multiplier and low pass filter stage.

The bandpass filter limits the input's bandwidth (BW) to the 350 - 2500 HZ BW. Multiplying the BW-limited signal by a cosine signal results in a freq-domain equivalent of convolution, producing two sidebands. The resultant signal is low-pass filtered to produce the freq-inverted signal (Fo-Fi) by truncating the unneeded upper sideband (Fo+Fi).

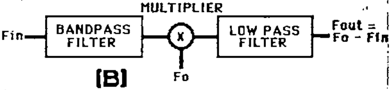
Freq-inversion of the voice band is practical (the wider the BW, the greater the circuit complexity). The BW of concern here is the voice band, but certainly any band of real time data could be scrambled by adjusting freqs accordingly. The BW used here can be changed to meet your particular needs (ex: customized for YOUR voice BW).

Because the input and output freqs occupy the exact same BW, (C) can be used as both the scrambler and descrambler. For half-duplex commo, both parties have one scrambler/descrambler unit each. For full-duplex commo, each party has two units each - one used as the scrambler and the other as the descrambler.

The oscillator freq (Fo) equals 2850 HZ (350 HZ + 2500 HZ). Center freq is half of that or 1425 HZ. Calibration is straightforward. With no input signal applied, first adjust the Sine DC Null pot until a 2850 HZ oscillator feedthru disappears from the output. Then adjust the Oscillator Null and Sine Distortion while applying an input sinewave until a pure output sinewave results (freq-transposed from input sinewave).

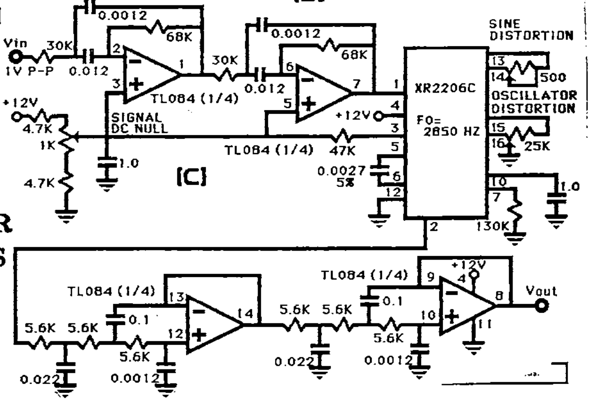


[A]



[B]

VOICE INVERTER CIRCUITS



[C]

CONTINUED FROM PAGE 19...

These techniques are only usable for small objects, and will not withstand a thorough search, but if done properly all will withstand a cursory inspection, and a couple will withstand a pat-down.

EXTERNAL

A common method used by shoplifters and immortalized by spy movies is concealing objects in hidden pockets in one's clothing. A piece of cloth can be sewn to form a pocket on the inside of a piece of clothing, usually a jacket or in a pants leg by the inner side of the thighs. Provided the object is no bigger than a cassette tape or pack of cigarettes, this will be effective against a cursory inspection. Trench coats work best, as well as any other loose fitting garment. Pro searchers are aware if this technique and will be alerted if they notice you wearing loose fitting clothes.

One can also use shoulder and ankle holsters to conceal objects. With a few modifications, regular gun holsters can hold other objects about the size of the gun they were designed to carry. Several suppliers also sell shoulder and ankle rigs specifically designed for that purpose. A well done shoulder rig will pass a cursory inspection, but will be found if they do a pat-down. An ankle rig offers the same amount of concealment, and will also evade a pat-down if the searcher is sloppy, or gives you a quick pat-down and misses your ankles.

Money belts are ever popular for very small objects and will withstand pat-downs. No one can also tell if you're wearing one unless it is examined very closely.

One place that will evade both cursory inspections and all but the most intimate pat-downs is on the inside of your thighs, just below the crotch. Provided you place it close enough to the family jewels (or whatever you have down there), only a real depraved person will check that area in a pat-down search. Of course, if they think that's what you're doing, a legal strip search via a judge's approval may be quick in coming, but it works for ordinary situations where a pat-down is as far as they (can) go.

One can also hide very small objects in your shoes. Nobody every bothers to look there; altho if you're held captive/detained by anyone semi-intelligent they'll take your shoes. Heels can also be hollowed out, and objects concealed in the hollow heel beneath the footpad.

INTERNAL

The "classic" internal hiding place, used often by convicts, is the rectum. While many people are aware of this hiding place, they don't seriously think that someone will shove something up his ass in order to hide it. While this will definitely withstand a cursory inspection, pat-down, and strip search, a body cavity search will find it. And unless your a practicing male homosexual, you will only be able to conceal an object about the size of a cigar tube. Don't look at me that way. You spent your hard-earned money on this book, so you might as well learn all the angles.

Another classic is the hidden compartment in a false eye, or similar prosthesis. Now don't go off and maim yourself because I said you can hide stuff in your prosthesis, but if you do happen to already have one, don't ignore it as a hiding place. This is one that everyone has heard about from spy movies and novels but really isn't aware of. Again, if your searcher knows his stuff, he might check this angle out, but your average guy won't figure it out.

The ultimate (I did not say best!) method of concealing something in/on your person is to have it surgically implanted in your body where it won't get in the way of anything important. This will evade every search, except an x-ray, and a metal detector if the object is metal. The disadvantages is that it requires surgery which will keep you laid up for at least two days, and that you run a chance of infection from having a foreign object in your body, which puts your immune system in overdrive. I don't advise this, but if you feel that the object you have to conceal is so sensitive that you must do this, then make sure the object is sterilized until the object is better than pristine, and get a competent surgeon to do it for you and not some back door schmuck. Since no competent surgeon in his right mind would attempt this, what you should do is handcuff it to your wrist and bring along a couple of bodyguards if it's that sensitive.

OBJECTS

There are several ways to hide something:

1. A bar of soap and be cut in half, hollowed out, and used to store small objects. Make sure the object to be concealed is wrapped in a couple layers of plastic wrap, and sealed. One then reseals the soap bar with water.

2. Papers can be hidden behind framed pictures.

3. Empty cans can be cleaned out, and used to store objects in. This is particularly effective if one then places this hollowed-out can amongst regular ones.

4. Desks have loads of space for papers and small objects just above and below their drawers. A false back can also be installed on filing cabinets which does the same thing.

5. Appliances such as TV's, stereos, washing machines and dryers have plenty of space in the enclosures that don't have any parts. Just make sure the object you're hiding is sealed in insulating material, and secure it well.

6. Electrical wall sockets usually have about an inch of space in them which is useful. There are also "wall safes" which look like electric sockets and have more space. And you can easily make a phone one yourself.

7. Most closets have quite a bit of space between the top shelf and the ceiling. A false ceiling could be installed here to provide space.

8. One classic move is to bury it. Just make sure the spot you bury it in doesn't look too obvious.

9. In some instances, you can always hide something in plain sight. Make sure it is well protected, cover it with dirt and grease and stick it in your basement or garage some place. It'll look like it's been there a while, fade into the background and most people will ignore its presence.

10. One easy way to hide something is to put it where the searcher won't think of looking for it, such as a commercial storage space. Rent the space under an alias, and then all you have to do is hide the key.

11. Ceiling lighting fixtures have a small amount of space available, although one must be careful to make sure the object cannot be accidentally discovered if the light is turned on. The above is just a small sample of the possibilities for hiding something. Use your imagination.

IN VEHICLES

Hiding something in a vehicle entails the same difficulties as hiding something on your person - a limited amount of space and some obvious places NOT to hide anything (ex: glove compartment). Personally, if I had to transport something that I wanted to keep safe via vehicle, I would lock it up, put a guard on it and not do anything to get me pulled over. The police are experts at searching cars and will find anything you've tried to hide. Take your object and stick it some place where it won't be seen by a cursory inspection, and don't look suspicious. If you do look suspicious, then expect a more thorough search.

SURVIVAL LOCKSMITHING

Every survivalist and potential freedom fighter should at least learn the basics of locksmithing. Locks are a totally integrated aspect of our world, and in your line of work, you will frequently encounter them with out the normal means of opening them. You may also have the need to make something highly secure - to know what is secure and what isn't.

Anyone seriously interested in playing with locks should write for a correspondence course from a reputable firm. It'll cost you about $500, but it comes with equipment and gets you certified. As an added benefit, you could make some money as a legit locksmith. To be truly effective at bypassing locks, you need to be knowledgeable about how locks work. Lockpicking is much more than sticking some wonder tool in a keyhole and opening it up in 10 seconds. A good start in your studies is the book, "*The Complete Guide to Locks and Locksmithing*" published by TAB Books.

PICKS

Picks are available via mail order thru various magazines. Some of these places require a locksmithing license or signed statement stating that you're a locksmith, while others will sell to anyone. It is also rumored that some cooperate with the police and hand over lists of customers, or are actually undercover operations. Exercise caution.

Your standard tumbler and warded lockpicks can be homemade easily. Use thin sheet metal stock and a metal saw. Use a bench grinder, sand paper, and files to get the desired shape. If you are handy with tools you can make a good set of picks for about 1/4 of the price.

PASS KEYS

Pass Keys are a type of master key designed to open all of a particular type of lock. The term mostly applied to the old warded locks, altho there are other systems this applies to. Pass keys are useful as they open a lock as fast as the regular key. Several locks have pass keys available for them.

Warded padlocks are designed for low security applications and many people use them because they are inexpensive. A pass key can be made by filing down the key as illustrated. What this does is bypass the wards leaving you with the last projection on the key to turn the lock's lever mechanism. Better locks use two levers in which case you leave the last two projections as illustrated.

Disc tumbler locks used in display cases, filing cabinets and some lower-quality alarm systems often have loose tolerances, which means that one key could fit another lock. Insert the key and wiggle it around while turning.

Double-sided disk tumblers are more secure. They are used in higher-quality alarm systems, commo and computer equipment mounts and other applications. There are a limited number of key cut codes used, and each individual application generally uses the same key cut. That is, a key for one alarm system will usually work in another of the same type.

While not a pass key per say, Master keys for a lock system are generally useful. Many corporations use master key systems. If you get a hold of any master key, hold onto it or duplicate it. When it comes to key duplication, it's best if you have your own equipment. You can do it in the privacy of your own home, and not have to worry about "Do not duplicate" stamping on the keys, or with someone turning you in for possible criminal activity.

ALTERNATE METHODS

Often, you need to get into a place and don't have the time or ability to pick the lock. Some of these alternate methods leave no trace, while others are brute force types that leave obvious evidence.

The first way is to look around for another less secure entry point. Burglars do this all the time. They encounter a secure front door, walk around the house and discover an open window! The moral of this story is to make sure everything is taken care of when you secure an area. On the flip side, when penetrating an area, check out all angles for a weakness.

When you encounter a door that has a lock you can't pick, there are a number of things you can do. If the bolt is exposed, you can try shimming the door open. You take a thin, sturdy, rectangular strip of metal and use it to push back the bolt. Spark plug gauges are one favorite. You can check for a weakness in the door. If it's of inferior construction, you can cut the lock out with an axe. If the bolt plate isn't secure, you can ram the door to tear out the bolt plate.

Padlocks are fairly easy, but both of these methods leave evidence of passing. The first way is to use a pair of bolt cutters. This is the preferred method as you can replace the cut lock and have it pass a cursory inspection. The second way is to take a crowbar and tear off the hasp. This is done when bolt cutters won't work (ex: high-security locks).

Another technique, used by the military in urban combat, is to take explosives and create your own door. Altho loud and obvious, it's quick, works every time, in a combat situation it stuns the enemy inside and is often safer than using the door.

KEY DUPLICATION

Anyone interested in locks should procure a key duplicator and a good supply of blanks. Even more interesting is the code key cutter. Many locks have a code which is used to duplicate a key with out having the original. This is most commonly used in vehicles. Both types of key duplicators and the code books which tell the machines settings for each key code are a worthwhile piece of equipment if you can afford them. The starting price for a code key cutter is about $500.

HIGH SECURITY LOCKS

There are two brands of locks which in my opinion offer optimum security when combined with other security enhancements. They won't do a bit of good if you put them on a cheap door or leave your windows unlocked.

The first and better known one is the Medico. This is a pin tumbler lock with an added twist. The pins rotate as well as go up and down. This is done by angling the ends of the key cuts. This makes for a highly secure lock. It's also reasonably priced for its security level. The locks average in the $100 price range.

The other (and less well known) is the Kaba, altho it also goes by other names. It offers even more security than the Medico. A Kaba key is a rectangular block of metal with holes all over all 4 sides of varying depth. These holes are the key cuts for the tumblers. The large number of tumblers and their presence on 4 different planes make this lock virtually impossible to pick. They cost a lot, but for secure applications, they can't be beat.

SURVIVAL COMPUTERS

Due to their influx into the world on such a large scale, the use of computers is necessary to any survival operation during all stages. While some may believe that after a disaster the technological base may be destroyed or heavily damaged, such as in a large-scale nuclear war, the probability of such a totally catastrophic scenario occurring is slim.

In fact, many scenarios, such as an internal takeover, will make computer use by survivalists and resistance forces as necessary as firearms or supply stockpiles. Actually, in virtually every scenario where microcomputers are available, there is power to operate them (ex: commercial, self-generated or even batteries) and there is expertise to use and program them, computers are almost always an advantage -usually a decisive advantage - over not having them.

Also, in pre-disaster operations and preparedness, computers are needed to operate at a high level of sophistication, freeing you from many time-consuming and tedious tasks in order to devote your time and attention to more important matters, thus allowing for more complete preparations.

Also, computers can be programmed to predict the future to some extent and render decisions - based upon the cold, objective data produced by current political and economic situations - that will allow you to anticipate upcoming events (ex: shortages and political events) that can put you far ahead of the game.

And if there are any phone lines, data links or networks remaining intact or restorable after a disaster, computers can transfer data between strategic points far faster and far more efficiently than by any other means.

The computer's impact is as great, if not greater than that of the firearm and printing press. Certainly it is as powerful as those two inventions. Simple to use and easy to master, a properly programmed computer is a massive computational, data storage and manipulation system. They are also capable of interfacing with most modern technology for fast and accurate operations.

It can also monitor various conditions for an indefinite period, and alert its user to a change in those conditions. Just look at everything which is done by computer these days and one can begin to appreciate the power of this invention. The good news is that anyone can accomplish this with a minimal amount of the proper training. With today's highly sophisticated PCs and MacIntoshes (Macs), parallel processing logic boards are available that will give you awesome computing power for only about $2,000.

Affordable astronomical power (literally meant) in portable sizes is crucial when dealing with complex survival applications where computer systems must be very powerful, yet must be very portable and able to run off of "nonstandard" power sources.

With the state of computing today, there exists many "off-the-shelf" systems packages which have this capability. Prices start at about $800. There are also several other systems which sell for much less that can be easily modified for such operations. And there are logic boards available for today's sophisticated computers that will interface it with virtually every real-world situation from commo to A/D and D/A converters - and software available to suit virtually any use.

PC OR NOT PC?

The term, "PC", refers to IBM-PCs and all microcomputers that are IBM-PC compatibles and clones. Don't be misled by the term, because altho the "PC" includes microcomputers of many makes and models, there are some makes and models that are not truly PCs. "PC" does not include Apple, TI, and Amiga, systems.

One of the biggest questions asked by survival computerists is whether or not to use a PC as their system of choice. The answer to this question depends upon your objectives. Currently, and for the foreseeable future, the consensus is that a PC is THE system to get, as "everyone" is using it, and you'll be compatible with everyone else.

Actually, PCs are the primary computers of about 85% of the business and scientific world today that uses microcomputers. It's nearest competitor is the Mac, which has about 10% of the market. Everything else makes up the remaining 5%. With the popularity Microsoft Windows for PCs, the Mac will be written off by about everybody over the next 10 years. Mac software and peripherals have all been overpriced for years when compared to PCs.

While this is all fine and dandy, the major aspects of survival computing are application cost effectiveness, security, interfacing, portability and repairability. *Consider:*

(1) **APPLICATION COST EFFECTIVENESS**: The myriad of uses of computers in survival situations are about as broad as what computers are ordinarily used for today. Applications range from simple controllers and dedicated computers to those requiring the number-crunching capabilities of a supercomputer. Many survival situations require the ability to monitor real-time events that don't occur at blinding speeds and that can be easily handled by a primitive computer. For example, it makes no sense to use a $5,000 PC system as a power supply controller/switcher when you can get a Timex-Sinclair 2000 portable computer for about $10 that will do virtually the same job!

Most people are on a limited budget, cannot afford to solve computer problems using the most expensive solutions, and MUST either adapt old and cheap systems to support applications or just simply not sup port the applications at all!

Some other important very considerations:

(A) While the newer systems are certainly much more powerful than their older versions, the software and hardware accessories required to harness this awesome additional power for a particular application may not even be available yet! And, if available, it too will be very costly. To develop this missing software/hardware yourself requires extraordinarily high computer capabilities.

(B) If your application requires multitasking (ie: performing more than one task at a time) and multi-user (ie: more than one user using the system at the same time), you SHALL require a PC-AT or better system (PC-386 or better much preferred). The most important multitasking, multi-user environment is networking. And if your system application requires more than 1M RAM (ie: on-board memory), a PC-386 or better system is required. Altho you can certainly use a hard disk to store hundreds of megabytes of data, many of today's PC programs are enormous in size, and if you require such a program you MUST have the system RAM to handle it.

(2) **SECURITY**: Those computers that are most popular are of course, by virtue of the attention they get from computer specialists, are also most vulnerable to compromise. In spite of sophisticated techniques used on today's PCs to encrypt data, not only is much of these schemes vulnerable to heavy-duty cryptanalysis attack but in many survival situations, it's just not practical to encrypt data. There are now so many older, nearly extinct, "nonstandard" computers that, by virtue of the fact that only a very few people have access to them AND know how to use them, they are secure. And the fact that their DOSs, disk formats and interfacing are totally incompatible with popular computers, data stored on their disks is intrinsically very secure. And by encrypting this data, an extra layer of security is provided.

On the other hand, if you are considering computer phreaking as a part of your resistance operations, a standard system is necessary in order to phreak the enemy's system when it comes to phreaking small single-user and Local Area Network (LAN) systems. Chances are, the standard enemy system will be a PC.

Another critical aspect to computer security is in the realm of Tempest (see our **BEYOND VAN ECK PHREAKING**). Because of less-stringent FCC regulations, most older systems produced a lot of system RF that could be monitored using very sensitive equipment up to about 100 meters. However, modern systems using color monitors have another major problem - emanations from the monitor itself. Unshielded monitor emanations have been picked up and displayed for a distance exceeding 1000 meters.

(3) **INTERFACING**: In many situations, the computer of choice is the one that best interfaces with the required application. Some computers are so boxed up that you cannot access external ports (as there are few or none), and cannot interface them with the real world. These computers have what's called a, *"closed architecture"*. Other more modern computers have external ports, but to interface them with the real world means creating very sophisticated interfacing. Most of the older 8-bit computers have an externally accessible data bus that can be interfaced to a real world application with a reasonable effort.

(4) **PORTABILITY**: In most survival situations, you don't have the luxury of unlimited weights, sizes and power consumptions. While it may be nice to have a full-size system in your home or business operating from 120 VAC, in the field, laptops are definitely an advantage -the smaller the better and the smaller power consumption the better. If you want portability, you are looking at a PC-XT or better laptop. But a new laptop design is being released everyday, so happy shopping!

(5) **REPAIRABILITY**: Unfortunately, most survival uses of computers require operations in harsh environments with replacement parts, electronic test equipment and service manual availabilities at minimums. Most older computers - including PCs and PC-XT compatibles -are largely built from standard parts. However, all of today's sophisticated microcomputers are largely built from proprietary parts that are only available from distant and nonresponsive repair depots and manufacturers - if at all. A system does you no good if it's broken and non-repairable. Even if you are relying upon sophisticated state-of-the-art computers for survival situations, you should always backup with more basic systems.

The absolute best way to deal with the question of "PC, or not PC?" is to have at least two different computer systems: One nonstandard system for your private work, and a PC to phreak with.

SYSTEM REALIZATIONS

Once you have a good idea as to what purpose your computing equipment will serve, you can start talking about what type of system, soft ware and accessories to buy. It's best to keep an open mind when planning a computer system purchase (as with everything else in life).

Most "professionals" will tell you, as a knee-jerk reaction, to buy a PC. Some will even go so far as to say that you need a "real IBM". That's pure BS. Yes, it might come down to you needing 100% PC compatibility, but seriously consider the factors described above. If the "professional" does not clearly understand your objectives, you're wasting your time talking to him.

The PC-386 systems are the best values when it comes to power and price, allowing for heavy-duty computational power and multitasking and multi-user with a standard desktop-sized system.

(see our COMPUTER PHREAKING and BEYOND PHONE COLOR BOXES manuals for much more information on hacking).

COMPUTER APPLICATIONS CONCEPTS FOR SURVIVALISTS

The technological survivalist and freedom-fighter has many needs of which computers are well suited for. Again, with current technology, many new possibilities are now open which will allow one to integrate computer technology into one's operations at any level of involvement and sophistication. The possibilities are limited only by one's imagination, desires, ability, and pocketbook (if ability is lacking).

COMMUNICATIONS: This includes both publishing and networking. Publishing is an important capability both before a disaster, as well as after. Before a disaster, publishing is a good way to make some extra cash, as well as exercising one's right to free speech. After a Government takeover, underground publishers will be able to keep the public informed and educated, unlike the media today.

After a particularly serious disaster, especially one where the mass media is disrupted, or the technological base suffers major damage, small publishers may be entrusted with the weighty task of preserving knowledge so future generations won't exist in ignorance. Computers come in handy because of software available such as word-processors, and "true" desktop publishing software which makes the publishing process much easier.

A higher-tech form of publishing is networking, or electronic commo via computer. This can not only be used to obtain news and information, it can also serve for intergroup commo, and in certain scenarios, as a powerful weapon which would be used to access enemy computer systems for intelligence-gathering or to sabotage operations.

CONTROL SYSTEMS: In this realm are CAM (Computer Automated Machinery) and computer operated security systems. The computer's ability to interface with most modern technology, and monitor a set of conditions indefinitely and real-time make it a natural for such combinations. Usually a special-purpose or "dedicated" computer is used for such purposes, but there are many microcomputers which are lying around in flea markets which serve well, are less expensive than designing a dedicated system, and can also do other things. One good example of a cheap system which does well in many control functions was the Timex/Sinclair.

ANALYTICAL ASSISTANT: Computers are very well suited for providing assistance with complex problem solving. Now with the introduction of VLSI systems the capability for analytical assistance is better than ever.

MASS-DATA STORAGE: On a 3.5 inch floppy disk, one can store an equivalent of 2000 pages of data on a 10 square-inch object 1/8" thick. Future technology promises an even greater capability with such things as optical storage devices (CD-ROM). Combined with video and sound digitizing technology, true mass-data storage is becoming quickly possible. This large data capacity to physical storage space ratio is also very good for scenarios where knowledge must be preserved after a large-scale disaster, where a large portion of society and the technological base is destroyed. A well-stocked "library" could increase the rate of recovery after a large-scale disaster, and could very well mean whether or not recovery happens at all! Knowledge that is lost may take years - even decades - to replace.

INTELLIGENCE GATHERING: Use of computer technology by "enemy" forces requires that computer literacy is a necessity for any type of real resistance/military operation. Thus, we see an expansion of "hacker" activities into the realm of espionage for resistance operatives.

CAD AND SIMULATIONS: Computer-Aided Design allows for concepts to be executed with greater first-attempt accuracy. A nice idea in peacetime. This little benefit's importance is greatly magnified when times aren't so great. The same runs true for simulations, as well as providing an effective training aid.

CRYPTOGRAPHY: Due to the large amounts of data-manipulation going on in cryptographic operations, computers are well-suited and usually indispensable for cryptography. Good cryptographic systems are also necessary in any data-storage system or commo network for better security.

CONSUMERTRONICS offers two services (refer to our catalog for details) that are particularly beneficial for people involved in electronics and computer interfacing:

(A) TECHNICAL RESEARCH: We have a data bank consisting of 100,000 circuit designs, computer programs, tutorials and nomographs. Circuit designs range from component tips to how-to-build-your-own-computer.

(B) SPECIAL PROJECTS: We will build anything for anybody (100% confidentiality guaranteed), for educational purposes only. Have a special survival need? Working on an invention? Call us!

CRYPTOGRAPHY

Codes and Ciphers

Codes and ciphers are a way to send a message or protect data so only the person who has the "key" can intercept it. There are many different codes, some of which are commonly known. Such as code (not a code, but a cipher actually) is Morse Code. Morse Code is based on two sounds: a short beep called a "dit" and a long beep called a "dah". For example the letter "A" is "dit-dah", or a short beep followed by a long beep.

Codes and ciphers can also be a system of letters, words, symbols, numbers, flags, or just about anything else. They are used for secrecy, accuracy in sending information, economy in message costs, saving time and brevity. They may be secret or non-secret; private and restricted to the use of individuals, business firms, or trades; or they may be open to the public for use by anyone.

In ciphers, each ciphertext character represents an alphanumeric character in the plaintext (usually, but not always one-to-one). While this allows for greater flexibility, it allows someone with a knowledge of the encryption/decryption algorithm and-or password(s) to be able to break it. Most encryptions rely both upon an algorithm and at least one pass word. However, some use only an algorithm. For example, versions of the XOR algorithm XORs the computer byte equivalents of all of the plaintext's characters with either a constant value or an adjacent character's byte.

There are two basic encryption techniques used with ciphers: Substitution and Transposition. For Substitution, one character is substituted for another. For example, each "A" becomes a "3". For Transposition, the relative position of plaintext characters are changed. For example, "Mary Jane" can be transposed to, "nMrey aaJ". Most encryption systems employ both techniques (and add garbage characters to boot). See our "**Cryptanalysis Techniques**" for much more information.

With a code though, each symbol is the expression of a certain word, sentence or subject. For example, the word "apple" may mean the word "tank". Codes require codebooks where all of the equivalencies are listed. Because of this, a code is often unbreakable provided the code book remains secure as a cryptanalyst (code breaker) cannot use his knowledge of language mechanics to decode the encoded text. How ever, one can only send messages which are defined in the codebook. If, "Send me a large pizza with anchovies" isn't in your codebook, then forget about ordering it.

Ciphers are usually used over codes altho they are more complex. Some times, codes and ciphers are used together for added security.

The Survivalist's Viewpoint: A good working knowledge of cryptography is essential to a survivalist. By knowing even the basic procedures one can reasonably assure the privacy of one's communications and data, as well as having a good crack at what the other guy is saying if he's encrypting his communications/ data. It reduces access to vital information on a need-to-know basis. For example, if the messenger is caught, the message remains secure.

A good system of codes and ciphers, when properly used, greatly increases the security of any type of commo link with little chance of a third-party making sense of what you're saying/ sending. Cryptography is also important in the protecting of computer files, and occasionally the compromising of same.

Actual Codes & Ciphers: What follows are a couple of easy, fairly secure codes and ciphers. Remember nothing except a good code is secure when using these ciphers, and be original & vary the actual encryption keys if you decide to use these.

The Pager Code: This code is used with a display pager. Display pagers are great for sending messages as with a common 10 digit display you have 1,000,000,000 different numbers, each of which can represent a different meaning. If you want, you could possibly make a 10-digit based numeric code for every message you need to send, and unless the very large resultant codebook falls into enemy hands you will have nothing to fear about your code being cracked. You'll also go crazy trying to remember if "17 65487639" means "Enemy approaching from north ridge" or "Get two pies with anchovies from Cousins".

To make this code more workable I brought it down to a two digit numeric code, which will allow for all the numbers and letters in the alphabet, with room for 64 more code meanings. This allows for regular, common messages to be quickly sent with a two digit code, yet still allow to convey ideas that aren't in the codebook. (A common problem with codes.) While this code goes natural with pagers, it could also be used with computer commo and on conventional paper as well. *A Pager Code Example*:

Number(s)	Meaning
00	Null
01-36	Letters A-Z & numbers 0-9
37	Change Code
38	EMERGENCY
39	Follow Plan A
40	Follow Plan B
41	All is ok.
42	ID Code for unit commander
43	ID code for whomever
44	End of message
45-49	Whatever you want....

Null - This is used when the code is sent via a paging system. Paging systems look for 10 digits, so the null is used to pad a message that is less than 10 digits in length. It can also be used to help confuse a cryptanalyst by just sticking this in random parts of the message. For added strength, it is also recommended that one uses more than one number to indicate a null, or include a number to indicate the "end of message", which tells the receiver that anything which follows should be ignored. Change code - For added strength use this indicator to switch to another, different code set.

The one thing to remember when using this code is to make full use of your 64 "message numbers". From my example I have a digit assigned to messages indicating which plan of action to follow, for an emergency situation, for an all is ok message, and for ID of group members. By using those message codes, the act of encrypting and decyrpting the text becomes a lot easier, and there's no way a cryptanalyst can figure out that "69" means "Not tonight, I have a headache".

Red Cross Cipher: This cipher is named in honor of the Red Cross Worker who told me about it. He said that he created it; which may or may not be true, but in any event needs a fairly high level of sophistication to crack.

A-1 B-2 C-3 D-4 E-5 F-6 G-7 H-8 I-9 J-10 K-11 L-12
M-13 N-14 O-15 P-16 Q-17 R-18 S-19 T-20 U-21 V-22 W-23
X-24 Y-25 Z-26 0-27 1-28 2-29 3-30 4-31 5-32 6-33 7-34 8-35 9-36

In the first stage we take the plaintext, "DAVE14", and convert it to it's respective numbers: D-A-V-E-1-4 4-1-22-5-28-31 ————————————1-! 2-@ 3-# 4-$ 5-% 6-^ 7-& 8-* 9-(0-)1n-= 2n-+ 3n-?

The next stage is to convert the numbers to their respective symbols. With the two-digit numbers there is a symbol which indicates the number for the "tens" digit.

4-1-22-5-28-31 $!+@%+*?! Ciphertext: $!+@%+*?!

The symbols could also be hidden in some abstract illustration, making them difficult to detect, yet alone to decrypt. By also using a good code with this cipher, the message "DAVE14", could mean something much longer.

Making Codes & Ciphers More Secure

A good code or cipher may be already as secure as it could be. However, they should be changed on a regular basis as an enemy could wait and see what you do, and then determine the plaintext based upon the analysis of a large sample size. This could also be used to your advantage by using a codeword to indicate some action a few times, then use the codeword to do something else entirely different. It's also a good idea to choose words or phrases that have no relation to their actual meaning.

The key to making a cipher more secure is to mess up it's character and character combination frequency count as much as possible. You do this by having a symbol or phrase to indicate a cipher change in the middle of a message. Do this enough and they'll have a hard time breaking it. You could also add "nulls" to your message which are symbols that have no meaning and encrypt into garbage. The people who know the cipher already know that the symbols have no meaning, and they are automatically filtered from the resultant plaintext. Those who are trying to crack it don't though. Finally, using a code when possible with the cipher will make it secure even if it is cracked.

A method common of Electronic Fund Transfer (EFT devices - example Automatic Teller Machines), do what's called, "real time encryption". They do this by including time or some other variable (ex: machine number, bank number, etc.) in the plaintext and-or in the password. Thus, the same plaintext results in different ciphertext during different times and dates and on different machines.

TELECOMMO TECHNIQUES

PHONE PHREAKING

For much more information on phone phreaking, order our, **"Cellular and Cordless Phreaking", "Beyond Phone Color Boxes"** and **"Voice Mail Box Hacking"** manuals, and others.

Phone phreaking had its origins as a hobby in the 1960s. At that time, Ma Bell had designed a new automatic signaling system for their long distance network. The operation of this system was based on a set of 7 audio tones. One was used to indicate an idle trunk (2600 HZ), and the other 6 were used to send routing codes. Each routing signal consisted of 2 of the 6 tones played together. This was/is known as MF (Multi-Frequency) signaling.

When this system was implemented, a small group of technological experimenters - for the most part unaware of each others existence -discovered that the signaling tones were within the range of sound freqs in the standard trunk transmission bandwidth, and by generating these tones at the proper time, their phone call could be rerouted allowing them to avoid toll charges, and to reach special telco/Bell internal test numbers. The device that accomplished this function was, and still is, known as a "Blue Box", and still sees limited use today.

Besides hobbyist applications, the blue box was also used by organized crime rings to avoid toll charges and being traced. However this is no longer done due to telco advances in technology, leaving the use of the blue box limited to a few older "phone phreak" hobbyists as an aid in exploring the telecom network. The following techniques have been in use for some time now and still work. The only reason that the telco's haven't done anything about them in a major way is because the cost of doing it cannot be justified; however, if these techniques are frequently abused, telco might then be able to justify the cost of eliminating them.

These techniques are a great way to save money from the rip-off rates that the phone companies charge; as well as being very useful in the event of an emergency should you need to contact someone and are somewhat destitute at the moment.

GENERAL FREE CALLS

There are several ways to avoid getting billed for phone calls. While these techniques do work, recent advances in phone company anti-toll fraud technology make using most of them riskier as time goes on. As a general rule, if a phone company (this term encompasses local BOCs (Bell Operating Companies) and LDSs (Long Distance Services)) wants to find you, they'll find you, and if they want to make your life miserable, they can and will. Due to a loophole in the public utility laws, the phone companies have unrestricted power to surveil everybody who uses a phone to protect their interests and to combat toll fraud. It is known that at times they have abused this privilege by using overheard information for its own business purposes and advantages.

The telcos also have the instant cooperation of the Secret Service and FBI when they need it. Because of this, it's best not to commit toll fraud from a phone that is traceable to you, like your home or business phone. It's better to use a payphone, or the phone of a neighbor or office worker you don't like. If you use phones that aren't traceable to you, and move around a lot, then your chances of getting caught will be greatly reduced. Yes, if you are annoying enough to them they will attempt to track you down, and will be successful initially, but their attempt will run them to a dead end. Of course though, if you're smart you won't be extremely annoying to them, and they won't put much effort into catching you. If you use common sense and only make a couple phone calls to people who'll forget you called from "dead-end" locations, you'll be all right, but if you don't use common sense and do stunts like call up AT&T security every day at 3 PM to say "Screw you, asshole". using the same technique and phone line for 3 months, you'll get caught and royally screwed over.

LDS & CALLING CARD CODES

The classic and once most common method to make free phone calls is by using LDS (Long Distance Service), calling card and extender codes. These techniques were used by convicts and novice phone phreaks for years until equal access came along which eliminated the need for most LDS codes. But since equal access hasn't been implemented everywhere and is only used by major LDSes, codes still see limited use.

There are three types of "codes" in use today. The first is the classic LDS code. While most of these codes have gone the way of equal access and calling card codes, a few still exist. These are basically "forgotten" nodes which belong to the bigger LDSes and were never phased out or nodes which belong to smaller LDSes that never went equal access to monetary factors. These rate second in regards to safe use because for the most part they are not set up to receive ANI (Automatic Number Identification where your number is sent to them as part of the routing function) information, but if you make your presence known in an obvious way, they can still easily hunt you down.

Calling cards are an advancement of the old LDS codes with increased ease of use and security. Being one only has to dial 0+phone number to use a calling card for any (major) LDS, major amounts of calling card abuse is thwarted by ANI. Of all three methods, calling cards come in last in regards to relative safety. The last type are WATS Extender and PBX codes. While WATS extenders are still used by a few small LDSes, there are primarily used by other non-telephone companies for their employees to make inexpensive long distance phone calls.

The difference between an extender and a PBX is that a WATS extender is an 800 dial-up which is used as a "mini LDS" and has more than one code on it, while a PBX is a dial-up into the companies phone system which is used for "after hours" access to internal extensions and "outside lines" and has a single code that is used to get in. These are the safest to use but also the hardest to break into due to the more limited number of codes on the system. LDSes and extenders vary in their access procedures, but the general format is CODE+A/C-XXX-XXX where CODE is the access code and A/C-XXX-XXXX is the destination phone number. There are also others in which the destination number is sent first, or a "1" is put before the destination number, but CODE+NUM is the most common. The length of an access code ranges from 5 to 10 digits with 7-9 digits most common length for LDS services and 5-6 digits most common for the smaller WATS extenders.

To use such a service is fairly straightforward: One calls the access number to the service, also known as a dial-up, and enters the code and destination number in the correct format. If the code is correct and the number is a proper number, then the call will be completed. If there is an incorrect code or other "mistake" then the user will hear an error message of some sort.

On PBXes, one usually calls the dial-up, enters the access code, enters the extension for an outside line and then dials the destination number. PBX access codes are usually 4 or 5 digits long, occasionally as long as 6. Generally, there is only 1 code for a PBX. The most common code for an outside line is "9", but there are others (I have also seen 2-digit outside line codes which are usually two of the same number like "44" or a 2-digit number ending in "0" or beginning with "9"). With a calling card, one simply dials the equal access carrier code of their company, "0+destination number", and then either enter in the calling card via a touch-tone phone or verbally tell it to the operator that answers.

In some areas not under equal access, you might have to dial an 800 number instead of an equal access code if their company isn't AT&T. The carrier access code is 5 digits long and in the format of 10NNN. For example AT&T is 10288 and MCI is 10222. U.S. Sprint, while having a 10NNN code, is content to stick with their 800-877-8000 dial-up which is equipped with the same ANI capability as a standard carrier access code (they could change in the future). Calling card codes are 14-digits long and usually consist of the users phone number and a random 4-digit number, but I have seen calling card codes which have just been a random 14-digit number.

LDS SECURITY

In the old days of LDS fraud, one could just sit at a touch-tone phone, randomly enter codes, and get one in 15 minutes. The code would last for at least two months. When it died, all one had to do was randomly hack codes for 15 minutes again. Such early successes however paved the way for things to come. Customers, upon getting a $1,000 LDS bill, would become disgusted and go back to AT&T. This caused LDSes to do one of two things: Go out of business or invest some money in better security. Many LDSes did go belly-up or merged with other companies, such as SBS Skyline's merge with MCI and U.S. Telecom merge with Sprint.

Granted, all of the major LDSes are now using all new, state-of-the-art toll fraud detection systems that incorporate such innovations as Artificial Intelligence and Expert Systems. All this toll-fraud detection equipment does is watch for any irregularity, and upon detecting it, flags the account and alerts security. This wouldn't be half bad as it is though if equal access wasn't around. With equal access, any LDS willing to invest the money can have the same capability as AT&T to know what number your calling from. This isn't tracing, this is ANI where they know your number just as you come in on their trunk.

Besides ANI, there is also one other way LDSes detect and prevent toll fraud on their systems, with the use of expert systems. This computer has the job to detect any irregularity on the company's network. This system operates in two areas, billing and front-end security. Of the two, billing is the simplest in operation. It simply checks each account for a sudden increase in usage. The billing expert-system starts by monitoring a (at the time) new account, making notes of such things as total number of calls and areas called. As time goes by, it begins to get an idea of your calling habits and makes note of them. Now, if someone were to get your code and use it, chances are the computer-noted calling habits would be deviated from as the code-abuser dials off to Podunk, Iowa for a long conversation with his lover every night.

At this time, the billing expert-system would notice the deviation and invalidate the account. The front-end expert system is more complex. In simple terms, it monitors the front-end security for anything "out of the ordinary". Examples of such activity are sequential invalid code attempts, code attempts with some recognizable pattern, repeated invalid code attempts with the same destination, and calling numbers which have a history of being used in invalid code attempts.

Once the expert system detects supposed fraud, there are a number of things it can do. The first (always done) is to notify the LDSes security department. The second, which is in particular regards to the billing ex pert system, is to invalidate the account and then notify the subscriber. What happens beyond that is up to the security personnel of the LDS. However, there are a number of things they can do and have done in the past. On the front-end system, they can often get a pattern of your code-hacking and simply give you a continuous stream of invalid code mess ages. This means you could hack codes forever and not get a single thing. They could also let you hack a code and then monitor it in the hopes of getting some information on you for a later bust. They could also call your destination phone number afterwards and try a little strong-arm techniques to try to get the person you called to provide information.

GETTING CODES

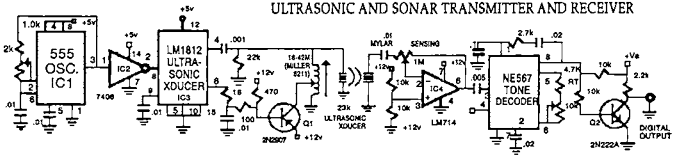
One of the earliest methods of getting codes was random hand hacking. One simply sat in front of a phone and entered random numbers until they got a valid code. But now with 14-digit code lengths most people use this method with a computer. They have the computer call up the LDS, enter a random code followed by a destination number. The destination number is another modem that is almost never busy, like a computer network (Telenet, Tymnet, Uninet) dial-up. If the code is correct, the destination computer would answer, the hacking computer would register a connect and note the code used as valid.

There are two primary methods used to defeat computer code hacking. The first is the front-end expert system described above. While a front-end expert system is hard to beat, the way to do it, which works if done properly, is to hack codes as randomly as possible. This means using random (or at least pseudorandom) code generation, and as large of a data base of destination numbers as possible. One also should have a random few seconds of delay between code hacking attempts. If done properly, this will keep the expert system from getting an idea of what you're doing, and will also take a long time to crack you.

If hacking codes, it is generally best to stay away from the bigger companies, as they have the best security (expert systems) and often have ANI. Stick with the smaller companies which don't have as good security, but also have less subscribers.

Note that the above techniques don't work with calling cards because the 14-digit format makes random hacking infeasible, and the fact that all calling card front-ends have ANI. The quickest way to get a code or calling card is to take a DNR (Dialed Number Recorder described elsewhere herein) and hook it up to a heavily-used payphone. The best way to do this is to mount a box next to the payphone wires, label the box "telephone company property" or similar, and lock the DNR inside it. Come back in a couple of days and chances are you'll have large amounts of codes and calling cards. You've also defeated the front-end expert system by not hacking them out. When using codes or calling cards (in particular), it is best to use them from payphones or other phone that cannot be traced back to you, and to call people who'll forget that you called as soon as you hang up.

ULTRASONIC AND SONAR TRANSMITTER AND RECEIVER



This circuit is very versatile in that, with a few modifications, it can be used in ultrasonic and sonar uses. It is shown wired in the ultrasonic mode. Max. range is about 22 feet, but reliability may suffer beyond 15 feet. Anything passing thru the beam will be detected. Output is digital. Select transducers for freqs. most suitable for your uses. For air uses, the transducer should be 20-70 KHz. Below 20 KHz, the signal becomes audible. The preferred burglar alarm range of 20-40 KHz is most detectable (and annoying) to pets and commercial animals, and should be avoided if that is a problem for you. 30-60 KHz is preferred to deter rodents. 40-70 KHz is preferred to deter insects. Above 50 KHz, air attenuation is substantial and range is reduced.

BUTT-SETS

The term, "butt-set" is telco slang for a lineman's test-set or test-phone. This is a ruggedized telephone with alligator clips on the two phone line wires. This enables the lineman to hook into test-points along a phone line to check for trouble. It also has a monitor function which enables the lineman to listen to a phone line while still in an "on-hook" state, undetected. Outside of the monitor function, it's just a basic phone with alligator clips. What a butt-set enables you to do is to tap a phone line any where from just outside the guys house, to the MDF (Main Distribution Frame, where all the wires come in at the central office). See our new Top Secret Catalog about our infamous **Lineman's Test Set.**

This type of tapping is also pretty much undetectable unless the target of your surveillance has some fairly sophisticated equipment. It also enables you to make a free-call just about anywhere there's a phone line.

A butt-set can be functionally duplicated by taking any phone, preferably a 1-piece phone, and adding one of the circuits shown in figure TP1. What these circuits do is block the DC from reaching the "off-hook" phone, while allowing the AC (voice) to pass. While this works very well and is inexpensive, I prefer a real butt-set as they are more rugged than any other phone which is a plus when you're using it outside and it gets banged around, and they are what the phone company uses, which is important when you are hanging off a telephone pole and want to look like you belong there.

Butt-sets are available from various suppliers or they can be simply ripped-off. The most common way this is done is to find an unoccupied and unlocked telco service van, make sure no one is looking and take whatever you need. It might also be wise to grab a tool belt and an official telco helmet. Just remember though that some lineman might get bitched-out when he reports to his supervisor that his gear got stolen.

There are various places where one can use a butt-set. The first is at the protector block just outside where a phone line enters a building. The second is at one of the distribution boxes also known as "cans" or "pedestals". These are rarely locked, usually fastened closed with a 7/16" bolt which is easily opened. Inside, one will find a set of terminal pairs. Just hook up various pairs until you get a dialtone and dial away.

If you are looking for a specific line, there are two ways to go about it. The first requires you to know the target phone number and the ANAC (Automatic Number Announcement) number for your area. When called, the ANAC number will tell you what number you're calling from in a computer-synthesized voice. The ANAC number varies from place to place, but a small list of ANAC numbers is listed in Table T1.

If you cannot get your local ANAC operator, try calling your operator, and asking what number you're calling from. Some telcos will tell you. If that doesn't work, then call again, and make up some story about how you're calling from this third-party payphone that does not have the number on it, your car broke down, you're almost out of change and you got your wife's/ parent's/friend's answering machine so you need the number to give them so they can call you back, etc. I find that a story like that works real well.

The other way to find a particular phone line requires you to be able to access it at the target's residence. You hook up a piece of test-equipment known as a "dweedle" to the phone line. This device puts a particular tone down the phone line which enables you to go down to the local pedestal and find it amongst the 200 other ones. A commercially made dweedle has a high-impedance that won't bring the phone off hook. But if the target picks up his phone and hears this tone in his receiver, he might think that something is wrong. When using a dweedle, it's wise to do it as quickly as possible, like with one man attaching it and contacting the other over radio to find the pair at the pedestal. Even though the target may simply ignore anything weird that goes away after a few minutes as a temporary glitch in phone service, if it continues for any length of time, it might get reported to telco as service trouble. So, for obvious reasons it's best to do this late at night.

PAYPHONES

Regarding untraceable calls, payphone cannot be beat. In any given area there are anywhere from several dozen to a couple of dozen payphones which get used by thousands of different people every day. This large exposure makes it very difficult to impossible to get tracked down using a payphone. Furthermore, with the proper knowledge, free calls from payphones are somewhat easy to accomplish. There are two types of payphones which are in use: BOCs (Bell Operating Company) and COCOTs (Customer Owned Coin Operated Telephone).

BOC PAYHONES

BOC payphones are those set up by the local Bell Operating Company. These are usually Western Electric or GTE phones. The payphone itself is basically a regular phone with a coin mechanism, as the control functions are done from a phone company switching office. This function is known as ACTS (Automatic Coin Toll Service). A BOC payphone is easily identified as the name of the local phone company will be on it, and upon bringing the phone off hook and inserting money, one will hear a somewhat-muted tone pulse.

There are three methods to getting a free call from a BOC phone. They are: Red Boxing, T-Networking and "Ground Starting".

Red Boxing: A red box duplicates the tones that are generated by a BOC payphone when the coins are inserted. While red boxes are fully discussed (with schematics) in **"Beyond Phone Color Boxes"**, I will go into a little detail here. Coin tones consists of a combination of 1700 and 2200 HZ pulse trains who duty cycles and rates depend upon the coin inserted. Due to the function of ACTS, a red box is only usable on calls that cost more than the basic local rate. A red box is used by dialing the destination number, waiting for the "please deposit...." message, depositing a real nickel and then beeping out the difference.

Coin tones can be generated by three different methods. The first is, of course, by building a red box. This method is the most versatile but also takes the most effort and some technical skills. And by using a TI sound chip, red boxes can be designed to also mimic the sounds of the deposited coins - one of the ways that operates use to determine whether or not coins are actually being deposited.

The second is by generating coin tones on a computer and recording them. Many computers can do this. The recording can then be played back into the phone. With the advent of powerful laptop and book-size microcomputers, external circuitry can be designed to produce the actual tones. And computers can easily be programmed to also mimic the sound of the deposited coins.

The last way is by calling up a friend with a tape recorder or an answering machine and then depositing various coins. This method offers the most reliable way of generating coin tones, as your are not only getting them directly from the phone itself but you are also getting the sound of the deposited coins. However, this method is not very versatile, and the repetition of the same sounds over several coin deposit sequences could arise suspicions. Also, recorders often make telltale recorder-type sounds. And if caught with a recorder, the evidence against you is fool proof, whereas red boxes can be designed and computers programmed to make confiscation of the equipment of little additional risk to you.

Coin (cents)	Duration
5	1 pulse: ON for 66 ms
10	2 pulses: Each ON for 66 ms, OFF 66 ms
25	5 pulses: Each ON 33 ms, OFF 33 ms

The T-Network: The T-network is a method which prevents a payphone from collecting the money when a coin collect signal is sent. In order to understand how this works, it is necessary to know how a BOC payphone collects money. To collect or return money, a 130 volt pulse is sent down the phone line, which activates the coin collect or return relay, depending on the polarity. This pulse is sent down the phone line, thru the payphone activating the relay, and then to ground. What a T-network does is prevent this from happening.

To make a T-network, all one has to do is disconnect the ground from the payphone after the money is deposited, and before it is collected after the one minute period. There are two places one can do this. In an out side installation, one can look for a thick wire going down to a metal rod embedded in the earth. In an inside installation, the yellow and-or black wires on standard 4-conductor phone line cable are used to bring the ground from the payphone to the outside grounding line which is at the distribution box. By disconnecting/cutting one of these wires, the pay phone is isolated from ground and the coin collect/return pulse will be unable to do its job. After disconnecting the wires and hanging up, wait about one minute for the collect pulse to go thru, reconnect the wires and then pick and hang up the payphone. The money will then be returned to you.

Some semi-slick people have been known to leave the wires disconnected, and return a couple of days later to collect the money still in the phone. While this technique does have some success, there are a couple of things which can go wrong. The first is that some telco employer might come by and notice the disconnected wire. The second is that a customer might get pissed when the phone keeps his money and give repair service a call. The third is that the coin mechanism might become overloaded and jammed, which will alert telco, and cause you to leave the phone empty-handed. The last and worst thing that could happen is that telco might relay what you're doing and if they're in the right mood, stake out the phone and wait for you to return. So to be safe, only use the T-network for free calls, and not as a money making venture. If used as a money-making venture, be sure to make the disconnect look accidental and don't repeat on the same phone.

Ground-Starting: When a coin is inserted into a payphone, a 10K Ohm resistor is switched in between the tip (negative side) of a phone line and ground. This tells ACTS that a coin has been inserted, and is used for local calls. So, by placing a 10K Ohm resistor between the tip and ground of the payphone line, a free local call can be made. One can also accomplish this technique by taking a sharpened nail, drive it into the phone's mike and touch it to the phone's case immediately after dialing the last digit. The later technique though can destroy the mike, making the phone useless if done improperly. Occasionally, one can unscrew the covers on a payphone handset, thus exposing the mike or earphone wires. Shorting these to the phone body also has the same effect, with no chance of damaging the phone or telltale evidence.

COCOTs

COCOTs are also known as *"independent payphones"* or *"third-party payphones"*. Unlike BOC payphones, COCOTS are owned by a non-BOC telco concern. This ranges from COCOT companies, to motel chains, to private individuals. These are the same type of phone systems recently written up in the media as rip-offs as they are known to charge as much as 10 times what a BOC payphone call would have cost you for the same call. They deserve to be ripped-off!

COCOTs are easier to rip-off than BOC payphones for the following reasons:

1. The majority of people in the COCOT industry are technologically ignorant. The exceptions are people with prior experience in the telecommo industry, or people who were slick enough to read books like this and so on.

2. Except for the hook-up to the telco line, COCOTs operate independently of the BOC. This in itself limits things, but to add to it the BOCs hate COCOTs because it cuts into their payphone profits, and occasion ally do make life slightly difficult for then.

3. A lot of COCOT industry people are scumbags whose greed causes them to make mistakes, which make it easier for someone with balls and brains to screw them good.

4. The actual quality of COCOTS in general is inferior to BOC pay phones and ACTS. While a lot of this has changed, a lot hasn't. Since COCOTs operate independently of the local BOC, there are no ACTS which runs things for the payphone. Instead, the entire accounting functions must be handled by the payphone itself. All COCOTs have a small computer built into them for this purpose. This computer handles coin accounting, toll charge determination/rate steps and even contacts another host computer in the event of a situation such as a full coin box, or "vandalism". This set-up allows for some interesting free-call opportunities.

By-Passing the Phone: Since all the accounting functions are handled by the COCOT itself, the phone can be attached to a POTS (Plain Old Telephone Service) line. This was done in the early COCOT days. After a while people learned that they could call the operator, who would put the call thru for them like any other phone line, thus avoiding them having to put money in the phone. This made the COCOT industry phreak out, and they began designing their phones so a voice chip would say "Operator, this is a pay phone", whenever the operator was dialed.

Eventually though, the BOCs would create a "third-party coin box" classification for COCOT lines. This solved the dial 0 problem for them, and the COCOTs control computer would handle everything else. Well, almost. By connecting a butt-set to the phone line of a COCOT, you completely bypass the phone itself, and can call anywhere in the country, for free of course. You won't be able to make any operator assisted calls if you're on an actual "third-party coin box" classified line, but many COCOTS are still hooked up to POTS lines, particularly the small companies. Or the generic asshole, who owns the business that the phone is in, bought a COCOT thinking he'll make a million dollars off of it.

Diagnostic Mode: Many older COCOTs can be put into "diagnostic mode", which allows for on-site programming. If one had knowledge of the proper access code, usually a 4- to 10-digit numeric string which defaults to something like 000000, and knowledge of the proper programming procedures, then one could reprogram the phone itself to make a free call to wherever. While this is possible, there are other methods which are easier, and take less time. Also, the newer COCOTS need to have a key-switch turned on to get them into diagnostic mode, or need a special terminal which is hooked up to an IC socket inside the phone. Finally, most phones will call a certain number to report that they've been tampered with. The more sophisticated COCOTS can be remotely programmed via computer. Yes, you can defeat all the security measures, and reprogram the phone without the guy knowing, but it isn't worth the effort just to make a couple of free calls, and the guy is going to know something was up when he checks his coin box. However, if you're out to screw up a COCOT company, the effort might prove to be worthwhile.

OTHER TECHNIQUES

Besides the above techniques, there are a couple of other techniques which don't fit in any of the above categories. These are kind of limited in their scope and application, but work very well regardless.

Help Phones: There are two basic types of help phones. The first are those phones that are in ATM installations that people are supposed to use when they have problems with the beast after the bank has closed. Nine out of ten times that ATM help-phone is an ordinary line hooked up to an autodialer. Some even have instructions telling you to pick up the phone and push the red button. One can pick up the phone, and instead of pushing the button, use a touch-tone dialer or flash the switch-hook and make a free phone call to anywhere.

On the one's which dial as soon as you pick up, just wait until the customer service rep. answers and ask for John Smith, or ask if this is Cousin's Pizza. When she hangs up, the dialtone should return, enabling you to dial-out. Of course some phones don't have a switch-hook to flash, and use pulse dialing, in which case you're out of luck.

To get into an ATM site, just use your ATM card or any other card with a magnetic strip to open the card-activated lock. At that stage they don't check to see whether or not the card is legit. Still, some have security cameras, so preferably wear a 10-gallon sombrero and some stage makeup.

Occasionally, about one in every ten times, the phone is an extension of the banks PBX, which autodials an outside line and then the service number. In which case, hacking the outside line number may be in order. See the section in General Free Calls for PBX hacking.

Diverters: were used before call fowarding was around. A diverter is basically a device, which upon receiving a call on one line, would call an answering service or whatever else (business owner's home) on another line. Occasionally, after the call was done, if the caller stayed on the line, he would receive, and be able to call out on, the diverter's line. Furthermore, any calls to operators or other number's with ANI would get the diverter's number, thus effectively avoiding the possibility of getting traced.

Call fowarding has replaced many diverter's, and diverter abuse has alerted many answering services to this type of fraud, and now policies such as operators being the last to hang up were put into effect. The newer diverters are also equipped with circuitry which detects when the service has hanged up and then automatically terminates the call.

However, if you're interested in finding a diverter, just call doctors' and plumbers' offices after hours, and wait after the operator hangs up on their end. If you receive a weak dialtone, and ANAC comes back with a number which is different than the tone you're calling out on, then you've found a diverter. Just remember that this is all old hat, and many people now do things like put tape recorders on their diverter's line, which you won't know about until the Secret Service play you the tapes after they bust you. There are also ways to do things that diverter's do, such as using a cheesebox, or a butt-set.

AOSs

AOSs (**Alternate Operator Services**) is a term used to indicate the many new up-and-coming "phone companies" that offer operator services in placing calling card calls and other "operator services". Obviously, they compete against AT&T, MCI and the other legit telcos. Many AOSs are scams and work in conjunction with COCOTs, charging $5 for a call that AT&T charges $1.75 for. They are identifiable in that they are usually reached by dialing "0" from a COCOT, and that they identify themselves as a "phone company operator" rather than as an "AT&T operator" or a "NYNEX Operator". Fortunately, they aren't as sophisticated equipmentwise as a real operator as they usually don't know where you're calling from.

Because most AOSs deal with COCOTS, they automatically assume you're calling from a COCOT. What they don't know is that they are also usually accessible via a 10xxx equal access code from any phone. Being generally unscrupulous in their phone dealings, it is very easy to scam calls off of them for a change. One method which works very well is to make a third-party billing call to some number which never answers or is always busy. Often, they will just place the call thru, and bill the third party anyway, in their greed. The AOS service called "NTS" is well known for doing this. To find AOS services, just randomly dial 10xxx0, where x is any digit. If the person doesn't answer with a reputable name, then you've probably found an AOS.

TELECOMMO SURVIVALISM

For whatever reasons, the majority of phone phreaks (and computer hackers) aren't involved in the technological-survival movement, instead just being content to acquire information and occasionally cause some technologically-oriented anarchistic act. This observation is interesting because of all the underground groups around. They have the best access to free technical information ranging from C-4 explosive to computers, and also have one of the most developed communications and intelligence network; which despite its totally informal nature, operates on a par with some of our Government's alphabet soup agencies.

Of all the underground groups, the phone phreaks and computer hackers are the best equipped, yet the least active, in trying to change the system. However, despite their non-survival oriented views, much of their telecommo technology information is of direct value to the survivalist. With this information one can not only make free phone calls, but also avoid tracing attempts and use an already existing network to much expand your C3 (Command, Control & Communications) capability.

AVOIDING GETTING TRACED

In the good old days, the phone company had to actually manually trace down the phone connection to find out what the calling number was. You may have seen this in 1940s-60s vintage detective movies. This required some special equipment to be set up, and no small amount of time to do. The caller had to be kept on the phone for several minutes.

However, where the suspect phone call was expected on a system with the old stepper switches, the telco installed something called "lock and trace" which held the connection open even if the caller hung up. This gave the telco time to manually trace him down. In any event though, stepper switches are mostly a thing of the past and have been largely replaced with the computerized switching equipment: ESS (Electronic Switching System, by Western Electric), and the DMS series (made by Northern Telecom).

For the purposes of "tracing", both of these switches function the same. They don't actually trace. Instead, they have what is known by various names including ANI (Automatic Number ID), CID (Caller ID) or CAMA (Computerized Number ID). What these terms mean, is that the switching equipment notes the originating call number on it's accounting tape along with the number being called, and other "billing" information. And it sends it in the routing code to the destination switching equipment. If the right equipment is hooked up at the receiving end, they know the originating number before they even pick up the phone.

Various methods are used to indicate where the originating number is being sent to. ANI is the general all-purpose method used. CID is used when the number is being sent to the destination. CAMA is used when the number is recorded for accounting/billing purposes. The effect is all the same though.

ANI is now standard on any BOC or LDS operator line (with the exception of some AOSs), any 911 emergency lines, any LDS access dialup (with the exception of some older lines mentioned in the phreaking section). It is capable of being quickly implemented on any non AT&T 800 WATS line, such as the new ones being offered by MCI and U.S. Sprint. If you call any of these systems, it is certain that they will instantly have your number. The way to avoid this is simple. Just make the call from a phone that can't be traced to you, and if it's a serious enough matter, disguise your voice and never use that phone again for that or similar purpose.

COMMAND, CONTROL & COMMO (C3) TECHNIQUES

The nationwide telecommo network is well suited for C3 operations. Unless you're in the middle of a wilderness or similar place, there are phone lines within a 30 second walk of where you're at right now. And a convenient place to hook into said phone lines is within a 5 minute walk of where you're at right now. From such a hook-in place you can dial just about any location in the country. The capability of the telecommo's network is expanded to the point where you could be some distance away from the actual phone lines and still be able to use it. When combined with other C3 techniques (see the freedom fighter's guide section), the telecommo network becomes a powerful tool. Furthermore, a powerful telecommo network of such a large scale virtually unique to this country, so an invading power will most likely underestimate it's capability to be used by freedom fighters and ignore it as a threat.

PAYPHONES

Payphones are commonly used for commo in large cities by drug dealers and illegal gambling operations. If they can use them, I don't see any reason why a survivalist can't. For outgoing calls, payphones can be bypassed using the techniques listed in the phreaking section. Most pay phones also receive calls, enabling people to call you as well. As a rule, BOC payphones can get incoming calls, altho sometimes the phone's ringer is disconnected or the line is classified to not accept incoming calls. However, this is rare.

COCOTS generally cannot receive incoming calls because of the phone's capability to be remotely programmed. However, some still can, and if the phone is bypassed, one can receive phone calls without the COCOT itself interfering. If one intends to do this, go around to the various pay phones in your area and copy down the numbers on the phones (or call ANAC to get the number). After a while you will have an impressive list of payphones and locations. The uses will be limited only by your imagination. The one major advantage of payphones is that they're always there and only a little bit of planning is needed to use them.

Payphones are also great for low-profile peacetime survival operations where running around with sophisticated commo gear might bring suspicion upon you and provide evidence against you. A person dialing a payphone or picking up a ringing payphone is nothing unusual, and you probably won't get noticed. Furthermore, spontaneous payphone use is undetectable, unless you've been a major pain-in-the-ass to the powers that be and are under surveillance or being especially observed.

BRIDGING HEADS

Bridging heads, also known as "B-boxes", "Cans" or "Pedestals", can be hooked into for a quick and reliable commo. The terms all mean the same thing, but *Bridging Head is generally used to indicate the larger boxes, Can is used for the smaller ones and Pedestal is for the ground mounted ones used with underground phone lines.*

For a more permanent set-up than a butt-set, one can just connect a long length of wire from the terminals to a modular jack and hook in conventional phone equipment. One can also hook up "field phones" to the unused terminals, also known as spare-pairs, in a bridging head and use them for commo to and from areas covered by that particular cable.

If one finds the main bridging head for an area, with a little work with some dweedles and some splicing, one can hook up a private line between any two locations in the neighborhood. This is done by taking the two dweedles, or even a regular tone generator, and hooking them up to the beginning of the cables where you want to have a commo link. You then go to the appropriate bridging heads, find the cables by checking for a tone, disconnect them from the telco side of the bridging head and connect them together.

If the lines are active and you're good with electronics, you could also make some tone-activated relays and hook your commo link to the telco side of the line to be able to dial to the outside world if necessary. This is possible because of the design of a bridging head (see Figure TP4).

A Bridging Head is just like two giant terminal blocks put together to act as a testing point, as well as a cable splice. Each phone pair is assigned two terminals in a Bridging Head. The two terminals are connected together and act as a splice. The line goes from the Central Office to one terminal set, and from the other terminal set down the line to the subscriber. This only applies to the bigger Bridging Heads which look like large (4 feet high) silver boxes on telephone poles, or the large beige boxes that sit on the ground. The smaller ones only have one set of terminals for each pair and are used as a splice from the telco lines to the subscriber drop line going to the subscriber's residence. To fully understand this, go visit some Bridging Heads in your area and examine them, or get friendly with a telco lineman who'll be able to explain it to you.

PAGERS

Pagers are another drug dealer favorite - ideal for one-way commo link with a lot of potential. For example, a local paging company in New York is offering a pager service package for $38 that features an 800 WATS dialup reachable from anywhere in the country and pager coverage from New Jersey to Massachusetts. It is available with either a display pager or VRS setup. For $38 a month, you have a reliable one-way commo link covering an area the size of 4 states.

There are four basic types of pagers in service. The first is the classic "beeper", which simply just beeps to indicate that you have a page. This is most often used by doctors and other professional and trades types to receive indication of an emergency call from their office and answering service. Or in conjunction with businesses who use it with an answering machine and a device which calls the pager when a message is received. Its advantages is that it's the cheapest service around, but unless you're using an answering service or machine, there's no way to tell who's paging you but only that you've been paged.

An expansion of this is the VRS (Voice Response System) pager. This is a voice mailbox hooked up to a pager. The person calls the pager, leaves a message and you get paged. You then call the number, enter a code and retrieve your message. This looks just like a typical answering machine or ordinary voice mailbox to the unwashed public, and it is a cheap way to have an 800 line if that option is used, thus enabling you to give yourself, your business or any "operation" underway a certain appearance ("Yes, you can reach me through this 800 number"). It's disadvantage is that the VMB on the pager is only protected by a 4-digit numeric code, and some one who knows it for what it is might be able to break the code and retrieve your messages.

The third and most popular method is the display pager. With this system, the person calls up the pager, enters his phone number with a touch-tone phone and then you receive his number when he is paged. This system allows for a very secure link when a code is used instead of entering a phone number. Indeed, a short message could be sent to you via a display pager. Pager codes are described in the cryptography section. The disadvantage though is that the person calling you has to have a touch tone phone.

The last type is the voice pager - not to be confused with a VRS pager. The voice pager allows the caller to leave a short message,.the paging system then sends the message over the airwaves and thru your pager. This system has a few disadvantages. The first is that once the message is sent, it's gone, you cannot hear it again. The second is that it isn't too private - your message is going out thru the airwaves and can be surveilled using RF techniques. Wrongdoers and pranksters can also place embarrassing messages on your paging system.

Even though the privacy bit could be taken care of with a quick verbal code, a VRS or display pager would serve better. Voice paging systems can be used for free though. To do this, one finds what exchange the voice pagers are in, and on what freq. Keep a receiver tuned to the freq and give your friends "the number" and a code phrase to say on the pager. When they call and leave the code phrase, you'll hear it on the receiver and call them back. This works well, altho you will be using someone else's pager number, who will keep receiving these cryptic phrases. When doing this, have the code phrases sound like a line test is going on and don't keep calling the same pager number.

WIRELESS PHONES

Once a status symbol of the upwardly mobile, wireless phones - including cordless, IMTS and cellular phones - are within most people's reaches. This is good because they offer many opportunities for the technological survivalist. To begin with, wireless phones offer all of the same opportunities as their hard-wired relatives, plus the added advantage of not having to be tied down to the physical phone line to enjoy the advantages of that commo medium. This all adds up to flexibility and mobility -often the keys to success. As expected, wireless phones offer their own opportunities for both C3 techniques, as well as for "phreaking" - the jinking around in the telecommos network to save money, and avoid being tracked/traced. Of course, they do have the same disadvantage as other radio equipment in regards to easy interception, but if you've read this far you'll know how to take care of that.

One form of wireless phone which isn't recommended are cellular phones. Cellulars are becoming increasingly popular, as the cellular industry, after successfully pushing the E.C.P.A., promotes them as being convenient, inexpensive (bullshit!), and oh so upwardly mobile. The truth is that the entire cellular system, as well as the cellular industries sales procedures, make cellular phones easily traceable and surveilled. Since the advent of cellular phones, there have been dozens of civil legal cases and criminal defenses based upon the surveillance of cellular phone conversations.

To start with, due to the design of the cellular phone system, not only is your phone instantly identifiable upon transmit by anyone, due to the ESN (Electric Serial Number) built into the unit. And due to cell-site layout, you are traceable down to a few square miles of area. Add to this the fact that the cellular system is completely computer controlled and you have the wireless version of Big Brother. About the only factor of this system that you have a remote chance to circumvent is the ESN on the phone, which requires (at this time) a contact in the part of the cellular industry which deals with ESN programming, which isn't worth the effort and money with everything else available. If you still want to attempt it, start with an early model cellular phone. The earlier the better, particularly Novatel or Radio Shack.

For much more information on cellular phones see our **Cellular and Cordless Phreaking** manual.

CORDLESS PHONES

Cordless phones need no explanation, as most everyone seems to have one or two. However, there seems to be an unexplainable lack of accuracy as to the freqs used on them. Cordless phones use two freqs simultaneously for full-duplex commo. Currently, there are 3 freq pair ranges used by cordless phones. The first is a 1.7 MHZ/49 MHZ split. These are used by the first cordless phones; where the base transponder transmits in the 1.7 MHZ range and the handset transmits in the 49 MHZ range. The 1.7 MHZ carrier uses the AC power lines in the house as an antenna (This is known as "Carrier Current" transmission). Because of this fact, the range was limited and the connections generally sucked because of interference from the 60 HZ power line freq. While no more of these units are being made, they still can be found used at tag sales and flea markets. These freqs are (MHZ):

Base	Handset
1.705	49.830
1.735	49.845
1.765	49.860
1.795	49.875
1.825	49.890

It is also interesting to note that the above 1.7 MHZ freqs are also used by those "Wireless Intercoms" sold by Radio Shack. The second pair of freqs is 46 MHZ/49 MHZ. All cordless phones today use these freqs. The elimination of the bothersome 1.7 MHZ side clears up interference and also allows for a longer range. Another thing which the FCC did when allocation the 46/49 splits was include more channels to lessen interference from other phones. These freqs are (MHZ):

Base	Handset
46.610	49.670
46.630	49.845
46.670	49.860
46.710	49.770
46.730	49.875
46.770	49.830
46.830	49.890
46.870	49.930
46.930	49.990
46.970	49.970

It is interesting to note that the 46 and 49 MHZ range is also allocated for U.S. Government use, specifically the military. This discrepancy stems from two reasons. First, the FCC doesn't handle governmental allocations - an organization called IRAC (Intergovernmental Radio Advisory Committee) allocates them. Second, the FCC feels that the range of cordless phones is so limited that it won't cause interference.

The third pair of freqs used is 49 MHZ/70 MHZ. These were used by cordless phones designed for export to foreign countries. While they are illegal, that doesn't stop people from using them.

"Cruising for dial tones"

In the early days of cordless phones, the lack of security features on them made it easy for someone to take his handset and drive/walk around the neighborhood, finding out how many dial-tones he could bring up. Nowadays, the addition of various features to prevent this make it very difficult.

There are four major security features used in cordless phones: The first one disconnects the base transponder from the airwaves if the phone is put in its charger slot. While there is no way to circumvent this, keeping the phone in its charger slot appears to many people as a limitation of its mobility. Thus, many people keep them lying around OUT of the charger slot, right by their side, so they don't have to run for the phone when it rings. Thus, their desire for convenience bypasses this security feature.

The second feature is a digital code which the handset sends to the trans ponder when it is brought off hook. The transponder checks the code and if it matches, a dial tone is presented. This code is either preset at the factory or user-set by manipulating a couple of DIP switches. The changing of the code on preset units requires you to go inside the machine and clip/add a few diodes. With the user-set ones, all one has to do is try every code until you get a dialtone. Most sets have 4-8 switches for the security code. The security code is transmitted via a digital tone, similar to that used by IMTS signaling.

To hear what I'm talking about, get your handset and a scanner. Tune your scanner to your handset freq and then bring your handset off hook. As you bring it off hook, you should hear a beeping tone. That is the security code being transmitted. Now, if you had a slightly modified 6-meter ham transmitter and lived fairly close to your neighbor with a cordless phone, you could possibly record his security code and play it back thru your transmitter (thus successfully impersonating his hand set). While I don't know of any compatibilities between cordless phone security codes at this point, if I hear of any, they will be posted in the next available reprinting of "By an Order of the Magnitude" or perhaps another CONSUMERTRONICS manual.

The third security feature, and most common, is the use of subaudible or "PL" tones used to keep other cordless phones to access your base. This is also used by commercial business band radios to prevent unintentional interference on shared freqs. This tone is a low level audio signal which is superimposed on a transmission. It isn't supposed to be heard, but often is as a low background tone on a signal. The receiver checks for this signal, and if present, opens the receiver squelch. On a cordless phone, the receiver checks for the presence of the PL tone on a signal, and if the proper tone is received, brings up a dialtone. There is a piece of test equipment available for about $100 and it will generate all standard PL tones, and one could be made for much less.

The fourth security feature was designed a few years ago but hasn't been marketed yet for some reason. This security feature is complete digitizing of the phones audio using PCM (Pulse Code Modulation), very similar to what's used on digital trunks. This makes the conversation completely unintelligible to the ordinary scanner listener. I've had no experience with this nor have seen any phones which used it. A good place to start with decoding it would be to get a hold of a phone which uses voice digitizing and work from there.

Increasing Your Range

Once cordless phones came out, someone got the bright idea of extending their range. Most people think that an amplifier can be built which would give you more power and extended range. It isn't that simple. Since a cordless phone is a full-duplex radio link, an isolator is needed to physically keep the two channels separate.

Unless you have a degree in Radio Engineering, your attempts at making this would most likely ruin the unit, and any successful attempts would make your cordless phone about 10 times its current size.

However, there is another way to extend your range and that is by adding an external antenna on your roof. This will only work with 46/49 MHZ units, as this antenna will only boost the 49 MHZ side on 1.7/49 MHZ units. On those phones, the 49 MHZ side is usually OK, and you'll still have to put up with the poor signal on 1.7 MHZ. In any event, you'll need 5 lengths of stiff wire (coat hangers) 47 inches long, one SO-239 coaxial cable connector and enough good quality (RG-8) coaxial cable to get from your phone to your roof. This cable should have a PL-259 connector on one end and alligator clips on the other. Take the wire, and attach it to the SO-239 as shown below:

```
                         |
Wire attached—›          |
to center hole           |
                         |
                         ^
Wire attached          /=\  ‹—SO-239 Connector
to outer              / * \
       holes——›      /  $  \  ‹—PL-259 Connector
       (ground)     /   |   \
                        |
Coaxial                 |
Cable ————›             |
                        |
                    Down to
                   Base Unit
```

At the base unit, attach the center conductor to the whip antenna, and attach the other connector to the chassis (ground). For those lacking in antenna building skills, there are also commercially available units for about $50.

IMTS

IMTS (Improved Mobile Telephone Service) is an automated telephone system which used to be the standard of mobile phones until cellular came along. IMTS freqs are (MHZ):

Channel	Base Freq.	Mobile Freq.
ZO	35.26	43.26
ZF	35.30	43.30
ZH	35.34	43.34
ZM	35.38	43.38
ZA	35.42	43.32
ZY	35.46	43.46
ZR	35.50	43.50
ZB	35.54	43.54
ZW	35.62	43.62
ZL	35.66	43.66
JL	152.51	157.77
YL	152.54	157.80
JP	152.57	157.83
YP	152.60	157.86
YJ	152.63	157.89
YK	152.66	157.92
JS	152.69	157.95
YS	152.72	157.98
YR	152.75	158.01
JK	152.78	158.04
JR	152.81	158.07

There are also freqs allocated in the UHF Range. The base freqs are posted below. The mobiles operate 5 MHZ above the base freq. Thus, the mobile freq for channel 21 is 458.025.

These IMTS freqs are (MHZ):

QC	454.375
QJ	454.40
QD	454.425
QA	454.45
QE	454.475
QP	454.50
QK	454.525
QB	454.55
QO	454.575
QR	454.60
QY	454.625
QF	454.650

The VHF high-band freqs are the most popular IMTS freqs. If you live within 25-50 miles of anything resembling a moderate size town, you will have at least 1 VHF high-band channel available. VHF low-band channels are used primarily in rural areas and those with mountainous terrain. UHF channels are being used in cities where the VHF channels are becoming crowded. If you live in a major city, expect to have most, if not all, of these channels available to you.

IMTS Signaling: IMTS signaling is accomplished by in-band signaling tones from 1,300 HZ to 2,200 HZ. Two single-freq tones are alternated, much like ASCII modem tones, to produce the digits for both the ID and destination numbers.

The tones are: BASE TONES: Idle - 2,000 HZ - used to indicate an available channel. Seize - 1,800 HZ - sent as an acknowledgment by the base that a channel has been taken.

MOBILE TONES: Guard - 2,150 HZ - used when the mobile goes off- hook to seize a channel, as the "space" tone when sending the ID and destination number and to acknowledge an incoming call. Connect - 1,633 HZ - used to "pick-up" and incoming call, and as the "mark" tone in sending the ID and destination number. Disconnect - 1,336 HZ - used to disconnect.

To originate a call, the mobile sends 350 ms of guard tone followed by 50 ms of connect tone. The base then stops sending the idle tone, stays quiet for 250 ms and then sends 250 ms of seize tone. The mobile sends 190 ms of guard tone and then sends the ID number at 20 pulses per second. The ID number consists of the subscribers A/C and phone number. The pulses consist of 25 ms of connect tone, followed by either 25ms of silence or guard tone, depending if the digit is odd or even. The interdigit interval is either 190 ms of silence or guard tone, depending if the last digit was odd or even. Once the ID is sent, dialing is accomplished by sending alternating connect and guard tones at 10 pulses per second - a pulse is 60 ms of connect tone followed by 40 ms of guard tone. To disconnect, send 750 ms of disconnect tone.

Getting an IMTS Phone: IMTS phones can be bought from electronic surplus dealers, however these may need some work and you'll have to figure out how to repro gram them. I've also seen the ID circuitry torn out of them when sold as surplus in order to keep people from doing what's described here. Your best bet is to go to a hamfest/electronic fleamarket and pick up a business band mobile radio. These are surplus units capable of transmitting in the 150-174 MHZ range. While these units are often modified by hams for 2-meter (144-148 MHZ) or 3/4-meter (440-450 MHZ) band, they can be modified back to the business band. All that most of these units require to be brought into the IMTS band is the proper crystal and the retuning of a capacitor or two.

This, along with a cheap VHF high-band receiver, makes a full-duplex radio setup (be sure to use headphones with the receiver to avoid feed back). You now need to duplicate the tones. There are two ways to do this. The easiest and most versatile is to use a computer and generate the tones, but since few computers with tone-generating capabilities are portable, an alternate method must be found. By wiring up an ordinary phone dial to a dual-tone audio oscillator, you can duplicate a mobile phone dialer. Plans for this unit can be found in 2600 Magazine. With your "IMTS Box", *you can either tape an ID number off the air or generate one with your computer. To use your homebrew IMTS phone, find a channel that has an idle tone on it, send your connect and ID tone sequence, dial your number and you're connected.*

Marine Band

The marine telephone band is for ships to communicate with landbased phones. A marine band phone call is put thru by finding an unused freq, calling the marine operator and giving her your callsign and phone number to call. The freqs are (MHZ):

Channel	Ship Freq.	Shore Freq.
24	157.20	161.8
84	157.225	161.825
25	157.25	161.85
85	157.275	161.875
26	157.30	161.90
86	157.325	161.925
27	157.35	161.95
87	157.375	161.975
28	157.40	162.00

Marine Band Radiotelephones: While you could take your business band radio and put in marine band crystals, Marine Radiotelephones are easily available and somewhat inexpensive ($100-$300 for a decent radio with VFO, memories and 25 watts output). Before using your radio, listen on the phone channels for a contact by another ship and copy down the callsign used. Wait a while and then use the callsign to place a call. DO NOT USE YOUR OWN CALLSIGN IF YOU GOT ONE! If you do, expect to pay for a buck a minute minimum call. Marine telephone is one of the easiest ways for "wireless" commo, however, it still presents the same dangers as IMTS phreaking.

Ham Radio Autopatch & Simpatch: Autopatch is a function put on many ham repeaters allowing the use of a phone-line over the air. While you could phreak using an Autopatch, I advise you not to as there is usually a control operator monitoring the machine (some do it 24 hours per day) and any attempts at hacking an access code will probably be flagged. Being a Ham, I'm not going into the subject of Autopatch any further than this, as there are better ways to phreak and Ham's are helpful people whom you can get assistance from on technical matters. Don't mess with Autopatches!

However, along the lines of an autopatch is something called a Simpatch, which is a simpler version of an autopatch designed for use with a ham transceiver. This device makes a wonderful extended-range cord less phone when hooked up into a Can (discussed earlier). It's major drawback is that it's expensive, but anyone with a little electronics background can probably build one.

A simpatch can also be used with CB's or just about any other radio. A good idea for an extended range cordless phone would be a simpatch and two CB walkie talkies. One CB would be connected to the Simpatch that is connected to the Can and accessed via the second walkie talkie. The entire setup could be hidden in a tree and using a wire antenna (dipole of 1/4-wave vertical) for a range of 5-20 miles.

C (cubed) POSSIBILITIES

Wireless phones offer some interesting possibilities in the area of C3 operations. Of all the various types, the most versatile are the cordless phone and the simpatch. The mixture of radio and telecommo technology seem to make a natural team together, greatly increasing flexibility for your survival commo network. This is particularly impressive when used in a "dedicated line", or private telecommo network like the field-phones used by the military.

Bridging Heads

Both cordless phones and simpatches can be hooked up to batteries and wired into a Bridging Head. This would make a nice quick & dirty patch into the DDD network. However, if discovered, you risk losing your equipment unless it's tamper-proofed (read: bobby-trapped), but at least you won't get caught, which has happened to people who have hooked-up butt-sets to bridging heads to reach out and touch someone.

Cordless Phone Tricks

There are plenty of cordless phones around and they'll still probably be around after the "shit hits the fan." Since they're so commonly avail able and are wireless commo equipment, they make excellent candidates for converting into expedient commo equipment. When playing around with cordless phones, remember that you can always add an antenna to the 46/49 MHZ models for increased range, (up to a mile which isn't bad for something improvised like this), and you can also go portable by hooking up the proper voltage batteries directly into the power jack for units that have separate transformers, or by simply wiring them in after the power supply circuitry.

Most cordless phones have a built-in intercom which enables people at the base transponder to contact the remote unit - instant two-way commo. If your unit doesn't have such a feature, it could be emulated by hooking-up a regular phone, talk battery and a ring generator to the line connector of the cordless phone. When combined with an external antenna, you'll have a full-duplex radio link with up to one mile range.

A cordless phone repeater of sorts could be rigged up and placed in a remote, high-elevation location which would allow two cordless phone remote units to talk to each other. This is done by wiring two cordless phones of different freqs back-to-back with the same setup used above with the addition of a touch-tone decoder hooked-up to either the intercom page section or to the ring generator. With directional antennas used on the base transponders, this would make a quick & dirty point-to-point commo link capable of extending a phone's range twofold.

You could also separate the phones by some distance as well, for example putting one end on the north side of a hill and the other on the south side. Most late model cordless phones have touch-tone dialing. So, each cordless phone handset is half of a complete remote control set-up. All one needs is a 49 MHZ receiver and a touch-tone decoder, both of which are easily bought or made. A remote control setup using a cordless hand set would be usable out to about 1000', and perhaps more depending upon the sensitivity of the receiver and the antenna gain on the receiver.

Telecommo Remote Control

There are two quick methods for remote control via a phone line. The easiest is ring detection. This can either be done with a ring detector/ driver IC or with a 120 VAC relay. The output of whatever you choose is hooked-up via the appropriate circuitry to whatever you wish to control. It's hooked-up to the phone line and when the phone rings, your device is activated. Radio Shack sells the "Phone Flasher" which is hooked up to the phone line and an electrical outlet, and will turn ON any 110 VAC device when the phone rings. Deaf people hook it up to lamps to tell them when their phone is ringing. The only disadvantage is that once it's hooked up, the next incoming call will activate your device. The way around that is to use the IC hooked up to a counter circuit. Now the phone will have to ring "x" number of times before your device is activated.

The most versatile way for phone remote control is via touch-tone. This device would consist of a touch-tone decoder, auto-answer circuitry and perhaps some transistor switches to handle the activation from the decoder to the device. In this case, you call, the phone answers itself, and you wait for the proper code to be entered. Besides using touch-tones, you could also use single audio tones and even AFSK tone bursts for added circuitry. It's just that touch-tones are more convenient.

One way to get the phone to answer itself is by electronically tapping into an answering machine's cassette motor-ON signal. This is really nice because it allows you to dictate the number of rings for the desired response, and you can follow up by leaving a time or other message on the answering machine as a record of your call. Another way is to audibly detect the rings by using a mike and audio amp similar to the el cheapo built-in units sold by Radio Shack.

A third way is to use an IC called the CPD or "Call Progress Detector". CPDs provide output returns depending upon the phone line activity. They are made by three companies: Signetics (811 E. Arques Ave, Sunnyvale, CA 94088), Teltone (120th Ave, NE, Kirkland, WA 98033) and Silicon Systems Inc (14351 Myford Rd, Tustin, CA 92680). The Teltone and SSI devices return outputs for each freq of the freq pairs that makes up ringing, dial tone, busy and reorder, while the Signetics devices return outputs for the actual ringing, etc. I prefer the Teltone devices because the external decoding circuitry I use with them provides a more reliable indication of ringing, etc. than does the Signetics devices.

THE CHEESEBOX

The Cheesebox is the one underground telecommo devices which has had more erroneous rumors about it than any other similar device. Since the cheesebox is one of the most misunderstood and useful devices a techno logical survivalist could have, I will clear up all the misconceptions about the cheesebox: What it can do, what it can't do, and finally provide up-to-date plans for one that works. Despite everything you've heard from other sources, this IS the definitive cheesebox explanation. I've researched the cheesebox for 5 years and would not say this unless I was absolutely sure about it, just like everything else.

Enough harping. The basic cheesebox definition is a device which allows two or more different phone lines to be connected together. This allows you to take two phone lines and make what is known by phone phreaks as a "loop number". With a cheesebox and two phone lines (A & B), you can call into line "A", have another party call line "B", and you will both be connected without the need for you to know each others phone numbers or to have to call the other party directly.

What this does is add a bit of privacy and security to phone use as nobody knows where the other party is, and the other party's phone number won't show up on a DNR. Also, a cheesebox can be put in a remote location far away from where you actually are, so if by chance the police decide to raid the place where all your phone calls go to, they'll run into a dead end. For those reasons, cheeseboxes were used by organized crime to run "bookie" operations in the old days.

A cheesebox would be combined with a Black Box (see **"Beyond Phone Color Boxes"**) to avoid toll charges. A cheesebox/ black box combination could be as small as a dime (the old plans I have use only 4 parts) so it could be hidden anywhere along the phone line and hooked in. This helped confuse police as they would raid a place and find nothing.

A couple years later, some phone phreak got the idea to modify the cheesebox so that he could call into Line A and be able to dial out on Line B. The reason for this was to avoid getting traced/ANIed, as the number that would show up would be Line B and not the phreak's actual phone number. This device was discovered by telecom equipment makers, mated with an autodialer and then called a "diverter", and later on an "automatic call fowarder"!

Both styles of cheeseboxes will still work, but there are some bugs with the system. With most of the country on ESS, black boxes won't work anymore, and as an almost integral part of the cheesebox, made all the old cheesebox plans obsolete as the zener diode black box was what picked up the phone. With ESS, one must use a relay or something similar and the free call side-benefit is no more.

The second problem is with the dial-out variation of the cheesebox. Unless one adds a tone-to-pulse converter, Line B (outgoing line) must have touch tone service. Figure TP4 shows the plans for a cheesebox. For a dial-out version, all one has to do is make one relay section and omit the isolating capacitors. The disadvantage with this unit is that anyone who calls in will be connected to the other line. However, this device requires no power other than that of the phone line, which saves the aggravation of batteries but can be easily detected and destroyed on the line. You could include a touch-tone decoder or a ring-counter with the basic circuit, but it would require external power. Radio Shack also sells an *automatic call fowarder* which might have some possibilities, and other such units are also available as well.

A cheesebox is very useful to the technological survivalist. It allows for anonymous connections with other survival groups who you may not fully trust at the time, and the out-dialing variant also allows for untraceable calls, which can be greatly discounted or free depending on where you put the cheesebox. While one could place it in the same exchange as you or to a close one, I feel that's a little too close to home. I'd put it in an exchange about 20-50 miles away and use one of the other free call methods to call it. That way, on their first "trace" attempt they wind up tracking you down to a location well removed from where you are. Cheeseboxes can be connected anywhere there are two phone lines. Tamper-proofing them is usually a good idea.

PRIVATE TELECOMMO NETS

In some instances, you may want or need telecommo capability which does not go thru the regular switched telecommo network. Your need for privacy may be too great to use an "open line", or that the switched telecommo network may not be functional in your area of operations due to extensive damage, or the fact that you live in the boonies where there is no service. It is in these cases that you may need to become your own telco - installing your own telecommo network for your own commo needs. A private telecommo network has the advantage of operating independently of Ma Bell. This leads to increased security in certain situations as well as the ability of staying on-line in the event that Ma Bell's network goes down.

INTERCEPTION OF TELECOMMO

Unknown to most people, a great majority of telecommo traffic goes over either radio or microwave links. These links range from simple cordless and mobile phones, to satellite and microwave links. Most of these commos are easily heard with readily, available equipment. One mode can even be received via a common AM radio!

Radio and microwave links open up many possibilities for phone surveillance, enabling one to remotely "tap" a line with little risk of discovery. This fact is multiplied when most people don't realize just how insecure their phone can be. For example, a couple of years ago I over heard drug dealers discuss their business over their mobile phones. They appeared to be totally unaware that anyone was able to listen to them. A couple of days later, there was a major drug bust. Obviously, others were listening as well.

At another time, I overheard two people discuss their extramarital affairs over a cordless phone. I happened to be tuning across the top end of the AM broadcast band when this sordid, graphic, totally uncensored conversation came in loud and clear over the radio! And I thought you had to watch daytime TV to catch a soap opera when there was a real-life one going on down the road from me!

Even regular phones aren't totally safe. If you make a long distance call, chances are part of your conversation will be carried over a satellite or microwave trunk. Satellite trunks are readily accessible to anyone will a common TVRO station, and any individual with a moderately technical background can adapt common hobbyist equipment to intercept microwave trunk commo.

Furthermore, it is common knowledge that all international telecommo traffic - particularly satellite traffic - is routinely monitored by the NSA, and other intelligence agencies. In El Paso, TX, the DEA maintains an awesome telecommo eavesdropping facility that covers the entire South West.

The Russian Embassy in Washington DC is placed on one of the highest elevations in the city, and has a roof bristling with commo antennas. It's really quite a sight! While the exact nature of their system is not totally known, it is reasonable to believe that at least some of those antennas, particularly the horizontal dishes, are used for interception of microwave telecommo traffic.

Little is done about these surveillance gaps in the telecommo network. Recently, the U.S. Government decided that they will begin scrambling their private networks, and switching to non-wireless links for added security. How long this will take is yet to be determined. The public telecommo services still, by far, deny any lack of security in their networks, and so far no steps have been taken to alleviate the problem.

Cordless and mobile phone makers are also loath to inform the public of a possible security problem with their phones, despite the fact that articles and at least one book have been published discussing not only the vulnerability of these systems, but also providing details as to eavesdroping procedures. Recently, a proposed law was scrapped by the U.S. Congress requiring cellular phone makers to put warning labels on their phones. Obviously, the makers didn't want buyers to know that their newly bought $1000 car phone was about as private as a PA system.

LAWS: Knowing that their new toy wasn't very private, the cellular industry needed an excuse to be able to push their phones without the public realizing their shocking security deficiencies. Thus, The Electronic Communications Privacy Act of 1986 - better known as the Cellular Phone Manufacturer's Relief Act - was passed, thanks mostly to heavy lobbying and bribery "contributions", by the cellular phone moguls.

The ECPA prohibits the eavesdropping of mobile phone conversations, and a few other modes of electronic commo thrown in to make the law look substantial. It also outlaws the manufacture of radio receivers specifically designed to receive mobile phone commo. The FCC and Justice Dept. stated that the law was unenforceable, and that they would not enforce it. However, it was passed anyway.

Since its passing, the law has been invoked. The first time was when it was found that MCI was reading its MCI Mail subscribers' private electronic-mail and publicly announced that they didn't care that they were breaking the law. Several parties attempted to bring charges against MCI for its many violations of the E-mail provisions of the ECPA. No-go.

Shortly thereafter, a cellular maker contacted the FBI because it was annoyed that a dealer of commo equipment had the gall to modify commo receivers to receive cellular frequencies. Despite the fact that such mods are clearly legal under the ECPA (it only bans specifically-designed receivers for that purpose), the FBI harassed and threatened the dealer, who stopped performing the mods. From these examples, we clearly see that the ECPA was designed only as a tool to help the cellular phone industry control both the industry and the people.

INVESTIGATIVE REPORTING: When cellular first became hot, I went to several cellular phone dealers posing as an individual interested in purchasing a phone. I saw 6 different dealers in my area, including AT&T, and the office of the local cellular phone service. The responses I received were one of two standard ones when I asked them about security:

(1) Knee-Jerk Response #1: *"No one can pick up what you're saying"* - sometimes infused with explanations about how such interception equipment is terribly expensive and thus unavailable.

(2) Knee-Jerk Response #2: *"Don't worry, there's a law that makes listening in illegal"*. In one such store, I observed a scanner searching thru cellular frequencies!

From these examples at least in my area, clearly the dealers must either be totally ignorant or purposely lying - probably mostly lying.

FREQUENCIES & TECHNIQUES: As stated earlier, most forms of wireless telecommo can be intercepted with commonly available equipment. There are a few basic pieces of equipment that one requires to intercept telecommo:

(1) A common VHF/UHF commo receiver or scanner. This device will receive mobile and cordless phone conversations. Some of the later models will also receive cellular, but usually some modification is required, such as the infamous diode on the Radio Shack Pro-2004, see our SECRET & SURVIVAL RADIO.

(2) A shortwave receiver. This device will receive the older cordless phones, ship-to-shore commo still on shortwave, and also satellite commo when hooked up to a TVRO station. The last piece of equipment is a TVRO receiver set-up.

CORDLESS AND MOBILE PHONES: The frequencies for cordless and mobile phones are discussed in the Telecommo Techniques chapter. You can usually expect a range of a couple of city blocks just from the built-in antenna of the scanner. An outside antenna can increase your range to a mile or more. On rare occasions, the older cordless phones on 1.7 MHZ have been known to go several hundred miles, but that is rare, and the older phones are obsolete. (see our CELLULAR AND CORDLESS PHREAKING manual for much more info)

The antenna discussed in the Telecommo Techniques section is perfect for receiving cordless phones on 46/49 MHZ. Expect a 1 - 5+ mile range. For mobile phones, one can get up to a 50 mile range from any omnidirectional high-gain 2-meter antenna, such as a Ringo Ranger or AEA Isopole (my personal favorite). With a 19", 1/4-Wavelength antenna, expect a 20 mile range.

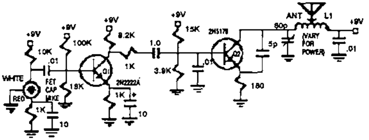
CELLULAR PHONES: Any standard cellular phone antenna will do a good job picking up transmissions. Expect a 5 - 20 mile range depending on terrain and extent of cellular activity. Use coax cable with low loses at UHF, and use as short a length as possible for your feedline. The frequencies are: 824.010 - 849.000 (Mobiles), and 869.010 - 894.000 (Base or "Cell Sites"). Frequencies (in MHZ) with a .030 MHZ spacing. (see our CELLULAR AND CORDLESS PHREAKING manual for much more info)

SHORTWAVE: Various frequencies are used for telecommo from remote areas over seas. A standard shortwave setup is all that is needed. The frequencies are (in KHZ):
4357 - 4434, 6506 - 6521, 8718 - 8812, 13100 - 13197, 17232 - 17356 and 22596 - 22716. Mode of transmission is Upper Sideband.

SATELLITE: To intercept satellite telecommo, you need a TVRO setup with a receiver that has a baseband output. One connects a shortwave receiver to this output, selects a transponder that has telecommo transmissions on it, and tune until the conversations come in. On the older trunks, one will also hear a 2600 HZ tone on the unused channels.

The mode used on this commo is known as SSB/FDM (Single Side Band/ Frequency Division Multiplexing). Table INT-1 shows some common satellites, locations and transponders which carry

108-110 MHz WIRELESS BUG



The design of the transmitter portion of this wireless bug is very similar to the 108-110 MHz TRANSMITTER described herein. See that section for optimizing the transmitter, antenna considerations, and increasing power, if desired. This circuit is very sensitive to the point of picking up whispers in a room. Q1 amplifies and buffers the output of the FET cap mike, while Q2 acts as a voltage-controlled oscillator to provide an FM output at 108-110MHz.

telecommo. Private Telecommo networks are also carried via SCPC (Single Channel Per Carrier) on satellites. SCPC is a way for companies to have multiple uplinks for their commo network, as opposed to one with the other methods. To receive SCPC, one needs a block downconverter which converts the 3.7 GHZ satellite frequencies down to something more easily handled. One then runs the output of the downconverter to a scanner to receive the signals in the 50 - 550 MHZ range. Such a down converter (BCD-60) is sold for about $400 by AVCOM, 500 Southlake Blvd, Richmond, VA 23236. TIP: When ordering, state that you want the 50 - 550 MHZ output option.

MICROWAVE: Much amateur radio and satellite TV equipment is modifiable for use in intercepting LOS (Line Of Sight) terrestrial microwave telecommo. There have been several cases of interference with TVRO receivers from LOS links. Most microwave telecommo is still sent out SSB/ FDM, altho the digital PCM/TDM (Pulse Code Modulation/Time Division Multiplexing) format is beginning to catch up. Besides modifying standard equipment, one must also get a fix on the LOS signal. One does this by searching the FCC records for a nearby town with a relay tower, and then determining the direction of transmission by observing the orientation of the microwave horns. PMC/TDM is a little more difficult than the standard S5B/FDM, but at this time the signals are not encrypted, so as long a one can receive the signal with a PCM receiver, there is no problem.

Table of Selected SSB/FDM Phone Systems

Satellite	Location	Transponders
Aurora (F-5)	143.0	3-5-7-11-17
Westar 4	99.0	14-24
Telstar 301	96.0	8
Galaxy 3	93.5	21-22
Westar 2	79.0	1-2-4-8
Comstar (all)	76.0	3 thru 8, 13 thru 17, 21-22
Galaxy 2	74.0	varies
Satcom 2R	72.0	3-4-7-8-9-11-12-13-17-19-21-22-23

Microwave Telecommo Frequencies (GHZ)
2.11 - 2.13, 2.16 - 2.18, 3.7 - 4.2 (also satellite), 5.925 - 6.425

Frequencies of Studio-to-Xmitter Link (GHZ)
1.99 - 2.11, 6.875 - 7.125, 12.95 - 13.2 CATV Studio Links: 12.7 - 12.95

WHO'S LISTENING

By: Ian A. Murphy, President & CEO Secure Data Systems Inc.

Over the years, there has been several studies and discoveries that would alter personal and electronic security over time. Devices able to "listen" to almost any form of commo have become commonplace and are available "over the counter" from a wide and varied number of sources. Such units range from $10 - $15 to expensive set-ups that use microwaves and lasers for the interception of almost any audio signal in the spectrum. But now with increased protection needed, several solutions have been implemented. More and more attention is now being directed on the electronic emanations endemic of today's commonly available electronic equipment.

Electronic phones, computers and commo networks, ATM's, radio and TV stations are just part of the overall electronic bubble that we have placed our society into with the hopes of providing better and faster methods to make daily life easier and more efficient. But with such a fragile structure as the electronic bubble, we have new opportunities to discover secrets never before possible. And to wreck havoc. As a general rule, the more you make something complex, the more vulnerable it is to attack and manipulation.

The same technologies that help us in one way or another are also those that help the people who wish to disrupt and destroy our way of life. Signal leakage, either by design or by accident, may lead to total collapse of protective measures due to "wide open spaces" in the protective sphere. We will discuss the possible problems that common office technology may bring in unsecuring your installation. For much more information (including specific plans), see many of our offers, including our BEYOND VAN ECK, COMPUTER PHREAKING and VOICE MAIL BOX HACKING manuals.

Our main focus will be in the areas concerned with the emanations or transmissions of "Tempest" frequencies (freqs). "Tempest," is the code name given to a specific area concerned with radio freqs radiated by computing equipment by the U.S. Dept. of Defense. This "concern" dates back to the late 1950's. The concern ranged from the possible interception of "*informational information*" by sources other than the intended users of such information.

The problem is more easily recognized by the current requirement of normal electronic equipment having to conform to emission standards dictated by the FCC in respect to the amount of electronic "noise" generated by common standard technology, so that such signals do not interfere with other such equipment or their operations because Tempest freqs are almost continuous from commercial AM stations to the upper reaches of 600 MHZ.

Tempest freqs, in the form of "Electro-Magnetic Interference" (EMI) noise, are generated or transmitted by all of your electrical and electronic systems. Your TV emanates certain freqs, and so does your stereo, phone (wireless or not), digital clock, microwave oven, computer - you name it! The Tempest freqs generated and their magnitudes are directly related to the type of equipment involved, its application and the amount of shielding used.

We will describe two possible examples of such "informational information" and the ability of some with directed intent to cause potentially fatal results due to the use of directed "noise". Note that the current specs for Tempest-approved systems are classified by DOD. These specs are not available to the author, and even if they were, could not be published without arrest. However, if one looked at the specs for normal computing equipment and reduced the allowed emission output by 80%-90%, that would be a realistic emission standard acceptable to DOD.

Example 1: "We had better 'Czech' this out!" In 1987, a strange incident occurred. Foreign nationals from an "Eastern Bloc" nation entered this country in a large camper-like truck via the border checkpoint at Niagra Falls, New York. The 4-5 "visitors" were here on tourist visas and were reported to be representatives of their country's vehicle industries here on a promotional tour to increase interest in their exportable products.

The problem with these "visitors" is that none of them had any connection with such industries in their home country. In fact, the visitors were far from what they supposively represented. The group description read like a Whos' Who of mid-level management of Eastern Bloc intelligence operations. The group reportedly consisted of a nuclear physicist, a specialist in aerial map-making (complete with a small ultra-light powered aircraft), a commo and computer expert, and two communist party officials (read KGB).

Over a 5 month period, the group was reported to have visited 17 states looking at 40-48 military and defense contractor sites. The vehicle and its occupants were followed by over 100 agents of the FBI, NSA, Secret Service and State Department and at least one over- flight of a military reservation was reported. Altho the overflown site was not identified, one site was. This site, was the sensitive Naval commo center for the Pacific Fleet located in San Diego.

It was reported that the truck and it's occupants were parked a few hundred yards from the facility for several days and according to law, were not in violation of any current statute at the time. The group was also in or near the 2,800 acre North Island Naval Air Station (Coronado, CA). The spokesman for the base stated that you could not see much of anything going on except for the take-off and landing of aircraft, which you could see from almost any place. Obviously, he missed the entire point.

Clearly, you don't have to be inside of a facility in either a physical or electronic (ex: using bugs) standpoint to collect highly classified data. You can legally park in any lot, street or campground close to your tar get and stick up your antennas - no property violations, no photo restrictions to comply with, no restrictions at all - you are legally parked with your "ears" on.

This method was clearly proved in an article published in 1985 in the prestigious security magazine, "COMPUTERS AND SECURITY", titled, *"Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?"*, by Wilm Van Eck. Van Eck is an engineer with the Neher Laboratories (Netherlands), on contract with NATO to seek out and test ways that Eastern Bloc agents could eaves drop on NATO facilities. In his paper, Van Eck stated that when they were conducting their experiments in the open on public roadways, with a van and antenna system that was quite noticeable, no one asked what they were doing or questioned the time they spent at it.

To continue with the story, at the end of the suspect journey, the truck and its crew were searched at the Nogales, AZ border checkpoint and were then released to go into Mexico! Nothing considered illegal was found in the search. Altho the truck was suspected of performing passive "eavesdropping" operations, the Federal Government had no legal right to hold either the truck or crew. And the probably intercepted information was then released from the country.

It should be noted that the truck could have had a number of standard "off-the-shelf" items, consisting of two general coverage radios with a combined tuning range between 100 KHZ and 2 GHZ, an IBM-PC or compatible, various cheap video and signal enhancement equipment, printers and modems and other such complementary devices.

None of the equipment need be any "James Bond" type of gear. The basic suspected gear could have cost the operation less than $10,000 (if budgeted correctly). Other off-the-shelf type radios, like the $200 unit available from Radio Shack that covers 150 KHZ - 30 MHZ, is also possible. Since most emanated signals generated by logical devices are within the AM and FM bands, the use of a standard car radio antenna would suffice to use as a pickup for most of them. Even so, it is not uncommon today to see ordinary passenger vehicles bristling with sophisticated antennas.

Of major concern is the fact that relatively simple equipment can detect, record and decipher such emanations with relative ease. The modest capabilities required to penetrate the electronic fog of our society should be a clear warning to those concerned with security.

__Example 2__: "Breaker, Breaker, Wally Gator!" During the 1970's, the United States had a short-term love affair with the Citizens Band (CB) radio. What were once clean channels were suddenly crammed with persons who wanted to communicate with any number of persons for any number of reasons (mostly frivolous and illegal). Suddenly, millions of people had CBs in their cars, homes and- or businesses. And many didn't even bother to obtain a license, and many used illegal high-powered linear amps.

A simple brief explanation of the CB phenomenon is:

(a) CBs legally communicate in the upper end of the 11-meter band (26-27 MHZ).

(b) CBs are legally allowed to operate with a maximum output of 5 watts radiated power. Of course, this limited power was not sufficient for some users, and thus the use of linear amps or "heat" was common place. Stations were known to feed 50-2,000 watts to their antennas, which in turn would increase such signals to a power of over 2,000,000 watts of radiated energy!

Some operators demonstrated the intense power outputs by lighting unconnected fluorescent bulbs manually held at some distance from their hi-powered antennas. Some users had virtually full control of channels in their respective areas and would blank out anyone who would not conform to their rules or procedures. Some outfits were so sloppily tuned that the entire CB band was swamped by their signal. And some set up pirate stations that broadcast music, commercials, news, weather and sports. All such actions tied up freqs and caused a general crackdown by the FCC in the later years of the fad.

But even today, the problem still continues and the FCC has all but given up on the idea of any enforcement of regulations concerning such operations on the 11 meter or 27 MHZ band. Largely because of such abuses, the CB craze faded by the late 1970's, and was back in the hands of those who would truly use such radios - mostly truckers and those who do a lot of driving. They are concerned with time and travel conditions as most of us are, and especially about police radar. The truckers always have some "heat" on-board for those times when they could not get their signal "out." It was and still is considered an insurance policy by most who have this technology, and is still in widespread use. Now, truckers are switching to amateur band radios in the 10-meter band, and are conversing as before. Since the 10-meter band permits much increased power output, the switch to 10-meters was inevitable. It is now reported that some truckers are using and abusing this band also and there is little that can be done to stop the abuses.

Part of the problems is due to the fact that many 10-meter (amateur radio) radios can be modified to switch to the 11-meter (CB) band with only minor modifications. And freq hopping is as easy as tuning in the average car radio. Another interesting aspect of 10-meter radios modified to the 11-meter band is their use of their built-in 10-meter output amps. Substantial 10-meter EMI is generated by the amps due to the lack of RF chokes and filters because the unit is designed for the 10-meter band, not the 11-meter band.

Enter the frequent traveller with a late model vehicle. Most vehicles today have some form of sophisticated electronic control (ie: micro computer) under the hood. This "brain" controls most of the common but critical starting and running operations (ex: carburetion, distribution), and some also control steering, braking, suspension, etc. And it receives its data from external sensors that are not completely shielded and that can pick-up stray EMI and relay it back to the computer to result in a malfunction(s) or even a total, permanent failure.

Clearly, the deliberate interference of such operations is a real possibility. This interference would make the vehicle much more likely to seize-up and-or crash, and the driver and passengers much more vulnerable to both fraud and physical attack. And there would be no evidence that would prove that the vehicle malfunctioned because of an electromagnetic attack, so the criminal or terrorist could operate for years without problem.

Many incidents have resulted in fatalities. Altho the causes of such incidents were certainly not all due to an "Alligator" radio, they were all caused by the same type of high-powered radio emissions.

In one such set of incidences, a certain helicopter was involved. The helicopter, known as the UH-60 Blackhawk to the Army or the Sea hawk to the Navy, is operational state-of-the-art in low-level air combat situations, and is highly electronic in its design and operation. The problem was twofold in nature, and both factors contributed to the discovery of the cause:

(A) The first factor resulted from the design specification of a unique horizontal stabilizer with the intent to improve its fly-ability. This stabilizer was controlled thru a series of electronically-activated hydraulic systems, controlled by an on-board microcomputer, that in turn was controlled from the cockpit thru a series of other logical and electronic relay systems. There was no mechanical connection between the craft's flight controls and the pilot of the craft. That is, the fly-by-wire method was replaced by a set of relays and hydraulic attenuators, instead of the old reliable cables and pulleys. Altho the cabled method was certainly not as smooth or responsive as the electronic controls and required greater artistic ability to fly the craft, it would take an explosive charge to bring the craft to a dead stick. And cabled controls can often be fixed with a pair of wire cutters and clamps by any mechanic, and not virtually impossible to repair in the field as is the electronic system.

(B) The second cause, more unknown and deadly, consisted of EMI emanating from a number of different sources. One such source was CB radios using illegally high-powered outputs. Another incident of the same type was discovered when one of the helicopters flew too close to a commercial radio station's transmission towers. Both times, the craft suddenly lost control, and the flight ended in fatalities for the crews. It was discovered that strong radio signals were the causes. According to published reports, 5 UH-60 Blackhawks have suddenly nose-dived into the ground killing 22 servicemen since 1982! And the Army instructed its pilots that flights near microwave antennas or shipboard radar may cause "uncommanded" altitude changes. In other words, the helicopter does a nosedive and crashes.

Unfortunately, this basic problem was not adequately considered by systems management in the now fully electronic battlefield. Consequently, these helicopters are believed to be not only worthless and dangerous for modern battlefield conditions, but vulnerable to any enemy or prankster who has a high-powered transmitter in his hand and knows enough to simply turn on a switch. For example, consider how these helicopters would have fared in Viet Nam once the enemy became aware of their EMI vulnerabilities.

Since these reports are now common knowledge, then what is to stop the use of high-powered transmitters from becoming a major new invisible tactic of war, terrorism and criminality that can not only disrupt commo but can actually disable and destroy equipment?

These examples reveal the serious types of damage that are possible. The second part of this problem is with the protection of such circuitry. Great amounts of equipment protection is in the form of deep trenches, grounding and shielding of buildings and equipment from the standard to the exotic methods, cable and support runways and concrete encasements - in other words, a steel bunker. From a military viewpoint where money is no object, you can spend enough to obtain satisfactory protection. But where money is not unlimited, the use of such protective measures is not reasonably possible even for the wealthiest corporations - not to mention families and individuals.

Not only can satellite and TV stations be jammed, $6 million helicopters wrecked and vehicles disabled because of EMI attacks, it is also possible to intercept vast amounts of data using similar technology! And unlike the destructive methods, the surveillance methods can be done quietly, over long periods of time, and without anyone becoming any wiser as to the quantity and quality of data intercepted.

Such interceptions are now commonplace with horrific results. For example, take a standard "Walkman" type radio and visit your nearest ATM (Automatic Teller Machines) or POS terminal (see our eye-popping AUTOMATIC TELLER MACHINES manuals!). Now carefully tune thru the FM band. At some spot(s), you should be able to "hear" ATM functions occurring. The noise produced by the radio at first sounds like ordinary "static", but if you listen carefully, you can observe how the sound changes as the ATM user steps thru the operation of the ATM. Using simple electronics, you may be able to receive and reconstruct such impulses into a readable format. This test can also be done near any piece of microprocessor-controlled equipment.

Interception & Weapons Uses: Think about what this really means in terms of data security. Commo may be encrypted, data may be stored under hardware or software lock and key, data may only be accessible to those with the need to know and in possession of the correct passwords - all to no avail if the computer monitor or Video Display Terminal (Unit) (VDT/VDU) leaks the displayed signal and the eavesdropper is able to receive, record and process it! When the authorized user reviews the data on the monitor, it must be in a plaintext form and that is precisely how it will be emanated to the eavesdropper. Potentially, no other method - short of actually sitting in the user's chair or obtaining a plaintext printout or disk file - is as effective, effortless and safe for obtaining highly classified data than by using the Van Eck method!

The Re-Process Sync Amplifier and Van Eck device are similar, primarily with the exceptions that the Van Eck device is designed specifically for surveillance purposes, is designed for European voltages, and has a built-in digital freq meter.

The Britton box, in general, is designed to restore and regenerate the sync and colorburst signals and ignores all information appearing during either the vertical or horizontal blanking. Its basic function is to supply artificial external signals for the low-freq sync signals that are poorly transmitted from the source. The reconstructed signals are inputted directly to any video monitor thru a simple $50 modification of the TV or video monitor. Without this modification, the received signal has a very weak sync at best (usually none), and thus appears as a scrambled signal.

The two most popular TV/computer monitors used today is the composite (analog) monitor and the digital monitor. The composite monitor is commonly used in color TV sets and RGB computer color monitors. The digital monitor uses TTL logic to control the screen and its pattern. The composite monitor construction of the picture is performed by a beam of electrons that are scanned across the screen at a rate of 525 lines per second. Since the majority of screens are of a composite nature (this is even true in most IBM environments), the ability to receive the signal is very possible from a radio emission standpoint.

The reception of such signals is not movie fantasy, but easily accomplished using relatively simple electronics. The first part of the reception project is to have a method of signal acquisition and amplification. Signal acquisition may be performed by the use of standard electronic equipment and parts (retail or from the advertisers of Radio Electronics, Modern Electronics, etc.). A base station is usually out of the question due to the weak signals normally available (unless you happen to live near your target). To get close enough to the source, a mobile unit is almost always required.

Antenna, amplifier, sync processor and TV/monitor must be powered in the mobile unit. Usually, power is taken from the vehicle battery and converted into 120 VAC using a standard inverter. Depending upon your budget and Basic Equipment List (BEL) requirements, a fully battery-operated set-up can be constructed for under $500 (much less if you can get the parts used).

Our two systems described herein will be different only in basic construction and BELs:

THE "RADIO SHACK" READER

(1) The antenna could consist of a Radio Shack TV/FM RS15-1611 for about $50.

(2) If needed, Radio Shack in-line signal amplifier (10 db gain) RS15- 1117 for about $16.

(3) The Radio Shack RF Video Modulator RS15-1273 for about $27.

(4) The Don Britton or Van Eck unit (total parts cost about $200).

(5) The tuning unit may consist of different commonly available FM/ TV/UHF tuners designed for the tuning of TV Sound & Picture reception and possible recording. Costs for such units range from about $120 to about $320. The $320 unit can operate on AC/DC, has audio/ video input jacks and can operate on 9 "D" batteries. Other possible usable units could be either the RS16-109 or the RS16-111. The units cost about $220 and about $160 each, respectively. Both are able to tune in the full commercial AM/FM and VHF/UHF TV signals. The low end of the cost spectrum would be the RS16-113 for about $120. This unit also has the same spectrum tuning abilities.

THE GOLD PLATED UNIT

(1) The antenna could consist of a Radio Shack TV/FM RS15-1611 for about $50 (or other electronics having built-in antennas). But because amplified signals must be inputted to the receiver, the RS amplified antennas are still good choices. Altho it is also possible to use any number of amateur radio antennas for the purpose of maintaining a low profile, we will use one of the standard active receiving antennas that has a reception spectrum from 50 MHZ - 1 GHZ. These units are avail able from mail order supply houses.

(2) If still needed, Radio Shack in-line signal amplifier (10 db gain) RS15-1273 is about $16. It is also possible to use the RS15-1105 Indoor FM Signal Booster with switchable 0/10 or 20 Db gain for about $25.

(3) Radio Shack RF Video Modulator RS15-1273 for about $27.

(4) The Don Britton or Van Eck unit (total parts cost about $200).

(5) The tuning units would consist of two separate radio units. The units, both ICOMs, have a combined tuning range of 100 KHZ - 2 GHZ:

(a) UNIT 1 (R-71a) tunes from 100 KHZ - 30 MHZ. This unit is nothing more than a shortwave receiver with excellent signal reception and freq stability that offers far better overall signal interception quality. The unit offers 1 Hz tuning and has a digital freq readout. As an option, this unit may be controlled by an IBM-PC or compatible. Cost for this unit is about $950.

(b) UNIT 2 (R7000) covers 30 MHZ - 2 GHZ. This unit is a general coverage receiver with excellent signal reception and freq stability that offers far better overall signal tuning and interception quality. Also, this unit can be computer-controlled thru an IBM-PC or compatible. The unit offers 0.01 HZ tuning and has a digital freq readout. Additional abilities of the unit include signal output, and an IF output of 10.7 MHZ with other freqs available. The cost is about $1100 each.

This particular unit also has an option for the output of the video signal and connection of any standard video monitor for about $130. For about an additional $160, this unit can have the ability to receive signals from 20 KHZ and go all the way to the specified 2 GHZ. The required unit is the Kuranishi FC-7000 freq converter. With additional commercial TV MDS tuning equipment, ranges can exceed 2.7 GHZ. Costs for this ranges between about $80 and $109. Since we will be mostly dealing in the lower ranges of freqs, an added piece of gear may be used to gain the best signal reception points available. This is thru the use of a Radio Direction Finder, available from American Electronics, for about $100.

Such interception capabilities are possible and have occurred without the interceptee knowing until the FCC contacted the source of the emitted signals usually thru somebody else's complaints.

For example, emanations from some PCs and their respective monitors have been picked up on the TV screens of their neighbors by only using the TV's standard rough and fine tuning controls. The reason is due to the fact that TVs have the ability to automatically adjust the received sync signals to those close to the freq of an intercepted computer monitor's sync freq. This "ability" is due to the design of the standard tuners for black & white receivers with a normal directional antenna and a standard antenna amp. All three devices are an integral part of the standard b/w TV set-ups. You have such devices if you have an antenna on your roof or attached to your set as many have built-in signal amps to help boost weak signals in a noisy electrical environment.

Simply, the guy next door may be able to read your computer monitor without you even being aware of it! Consider the number of computer terminals in a standard corporate environment, the value of the information they process, and the ease at which these signals can be eaves dropped upon.

Business computer monitors display business plans, formulas and patent-trade information, client lists, contractual information, personnel information, access codes, passwords, PINs (banks) and other types of information that can be so valuable that the survival of the firm itself is at stake if it falls into unauthorized hands - not to mention the safety of its personnel and clients. And since that information will be routinely called up during normal work activities, by remotely electronically surveilling a firm, you have a completely free reign to monitor daily transactions with little possibility of ever being discovered.

"RADIO SHACK REALITY"

By: Thomas "ICM" Icom

BUGS & WIRELESS MICs: There is much equipment which can be used as improvised bugs avail able from RS. Starting on the low end, there's the RS33-1076 Wireless FM Tie-Clip Mike for about $20. This is a nice throwaway unit that you don't have to worry about losing if it's discovered, unlike the more expensive equipment. The range on it is 250 feet operating in the FM broadcast band. The unit could also probably get a better range and battery like those with some mods.

For those willing to spend a bit more, there are the 2-piece wireless systems RS32-1221 and RS32-1226 for about $70 each. These units operate on the 49 MHZ no-license band, and over a range of 200 feet. They also have their own separate receiver. The 49 MHZ band is substantially more private than FM, and these units could also be modified for better range by adding a more resonant antenna.

For those needing more esoteric devices, RS sells their RS32-2050 and RS32-2051 infrared wireless systems, which are hooked-up to a TV or stereo. Hooked-up to a mike and audio amp, these could serve as a very secure bugging system. The claimed range is 20 feet, but I feel that's a little on the conservative side. When set up outdoors at night, one could expect better range. The prices are about $60 for the RS2050, and about $90 for the RS2051, which is a stereo version. One could use the stereo version to receive sound from two different locations as well. Similar equipment is also available from discount department stores.

HARDWIRED SETUPS: Radio Shack has some equipment which is readily adaptable for hard wiring. For starters, there is the RS33-1052 miniature omnidirectional mike. Only 3/4" long, it can be easily hidden. It costs about $20. Even better and cheaper is their RS270-092 mike element for about $3! For small, hard-to-detect wire, RS also sells 30-gauge magnet wire, which serves for a short run in a minimally-inductive noise environment. 200 feet is only about $5.

Department, hardware, auto and electronic parts stores also sell "liquid weld," or "metal cement." The best of these is J.B. Weld (nonconductive). Some of these mixtures are conductive, and can be painted onto a surface to act as invisible wires (this type is available from electronic stores and are used to repair PC boards). When done properly, this is as close to undetectable as you can get.

For an amp at the other end, Radio Shack sells an assortment of OpAmps and Audio Amp ICs ranging in price from about 80 cents to $6 each. These units come with specs and circuit examples so even a beginner in electronics could make a serviceable amp out of them. Common stereo amps available from anywhere can also be bought, and used as field expedient equipment.

COMMUNICATIONS: Radio Shack sells various pieces of equipment which work very well for tactical commo. I've personally had good luck with their series of 49 MHZ hands-free walkie talkies. Their claimed range is 1/4 mile, but I've gotten a 1/2 mile range on a common basis in mountainous terrain, and up to 1 mile occasionally. Also, they have different units to meet various needs. Their "top-of-the-line" unit is their RS21-404, which sells for about $90 a pair.

These units use what they call an "audionic design", which picks up your voice via your ear canal, similiar to military equipment which came out in the 1940's. They also have standard units with the headset (RS21-400) for about $70 a pair, and their standard 5-channel headset model sells for about $50 each. There are also handheld walkie-talkie versions with 1- and 5-channel capacity. The 1-channel unit is their RS21-401, which is about $25 each, and their 5-channel handheld unit is the RS21-402, and retails for about $40 each.

All these units perform fairly well, and the price is about the same as mailorder. The 49 MHZ hands-free units are also available from other discount retail stores, at a cost probably less than that of Radio Shack, altho they might not have some of the more specialized units that Radio Shack has. Also, for quick and dirty field expedient commo, CBs are readily and inexpensively available from many sources.

TELECOMMUNICATIONS: All of the Radio Shack wireless mikes can easily be converted to phone bugs by replacing the mike with the circuit in the surveillance section. Radio Shack also sells a recording control RS43-228 for about $20, which starts a tape recorder when the receiver is lifted. While it works OK, it is easily detected and destroyed. You'd do better with one of their VOX recorders and the conversion circuit.

Radio Shack also sells a DNR ("Dialed Number Recorder"), which records the numbers a person dials on his line. Radio Shack calls it a "phone accounting system", RS43-152, and it's about $99 - the cheapest price you'll find for a DNR.

TAPE RECORDERS: The Radio Shack units that stand out for surveillance work are their VOX-operated ones. They have 3 different models. Their standard model is the RS14-800, for about $60. The second unit is the RS14-1057, for about $50, and their miniature model, the RS14-1055, for about $40. For those into microcassettes, they sell the RS14-1042 for about $50. All of these units perform well for their price range. Excellent tape recorders are also available from other makers as well, for example, there are quality units from Panasonic or GE.

SECURITY: Radio Shack sells a complete line of security accessories, including alarm system parts and some "consumerized" security products. The stuff works! Discount department stores also sell "consumerized" security items such as timer/light-activated switches, plug-in motion detectors, etc. Depending upon your situation, this stuff might be usable off-the-shelf, and can be modified to serve your particular needs.

MODIFICATIONS: An expedient method to procure equipment for your particular needs is to see what's available that approximates what you need, and then modify it to serve your purposes. Much of the "consumerized" stuff and its more specialized cousins have common basic functions. Their primary differences often lie in things like size, power requirements and the amount of "gold-plating". To modify equipment, of course, takes some technical skills, and it always helps to have a schematic (which are often difficult if not impossible to obtain).

With the described equipment, one can get a workable setup at a somewhat reasonable price. Granted, the stuff isn't the cheapest or best performing, but it works, and it's readily available.

ELECTRONIC WARFARE

Electronic warfare plays an important part in military operations to day because of the integration of high-tech in the battlefield. The definition of Electronic warfare is, *"Military action involving the use of electronic equipment to gain in intelligence - to exploit, reduce, or prevent an enemy's use of electronic equipment while taking action to ensure use of electronic equipment by friendly forces."*

While this may seem a tall order, the nuts-and-bolts of it are pretty simple, and easy to accomplish by any one with moderate knowledge in commo electronics - such as a ham radio operator. The definition above covers three basic tasks: Signals Intelligence (SIGINT), Electronic Countermeasures/Jamming (ECM), and Electronic Counter-Countermeasures/Anti-Jamming (ECCM). For about $500 (new retail value) one can assemble a complete, effective EW setup. For about $2500 one can assemble a top-of-the-line EW station. The equipment can also serve as part of your regular commo station, and should be considered part of it.

EW is an integral part of guerilla warfare resistance operations. By using SIGINT to gain information on enemy activities and order of battle, and by denying an enemy the use of his radio commo facilities, one can gain the added edge for successful operations. ECCM know ledge is also very useful, thus allowing you use of your commo capability should an enemy attempt to deny you use of the airwaves. When the proper techniques are used, EW can act as a psychological warfare device, demoralizing the enemy, and further contributing to his defeat.

In the U.S. Military, EW information and techniques are considered a subset of military intelligence have a Top Secret (highest known) security clearance - which should act as an indicator of the importance they assign to it. However, the techniques are simple in theory and applications, and are presented here in a scale most suitable for resistance activities, and put into easily understandable form.

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

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

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

1. Cover as wide a bandwidth, and as many signal modes as possible.
2. Search capability for finding unknown frequencies.
3. Continuous scanning of 100 to 400 frequencies in order to cover all known enemy commo.
4. Priority coverage of 5 to 20 "main" frequencies.
5. Tape recording of activity.
6. Decoding of known scrambling modes in order to provide understandable commo.

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

Once one has the basic set-up, certain accessories can be bought which increase the effectiveness of one's listening post. Audio and RF Filters are inexpensive to buy/easy to build, and can help clarify signal reception.

RF spectrum analyzers make finding commo signals easier by providing a "picture" of RF activity in your area. As quality spectrum analyzers are expensive, it is nice to know that you can accomplish much of the same capabilities with a $199 probe, called the Spectrum Probe (works with most oscilloscopes). Oscilloscopes make analyzing non-voice audio commo easier - along with frequency counters - which can also aid in determining operating RF frequencies of enemy commo during field investigations.

Finally, there is the computer. A good system will help you in, among other things, unattended operation of your listening post, logging of your commo intercepts, analyzing them, and in assisting in cryptanalysis of encrypted commo. Fortunately, for the budding signal intelligence interceptor/analyst, there is a wide variety of equipment avail able to serve myriad of operational situations. While by no means exhaustive, this list will hopefully act as a starting point to assist you in finding your optimum equipment set-up for your needs.

RECEIVERS

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

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

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

The Kenwood R-2000 and Yaesu FRG-8800 are less fancy than their higher-priced models, but are still have the same features as them, just a little less sophisticated. These two mid-level units offer the best value for someone de siring to have a fairly sophisticated shortwave listening setup, offering the best compromise between price and performance.

If one can get a multiband portable with SW and VHF/UHF coverage in decent condition at such a price, then it would make a worthwhile addition to one's listening post as an expendable back up unit, "fast-search" unit, or single-channel monitor. The tuning-dial function enables one to get a quick-fix on nearby enemy troops who are using commo equipment without having to do a mad rush programming in scanner search limits.

One can use it to listen to, say the local police/military tactical/ surveillance channel, your group's operations, or any other priority-type frequency which constant monitoring is needed. This can be done without tying up other equipment, particularly if you don't want to miss anything on your special frequency when your scanner is cycling thru it's other channels. Or to listen to a continuously active channel (ex: some ham repeaters, broadcasters on AM, FM, and/or shortwave, surveillance equipment (bug) frequencies, NOAA weather broadcasts, or TV/radio station studio-to-transmitter links), which would lock-up your scanner, and make you miss the stuff on the other channels.

VHF/UHF "Scanner" Receivers: The mainstay of your listening post will consist of VHF/UHF receiving equipment, as most of your listening activity will be centered there. Just like shortwave equipment, there are several price levels of VHF/ UHF scanners which offer different performance levels, features, and purposes. There are so many different specific makes out in the market, so I will only cover some of the more noteworthy types. The major brands are Radio Shack, Regency, Uniden/Bearcat, Cobra, and AOR. The ham manufacturers Icom and Yaesu also make notable VHF/ UHF commo receivers as well, altho they cannot really be considered "scanners" per-se. Starting at the top is the Icom R7000 @ $1000 featuring 25 KHZ to 2 GHZ all mode coverage (USB, LSB, FM, AM), 99 memories, optional shortwave coverage, audio noise blanker, infrared remote control, and optional computer control and voice synthesizer. While a top-line per former, particularly with the computer control option installed (more on that later), there are several lesser-priced models which will do the same thing. However, if you can afford an R7000, go for it.

A spectrum analyzer is a oscilloscope-like device which enables one to get a video representation of a section of the RF spectrum. It is very effective in countersurveillance operations, and in frequency hunting.

POWER

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

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

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

COMPUTERS

While not necessary, a dedicated computer for your commo set-up is a handy thing to have, and a necessity if you want to get into digital commo interception. You can use the computer for logging your intercepts an frequency information, as well as in assisting you in decoding encrypted digital commo.

You'll want as powerful and fast a machine as possible for any cryptanalysis you might be doing. CONSUMERTRONICS sells CRYPTANALYSIS TECHNIQUES, which includes software for IBM PC/compatible systems (this includes 386 machines). Also, read the CRYPTOGRAPHY chapter herein.

ANTENNAS

There are various antennas out there. What is currently the rage in VHF/UHF receiving antennas is the discone. This omnidirectional antenna, conical in appearance, presents a good match over the entire frequency range from 25-2000 MHZ, which is good enough to transmit over this range. They cost about $70. For the budget-minded person, and those seeking something more directional, one can pick up a TV yagi (beam) antenna at reasonable prices from Radio Shack, or any department store. They work well enough as is, but can also be modified for better reception. A figure herein shows the dimensions for converting your basic VHF/UHF TV antenna into a VHF/UHF scanner antenna. When doing this modification, one should also remount the antenna so that it is vertical (just like the picture), as opposed to horizontal.

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

Receiving antennas on shortwave are a different manner. With these, the best way to go is to make your own, as it really is too easy. For starters, get as long a length of wire (200'-300' is nice, but even 100' will do), and get it up as high as possible. Then add a good receiving tuner. Several manufacturers sell an antenna similar to this, usually a dipole with some traps. These work alright too, but the longwire is still your best bet as it works, and costs much less.

One can also use commercially available ham shortwave antennas for the approximate band that most of their monitoring would be on. For those with very limited space there is also what is known as an "active antenna" which is a small (3'-5') whip antenna with an amplifier. I've heard a few ok reports about this, and in my opinion it's better than nothing if you have very limited space, altho I would try as big of a longwire antenna as you can. With a long-wire, one can also run it inside along the ceiling molding, and still get a good length if one lives in an apartment, or similar situation.

SIGNAL TYPES/MODES

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

Voice:

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

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

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

Non-Voice:

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

RTTY - Radio Teletype: Generic Term for digital radio commo. Sounds like warbling or alternating tones. There are various types. NOTE: The mark/space frequencies shown here are only the most common. Actually, they can be easily changed by their users.

Baudot: 5 bit code used mostly on shortwave. Common speeds are 45.45, 56.92, and 74.20 baud with mark/pace frequencies of 2125/ 2295, and 1275/1445 HZ.

ASCII - American Standard Code for Information Interchange: The common computer language. Again used mostly on shortwave. Speeds run from 110-300 and 1200 baud. Mark/Space frequencies are 2125/2550, 1275/1700, and 1270/1070 HZ for 110-300 baud, and 1200/ 2200 HZ for 1200 baud.

FAX: Used for transmitting pictures. Various speeds and audio frequencies used by weather services and government.

AMTOR/STIOR: Error-Checking form of ASCII. Used mostly by hams, and ships. Has a unique chirping sound to it.

AX.25 Packet: Error free digital commo. Used mostly on VHF, UHF, and Microwave at speeds from 1200 baud to 19.2 kilobaud. AX.25 is the amateur radio version of the x.25 protocol, used by telenet, and other computer networks. However, it can just a easily be used by other entities if the need arose. The amateur network is also used for emergency disaster services, and a similar network an be set up for resistance coordination operations over a wide area.

PCM - Pulse Code Modulation (Digitized Voice): At this time difficult to receive, as there are no inexpensive PCM receivers avail able. PCM allows both "voice" and real data to coexist on the same channel. PCM commo is also a lot easier to make secure, as the digitized voice can be easily encrypted (see DVP). PCM usually sounds like a distorted tone - much like a 1200+ baud phone-line modem, altho some military units sound like any other low-speed RTTY signal. PCM is starting to be heavily used by the military.

Pagers: One way commo used to indicate the receiver to a certain condition, and often to transmit a limited amount of data. Used mostly by businesses. Sounds like a tone burst, often followed by a quick RTTY data burst.

Remote Control: This can be anything: Audio tone burst series, unmodulated signal on a certain frequency, digital signal, voice recognition, etc. Often very useful to intercept and analyze, as duplication of such a signal can cause, as a friend of mine once said, "major funky-ness". Good human-intelligence operations, and threat knowledge often help here more as R/C systems are often proprietary.

PL Tones:

Most VHF/UHF business and police commo make use of subaudible tones, also known as PL tones, channel guard, quiet channel, and a couple other names. This enables different entities to share the same frequency with interfering with each other. PL works by generating a low volume audio tone along with the transmission. The receiver has a tone detector hooked into the squelch. When it hears the particular PL tone, it opens the squelch, and allows you to hear the transmission, if the proper tone isn't present, then the receiver ignores the transmission. There are other variations of this, such as a tone burst sent at the beginning of a transmission that opens up the receiver's squelch, as opposed to a continuous subaudible tone.

To determine a PL tone, hook up a frequency counter to the audio out put of your receiver, and make a reading when there is no voice on the transmission (ie: when they first key up). The reading on the counter is the PL tone frequency.

SCRAMBLED COMMO MODES

Most security conscious radio users will use some form of scrambling to protect their commo. The biggest user so far has been the U.S. Government and Military who are using some form of DVP. Coming in a close second are satellite broadcasters with the video version of DVP - Videocipher. Most other users, including police departments, simply use a good voice code, or a non-radio commo medium - which is more secure, and less expensive.

In general user practice, radio scrambling generally falls into two types, extremely secure and pathetic. Users usually either get some thing really cheap and simple for their piece of mind just to say they did something, or they go all out, and buy what the salesman tells them really works - and also happens to be ultra-expensive. On the extremely secure end are the ones which digitize voice and then encode the digital signal with DES, or similar. On the pathetic end are the ones which alter the frequency spectrum of the human voice. There are also systems which lie in the middle, but they are rarely used.

The easiest scrambling mode to decode are the various speech inversion and band-shifting modes. These sound like Donald Duck with a bad old, or an improperly tuned SSB signal. With these the speech is either inverted, or it's bandwidth is shifted up or down. A speech-inverter circuit, and a couple of good audio filters will do the job with some experimentation.

In the middle are systems which take the voice transmission, chop it into very short segments, and then rearrange them in a pseudo-random manner. These sound like some sort of intelligible language. The most secure is DVP, or digital voice protection with this one, the voice is digitized, ala PCM, and then the digital signal is encrypted with DES. On the radio, DVP will sound like a tone burst, followed by a howling static-like data burst. Yes, DES is breakable, but not by the common man yet. Your best bet is to simply somehow acquire an enemy's scrambler unit.

ECCM: PROTECTING YOUR RADIO COMMUNICATIONS

Ok, a little about ECCM, or ELECTRONIC COUNTER-COUNTER MEASURES. I assume you don't want to spend lots of money on a DVP setup, and want something which won't become obsolete in 10 years when anti-DVP gear is finally sold at a reasonable price. Quite simply, I'd use the minimum amount of power needed to successfully communicate with the other station, and use a good code, or some arcane language. That's all there is to it. Don't worry about them hearing you, or spending lots of money on a scrambling system that may not work.

Simply ensure that they won't be able to make sense of what your saying. Change your codes on a regular, random basis, and if you really want to be nasty, use a little deception, and make your codes sound like normal conversation, and make the meanings the opposite of what you're saying. If you're in the eastern part of town, say you're on the western part. Use complete nonsense phrases to convey information, and change their meanings to the exact opposite after a short while. By doing this, you can keep enemy SIGINT teams guessing while to go about your business unhindered. When it comes to commo security, there are no rules, and there shouldn't be any preconceived notions. For more ideas, see the Cryptography chapter, and have fun.

To protect your network from being jammed, change frequencies on a regular basis, use directional antennas, and again use the minimum power needed to communicate. This will do a good job at keeping them from hearing you in the first place, which is half of ECCM. It might also help to design your code system so you don't sound like a resistance operations network - which might cause the enemy to ignore you, and continue to look for the "resistance." Of course the best, and easiest way is to simply use alternate means of commo.

JAMMING

One you have determined the characteristics of the enemy's commo system, you can begin your jamming attempts. One must exercise extreme caution when doing this, as it will provoke a major reaction from your target, and should you get caught, the penalties would be severe. It would be preferable to have a mobile, or remote-controlled setup for your jamming operations in order to reduce the risk of getting caught.

Jamming Methods:

Wideband - Wideband jamming is basically a noise blanket over a wide spectrum range. It is one of the oldest, and easiest methods to accomplish. However, it will also jam other non-enemy commo, including your own. Wideband jamming is best used as an expedient in someplace where 90% of the commo will be the enemy's, and where you will have a non-radio mode of commo to use.

Narrowband - Jamming activity restricted to a certain frequency, or frequencies. Narrowband jamming is considered a more refined way of doing it. Various types of narrowband jamming:

Noise - Your basic pink noise, just like static on an unused frequency. If deployed, the target will most likely attribute it to RF conditions, or equipment problems. While effective to a point, some other techniques do better.

Harassment- Basically getting on their frequency, and uttering a few selective words or insults. This works, and is a good psychological warfare technique, as imaginative comment on a target's frequency will demoralize him, and generally piss him off. The bad part is that if you piss off a police agency, or the military, they'll come after you. This type of jamming is also pretty obvious, and could cause the target to step up his ECCM capability, thus making it harder for you to jam him.

Deception - One of the more effective, and difficult means of jamming. Basically this is getting on their network, and acting like you belong there, calling in false reports, making false dispatches, etc. Very subtle, and more effective than the previous two. Once discovered, it also causes the target elements to think twice when receiving instructions over the radio, thus incurring delays in responding to an incident.

Feedback - Like deception, except you record actual commo, and play them back over the frequency later. Easier to accomplish than ordinary deception, and just as effective. A major mind-game.

Repeater Feedback - The fine art of playing cross link, by hooking up your receiver to your jamming transmitter, and sending another entities commo over the target's radio network. Very subtle, and confusing and often attributed to faulty equipment. **Substitution** - Used in broadcast jamming. This is where you simply override a broadcast signal with your own ala "Captain Midnite" and "Max Headroom." Great for getting your message across in a big way. A variation of this technique used for revenge purposes i to do a small-sale broadcast override on a target business's broadcast receiver, sending a nice message to their customers about their business's policies.

JAMMING EQUIPMENT TECHNIQUES:

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

Taking out a broadcast station is a more difficult prospect, unless you have one of your own that has a similar power output to your target. Broadcast jamming is mostly a psychological warfare trick - to confuse and demoralize any unknowing civilians who might be listening to your target. If your object is to "take it to the streets," and sent your views over the airwaves, then your best bet is to transmit on a clear frequency so your signal will get out better, than to add the difficulty of coming on top of a megawatt transmitter with enough signal so that not only an you override them, but also have enough signal left to send something readable over.

However, there are a few instances in which a Captain Midnite routine can be used. The first and most obvious is with satellites. Now, "every one" says that he was caught, but for the first time in history when someone overrode an uplink, it was played down very quickly. Corporations have had a history of suppressing things before, and right after the man was supposedly caught, we didn't hear a word edgewise about it - which is strange as most corps. would want to see him publicly castrated. This leads me to believe that his capture was faked.

STL links are pretty well defined, and by getting close enough to the receiving end of an STL, one can use minimal power and send out a nice strong signal. Some STLs are run over the phone network, in which case no transmitting equipment isn't needed. Finally, one can jump right on the actual broadcast frequency, and at least override every thing in a small area. With average equipment, depending on target signal strength and terrain, one can expect a maximum range of 100 yards to one mile.

This is perfect for getting even with your neighbors by doing such things as jamming the Super-Bowl by rebroadcasting MTV on top of it, or playing porno films over the kiddie channel so little Johnny and Susie can get a real education instead of being brainwashed by PBS! Besides the classic signal override, one can also simply jam the signal, in which case the equipment is less sophisticated as no intelligence is being conveyed over the signal, and less power is needed, as you're just conflicting with the target signal, not overriding it.

LASER SIGHT SYSTEMS: Everyone has seen the laser sight systems out in the market. To get one for less than 50% of the commercial product, pick up a laser at an electronics surplus dealer and use that. It may be a bit bigger, but it works. Another idea is to use the laser out of a CD player, which is nice and small.

For shotguns and night time combat, get a Maglite or similar flashlight and mount that on your weapon. Adjust the beam so that the shot pat tern is placed where the beam falls. This permits instant target acquisition. If you can see the target and the light hits it, you can shoot it. There is now available something called the Aimpoint sight. This is a small scope with an LED mounted inside of it. Used with both eyes open, a red dot appears where the bullet will hit. Same as a laser sight, but no emission. This sight uses your binocular vision to put the dot on the target.

SURVIVAL PREPARATIONS

A major part of surviving a disaster of any type is being adequately prepared. We will discuss assembling a short-range survival kit. The object of this survival kit is to keep you alive for 3-5 days, while being easily portable in a small backpack or in a car, and to form the basis for a larger equipment set-up. The 3-5 day time period is considered to be the maximum figure one will have to endure before intermediate help is available in most survival situations. Expect a longer average delay if you live in a remote area, and-or when/where rescue efforts will be minimal. *Within 3-5 days, you should be able to:* Obtain further help from the authorities in a natural disaster, reach your main supplies or retreat, or scrounge up something more substantial and lasting.

A 3-5 day survival kit should provide the following:

(1) FOOD & WATER: You should have at least 2000 calories of food, and one quart of water per day. For food, the best are the military MREs. Altho they take up a lot of space, MREs are designed to provide a high calorie diet for highly activity situations, such as combat and survival. Another good source are the single serving cans of chili, beef stew, sardines, weenies, etc., sold in supermarkets. They're inexpensive, easy to obtain and adequate. Water is the more difficult prospect, as it takes up a lot of space and is heavy. Packaged water is available, altho two 2-quart military canteens will provide a 4 day supply and are easy to carry around and store. One should also get a water filter to augment your supply, as water is one thing that you can't have too much of.

(2) SHELTER: I recommend carrying a "space blanket", and a military issue poncho. Both of these can provide overhead cover and warmth, don't take up too much space, and are lightweight.

(3) HEAT AND LIGHT: Candles and matches serve both of these functions. A candle will not only provide light, but will also keep you warm when you bring it inside the space blanket with you, and will allow you to do minor cooking. Matches will also enable you to start a fire if something bigger is desired. Waterproof camping matches are best, altho one can get book matches free from many places, and waterproof them by putting a coat of nail polish on them. Cigarette lighters are also handy as they out-last matches. Other handy light producers are cyalume light sticks, and Mini-Maglites.

(4) FIREARMS: For our 72-hour kit, a firearm will provide you with protection from many nasty situations, as well as a means to hunt game and fend-off pests should the opportunity arise. For most survival purposes, your best bet is a semiautomatic .22 caliber rifle. This weapon is suitable for both self-defense and for small game hunting. And it is accurate up to about 300 meters, it presents a less threatening image as far as firearms are concerned, and it has a far less report than high-powered guns.

For ammo, use CCI stingers, or a similar brand of hyper-velocity hollow-point ammo, for its added stopping power. I suggest carrying about 500 rounds, which is adequate for most situations that might occur, until you either get help from the authorities, get to your main supplies, or scrounge up something else.

For greater firepower, include/substitute with a 12-gauge pump shot gun and-or a rugged .223 semiautomatic (ex: Ruger Mini-14). However, for a 3-5 day survival-kit for noncombat type conditions, these will probably be excessive as you are certainly not going to starve to death in that period of time (most climes). High-power ammo and firearms weigh more and are bulkier and less concealable.

You should also strongly consider enclosing an assault rifle and-or high- powered handgun, with 1000+ rounds of ammo and additional rations, in a heavy-gauge plastic bag/wrap. Then safely bury it at/near your final retreat/refuge or enroute to it, at least 3-feet deep and not near a popular trail, body of water or expected digging or plowing. Be sure to first prepare the gun(s) with cosmoline to protect it.

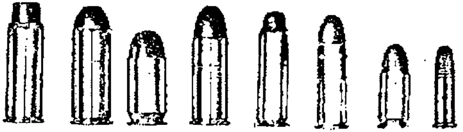
I also advise that you enclose it all in a 4-6 foot section of 4"-8" dia. PVC pipe, capped and sealed at both ends. The PVC pipe will not only further protect your stash - particularly from moisture, animals and heavy top loads - but if someone accidentally digs there and finds it, they might think that its part of a sewer line and leave it alone.

You should bury your gun(s) as close to the time that you will need it as you can predict, without being discovered or raising suspicions, but not more than five years before your anticipated needs (about now is the perfect time). About once every six months, run over the spot with a metal detector to verify that it is still intact.

(5) FIRST AID: A solid, well-stocked first aid kit should also be carried. There are many varieties out there which will suit your purposes well for YOUR PARTICULAR AREA. Include some aspirin or similar pain-reliever.

(6) TOOLS: We highly recommend a good Swiss Army Knife or a Leatherman Tool. You might also want to include some parachute cord, safety pins, fish hooks and various lines, and rubber bands. If you wear glasses, include a back-up pair. Also include a small pair of quality needle-nose pliars, and a small pair of channel-lock pliars.

CALIBER COMPARISONS



	44 Mag.	45 Colt	45 ACP	44 Spec.	357 M.	38 Spec.	9 mm	22LR
Bullet Weight (grain)	240	255	230	246	158	158	115	40
Muzzle Velocity (ft/sec)	1470	860	850	755	1410	855	1140	1255
Bullet Area (sq. in)	0.146	0.159	0.159	0.146	0.102	0.102	0.102	0.038
Relative Stopping Power	1.0	0.677	0.600	0.526	0.441	0.267	0.260	0.037

Many survival sources recommend sewing equipment. A much better alternative I have found is a tube of silicone rubber cement, because it will not only make many fabric repairs that both can and cannot be made by sewing but will cement/repair/seal wood, metal and plastic.

Virtually all survival sources also recommend a good hunting knife. I also include a heavy XACTO knife with various types of replacement blades. XACTO knives are razor-sharp and great for doing delicate and detail work, like notching wood for small-game booby traps, making minor repairs, performing minor surgeries, skinning small game, etc., and will save wear-and-tear on your hunting knife. A hunting knife provides good self-protection and quiet killing, is preferred for cutting branches and other heavier materials, and is better for skinning major game.

(7) SIGNALING: A signaling device is a handy thing if you're lost or trapped to let rescue personnel know where you are. Include both a high-pitched whistle and a small handheld mirror. The mirror is great for signalling aircraft and across mountain ranges in the day. The whistle is great for nighttime and poor visibility situations. If you are in a somewhat civilized area, you might also want to pack a CB Walkie-Talkie. For disasters in which the government is still around, a port able AM/FM radio might also be a good idea.

If you can get a hold of them, you should also bring along some bottle rockets (the poor man's flare), enclosed in watertight plastic. By firing one in the air, you can alert people for a 10-20 mile range typically, as compared to a 1-5 mile range typically of firing a gun in the air from any place except a mountain top or tall building. They get you above the tree tops, and are particularly noticeable at night!

Finally, the last and most important thing needed is the proper skills, attitude and physical conditioning. Without those your chances of making it are much-diminished.

TYPICAL SURVIVAL SITUATIONS

We have often stated that the hardest part of being a survivalist is not surviving when or after the "*shit hits the fan*", but right now, before that gruesome event. It is obvious that the world is heading for at least one type of major disaster, and that once this happens, then the rest of the dominos will fall. However, it superficially appears that the country is doing great, thanks to the media smokescreen and political song-and-dance, and the tendency for people to avoid looking at the dark side of things. The problem right now is that there doesn't appear to be a problem. As a result the attitudes of survivalism are currently "out", and anyone who adopts these attitudes is looked at with a jaded eye.

This ignorance and apathy causes various problems which are not conductive to the survival preparations you are, or at least should be, making right now. In short, if the country had already gone to hell in a handbasket, we'd have no problem as we'd simply step in and start running our own lives without government interference for a change. But since the government is still in power, we are faced with our greatest survival challenge - preparing for survival amidst the increasing government regulations and snooping which hinder such activities.

In the survival process, you will encounter three stages of condition in your efforts. The first is making and maintaining preparations before the event which we have christened "when the shit hits the fan". The second stage is implementing these preparations while this event is in process. The actions you will take then dependent upon what exactly happens. The last stage is after the end occurs.

Each stage presents it's own problems and objectives that must be dealt with. This is further complicated depending on whether you live in an urban, rural or suburban area, and whether you live in a "special area", such as the Canadian or Mexican border. Each of these areas will be discussed in detail along with the special requirements they may have for a successful survival operation.

Many brilliant men were persecuted, or at least thought strangely of, because of their above-average applications of their great intelligence. People like Einstein, Tesla, Da Vinci, Copernicus, and Galileo made great strides in the advancement of science, and were snubbed by their contemporaries. Except for occasional lapses, this "peer pressure to stay stupid" attitude continues today with the use of words such as "dexter" and "nerd", which are derogatory terms used to define someone who is intelligent and-or very knowledgeable.

The current attitude is against survival preparations, and survivalists in general. Some people will think you're just "strange", others will think you're a fanatical right/ left wing terrorist that should be locked-up so you can't harm society any more. Have you noticed that every time a person commits a mass-murder, the media describes him as a, "Survivalist"?

From my observations, there are two major forces in the anti-survival movement:

(1) The liberal political persuasion, which has been anti-survival for as long as I can remember. As any good technological survivalist knows, one of the things that they are hardly "liberal" about is the possession of firearms by citizens.

(2) The major corporations and big businesses. Since the 1960s, the number of corporate abuses against the people have risen to a point where they have computerized access to your complete history right down to your underwear size, and have made it legal to rip you off

EVALUATION OF WELL-KNOWN AND /OR POPULAR SUBMACHINE GUNS AND ASSAULT RIFLES

NAME	CALIB.	CYLIC RATE	MUZZLE V. fps	EFFEC. RAN. yd.	WEIGHT lb.	LEN. in.	BARREL Length	I	II
M-60	7.6	600	2800	800+	23.0	43.8	25.5	W	G
UZI	9mm	650	1350	220	8.9	25.5	10.2	W	B
Ingram M10	45 ACP	1100	900	200	6.4	13	5.8	M	B
Walther MPK	9mm	550	1210	250	7.7	26	7.8	M	B
M3, M3A1	45 ACP	450	900	100	10.3	29.8	8	M	B
Berretta M.12	9mm	550	1250	250	6.6	25.4	7.9	M	B
Vigneron M2	9mm	600	1224		8.7	34.9	12.0	M	B
Sten Gun MK2	9mm	550	1200	150	6.7	30	7.8	M	B
Reising M.55	45 ACP	450-500	920		6.3	31.3	10.5	M	B
ERMA MP 58	9mm	700	1250		8.1	27.6	6.5	M	B
M16, M16A1	5.56	700	3250	500	7.2	38.6	20	P	G
AK-47	7.62x39	700	2230	300	9.5	34.3	16.3	M	G
M2, M3 Carb.	30 Mi	750	2000	300	6.6	35.6	18	W	G
M14	7.62	750	2800	650	8.6	44	22	W	G
Colt Commando	5.56	700	2750	400	6.5	31	10	P	G
AC-556K (Ruger)	5.56	750	2750	400	7.7	32.5	18.5	M	G
HK 33	5.56	600	3145		7.7	37	15	M	G
AR-18	5.56	700	3000	450	6.5	38	18.3	P	G

I = Composition of Stock (W = Wood; M=Metal; P=Plastic). II = Gas (G) or Blowback (B) operation.

in many ways (ex: car insurance).

Ever have a problem with a major corporation and try to resolve it? Or know of someone who has? Then you know what I'm talking about. This situation is also made worse by the fact that most major corporations are owned by foreign interests. In fact, of all the Fortune 500 businesses, only two are majority-owned by Americans: IBM and Exxon (both of which are guilty of major infractions against the people - IBM with it's anti-consumer attitudes and unfair employment policies - and Exxon ("The sign of the double cross") by damaging the environment and getting away basically scot-free). Of the remaining 498 Fortune 500 businesses, about half are mostly or completely owned by the Japanese.

The fact that banning guns in The United States of America could even be contemplated is a very disturbing thought. The fact that it has almost succeeded on occasion, be it not for the will of the people, is doubly disturbing.

You now see why surviving before the Day After can be the most difficult experience in the survival process. You have to make preparations for when the shit hits the fan while the Government and big business try to stop you by passing laws to disarm you and make you incapable of running your own life the way you wish - as opposed to the way some bureaucrat in Washington DC or corporate big-shot wants you to.

There are two major things you can do at this stage. The first is to prepare as quickly and discreetly as you can for the future. Once you are prepared, there is nothing they can do to stop you short of killing you, and even then they'll have a hard time as you'll be shooting back!

The second is to fight back as much as you feel is safe, and within "legally acceptable means". As I once said "*Only fools and cowards tolerate injustice. Those who publicly protest are often dead right.*" Altho we live in a "free country", our freedoms are slowly diminishing, and I feel it's only a matter of time before the Government and corporations step up their level of oppression and repression to dragging away people in the middle of the night. Some people believe that it's already happening today. Remember though, that once you are fully prepared, you'll be able to fight back.

Two major tasks you will have during the "beforemath" stage will be acquiring your survival supplies, and becoming proficient in their use. While you might still be able to acquire items after the shit hits the fan, chances are you'll be too busy to effectively learn how to use them.

In procuring your supplies, keep in mind the potential use that a piece of equipment will be put to, and any secondary uses it may have in it's unmodified, or in a slightly modified form. The best way I have found in procuring supplies is to take inventory of what I already have, then make a list of what I need (or vice-versa) and how much I have to spend. From there I can then go about completing my stockpiles, noting the best value for each item I need (note: I didn't say "cheapest", or "most inexpensive" - a cheap piece of equipment is worthless if it breaks the first time it's used). While you are procuring supplies, you should also be finding places to hide your supplies and equipment.

During the pre-disaster stage, one should also be making specific plans for what to do when the shit hits the fan. These plans should cover different scenarios, as well as various situations and conditions in each scenario. Even if your original survival plans are only for one type of scenario, it would be in your best interest to expand upon it, as anything can happen. Keep your plans to yourself, and if you're in charge of a group, only let those members who are essential to the early stages of the plan know of any specifics. At this stage, if you are in a group, you should be able to trust the people in it.

These plans should take into account:

(1) A probable scenario for your location.

(2) Any areas near your location which would have an effect on your plans.

(3) Whether you're going to stay at your current residence or evacuate to another refuge.

(4) Routes and transportation arrangements if you're evacuating (with alternates).

(5) The state of the area you'll be evacuating to, as well as the state of the route(s) you'll be taking.

(6) What to do in case of government (or what's left of it) interference. Consider local, county, state and federal government.

(7) Group rendezvous, and contingency plans if members of the group don't make it according to schedule.

(8) And any particular effects a particular scenario will have upon your groups long-term plans.

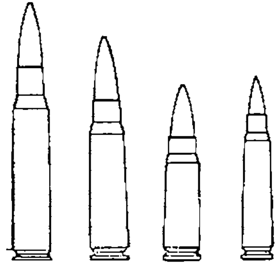
NUCLEAR WAR

Don't let the fact that the dissolution of the Soviet Union means nuclear war could never happen. Communist China is a constant threat to our country, as well as the dire consequences of a country like Iraq or Iran acquiring long-range nuclear warheads. If you don't think one of those countries wouldn't send over a nuclear warhead in a heartbeat, we've got some oceanfront property in New Mexico we'd like to sell you!

But I do feel that a full-scale nuclear war is unlikely because of its immense destructive force. The United States has the best and largest commo matrix in the world, the biggest transportation network, and has great capabilities in agriculture, industry, science and natural resources. Until very recently we were one of the best in many of these fields, and still have a pretty respectable standing. Because of this, we would be a great prize to any foreign invader, and the full-scale use of nuclear weapons would destroy our great resources.

However, it is entirely possible that nuclear devices could be used on a small-scale tactical basis to destroy defense systems that could be used in a retaliatory action if we were attacked, or as a psychological warfare weapon against the civilian populace in order to keep our military and law enforcement personnel occupied with the civilian population while we are invaded.

With the lack of a civil defense program, this becomes all too possible, and easily done. Nuclear weaponry could also be used against us by a nation that isn't interested in our resources, such as a religious fanatic attempting to destroy the "Great Satan".



	30-06	308 NATO	7.62 Bloc	223NATO
1.	150	150	122	55
2.	2800	2750	2330	3200
3.	1.00	.965	.563	.479
4.	1.00	.982	.677	.419

30-06 compared to the three major modern assault rifle cartridges: 1. Bullet Weight (grains). 2. Muzzle Velocity (ft/sec). 3. Relative Muzzle Energy. 4. Relative Muzzle Momentum.

However, the United States Government is also aware of this problem, and supposedly does something about it when such a threat is received. Perhaps it is fortuitous that most of these "fanatic" countries are also enemies of Israel. Israel attacks and destroys nuclear facilities of various Islamic nations - knowing very well that their real estate would be destined to become a giant radioactive parking lot if one of them got his hands on an H-bomb.

FOREIGN POWER INVASION

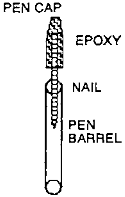
One of our greatest threats lies in a foreign power invasion. Fortunately, this one will be relatively easy to survive. Getting the country back might be a little tough though. Two countries in the world pose a real threat in this respect to our country. They are the China and Japan. Of these two, the country who would try an invasion in the truest sense of the word would be the China.

A nuclear or large-scale conventional blast might also be used as a psychological warfare diversion as discussed earlier. A large Astrolite warhead could be delivered via missile, and put out much of the physical effects of a small nuclear device, fooling many people into thinking a city was just "nuked", causing many lethal and many more nonlethal casualties, and many panicking people who won't have the slightest idea what to do or of what's going on.

These attacks could be delivered via a cruise or other short to intermediate range missile from a submarine or "fishing trawler", and come in under radar thus insuring a surprise attack.

As could be expected, an invasion of the United States would result in a high level of resistance by the American people. Combine this with the fact that despite all the laws the Washington prostitutes are trying to pass, the American people are armed and equipped well enough to be kick-ass freedom fighters. If an invasion were to occur, the American people would be able to form the most effective resistance movement in history, operating with an unheard of level of sophistication, having one of the biggest and best commo, transportation and industrial bases in the world to work with.

PEN WEAPON



One may also use a fountain pen and small knife blade.

A far greater threat is posed by Japan. While militarily weak, their mass purchasing of U.S. property and corporations is probably leading towards an even subtler form of takeover. Their takeover of America is so subtle that one morning you could wake-up and find them in control. In this form of takeover, the Japanese could easily assume the position of this country's ruling body, and then suddenly take tyrannical measures to wipe out all opposition to them.

Some things that you should know about the Japanese that are already happening (in addition to their feeding-frenzy over here):

(1) The Japanese are basically a warlike and racist people. From polls I have seen taken of Japanese, the average Japanese has the elitist idea that if you are not of Japanese descent, you are automatically inferior. Don't be misled by the fact that the Japanese do a lot of bowing and have a lot of etiquette. Once firmly in control, I'm certain that you will see a very drastic change in their behavior. Ask anyone who has witnessed their behavior during wartime how much bowing they do.

(2) The Japanese are in control in many areas already POLITICALLY. For all intensive purposes, the State Legislature of Hawaii is an arm of the Japanese Government, and California is about there now (one good reason why they are on the forefront of gun control legislation)! Japanese interests spend hundreds of millions of dollars every year influencing U.S. political races from mayors of towns and cities to the President of the United States.

(3) If you look closely at TV and movie fare lately, you can't help notice an increasing trend of portraying Japanese in highly-positive lights. I find a lot of subtle and subliminal type messages all of the time. And there are special programs about Japan aired almost daily that look like they were prepared by the PR department of the Japanese Government. While no race or ethnic group should be portrayed in any kind of negative stereotypical light, I personally resent very much attempts made to "brainwash" Americans regarding anything or anybody.

DICTATORSHIP/INTERNAL TAKEOVER

In my opinion, the greatest threat to the United States of America lies in an internal takeover of the Government (probably secretly backed by a foreign power), thus causing a totalitarian state to assume power in place of our republic. This could come from many different angles, altho at this time the biggest threat lies from the multinational corporations, who are increasingly becoming controlled by foreign interests. Such a takeover would be preceded by increasing restrictions on citizen's rights, and moves to keep better track of the people.

This has already occurred. For starters, laws have been passed which have restrictions on listening to radio commo, thus violating the "free airwaves" doctrine which has been around since the dawn of radio. Laws were proposed which tried to regulate and restrict computer commo via the Internet - in direct violation of the First Amendment. And several attempts, some successful, were made at snatching away the right to keep and bear arms - the thin blue line that protects the rest of the U.S. Constitution. The modus operandi of any dictator is to immediately seize all guns and radios. Even a cursory glance at the world history of this century will prove this.

Perhaps this time though, people will be prepared and we can prevent what happened in the past from happening again. An internal takeover is one of the most difficult things to deal with. If you are going to do anything about it, as hopefully we all will, you'll be forced to exist outside of society as a "fugitive criminal".

While many people will be involved in the resistance movement, a great many will not want to get involved, and may even be profiting from the resulting situation. These people will naturally do whatever they can to hinder you in your activities.

The Government will also use distractions in the media - smokescreens based upon frivolous or much less important issues that will divert the attention away from the other, nefarious things that politicos are doing to us. Many of the issues that we are confronted with today are basically minor compared to the ones that should be addressed. Watch the TV news or any talkshow, or read your newspaper or magazine, or listen to your radio, and every time an issue is discussed, compare its importance with these truly life-and-death issues:

(1) Economic collapse of our Government due to massive frauds, swindles, waste and mismanagement.

(2) The takeover of our country by "Foreign Markets".

(3) Massive and routine violations of citizens rights to privacy by big business and government.

(4) The erosion and destruction of our most basic Constitutional rights.

(5) The massive erosion, destruction and selling-off of our industrial, transportation and agricultural base to the point that when we go into the next, upcoming depression, we won't have a way of economically pulling ourselves out of it.

How many times are these vital issues seriously discussed? Thanks to the suckasses that provide us the "news," I know everything that is going on in Disney World and Universal Studios, I know 100 different ways to do my hair, Marilyn Monroe's last words, and who is gay in Hollyweird. What I would really like to know is how are these vital issues going to be solved TODAY!

ECONOMIC COLLAPSE

Also high up on the list of possible disasters is an economic collapse. The dollar is only backed by faith, and not by any real amount of gold, silver or industrial base, and that money in the bank isn't all that safe. An economic collapse could very easily occur. If such were to happen, the best route would be to become as self-sufficient as possible, and have some effective goods to barter with. Both courses of action would be wise in any survival situation. One might also encounter some problems from an internal takeover if the Government notices that you are better off than you are, and "asks" you to share your wealth with your less fortunate neighbors.

NATURAL DISASTER

Most natural disasters are, relatively speaking, minor disasters - ones in which governments are still around and assistance from third parties can be expected.

Recently, the world has been seeing some strange things weather- wise. The earthquakes of large magnitude on the West Coast, the ones beginning to appear in the east, high-powered storms on the eastern seaboard, tornados in southeast New York, and a massive drought in Africa. Scientists have stated that this is just the beginning of what is to come. While the main intent of this work is for preparation against man-made disasters in which government assistance may be unavailable or undesirable, many of the techniques here are very suitable for natural disasters which may occur.

MOVING VS. STAYING: Among survival circles, there is much talk about the merits of heading for the hills versus the merits of staying where you are to slug it out. Each has it's advantages and it's disadvantages. "Bugging out" is usually done to insure that you will be in a safer place during the disaster. This would be advantageous if you live in a city, and feel it may be bombed, nuked or suffer from extreme civil disorder (ie: rioting, looting, wilding). It has some disadvantages:

(1) Unless you'll be staying at a "summer residence", or living out of an APC, you'll be at a defensive disadvantage, and will have to use extreme caution and stealth to avoid problems from better-armed, less civil, and larger groups who'll be heading for the same hills you are. You'll also have to put up with whatever the weather decides to throw at you. If you're considering living like that in the event of an emergency, then spend a week or two "vacation" in the middle of the wilderness, living out of a tent and off of whatever you brought in on your back. If you can handle that, then you're off to a good start at nomadic living.

(2) If you happen to have a "summer residence", you'll have to get there, and there might be the possibility that some other group may have found your "abandoned property", and set up shop there. In the event of an emergency, it is doubtful that the local authorities will look kindly at a bunch of heavily-armed and equipped people "roaming around", at the least you might get sent back to "where you came from", at the worst you could get shot or arrested, and have your stuff confiscated.

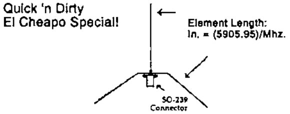
(3) Unless you are familiar with the area you will be staying at, you will be at a great tactical disadvantage. You can minimize that problem by obtaining Geological Survey maps beforehand, and if possible, visiting the area with the idea of learning all you can about its people, economy, topology, flora and fauna.

(4) Whenever you flee an area, there will be many other refuges fleeing with you! The risk of getting caught up in some massive traffic snarl is very high, and that would likely mean abandoning your vehicle and hoofing it with only what you can carry in supplies. If members of your party aren't capable of doing that for any distance, they would most likely be killed!

If you stay where you are, you won't have to move in the event of an emergency, which is a noted advantage. You will also have the advantage of knowing the terrain better than anyone coming in. And you will know who should be there and who are strangers. If you are on good terms with the local authorities, you should have no problems with them as long as they are in authority.

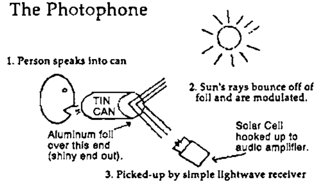
However, in some cases it won't be possible to stay where you are, such as if you live in an apartment in the city, or in a "target area". I recommend that if you don't live in the city, in an apartment or in an area which may be targeted for attack by a weapon of mass- destruction, then stay where you are. If not, then seriously consider getting a "summer residence" where you could go if things get bad. Of course, no matter where you'll be, if there is an emergency, and people "head for the hills", then there will be plenty of places you will be able to occupy, just make sure the previous owners haven't installed any secret access points.

As a general rule, you should do the OPPOSITE of what everybody else is doing, because the enemy will most likely both anticipate what the reaction will be and concentrate on the greater number.

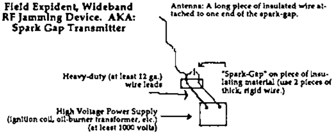


1/4 Wave Antenna

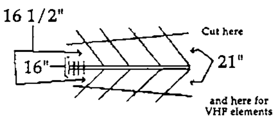
The Photophone



Field Expident, Wideband RF Jamming Device. AKA: Spark Gap Transmitter


Antenna: A long piece of insulated wire attached to one end of the spark-gap.
Heavy-duty (at least 12 ga.)
wire leads
"Spark-Gap" on piece of insulating material (use 2 pieces of thick, rigid wire.)
High Voltage Power Supply
(ignition coil, oil-burner transformer, etc.)
(at least 1000 volts)

Approx. Freq. Range: 500 Khz. to 500 Mhz.



Converting a VHF/UHF antenna for scanner use.

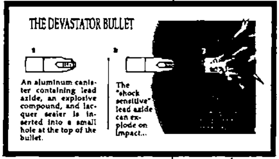
THE SURVIVAL RESIDENCE

There are several modifications you can make to your residence and property to make them more suitable for a survival retreat. The problem with your average residence is that a great number of it's functions are dependent on outside sources which may not be functional in an emergency/survival situation, and that most residences and property aren't designed with physical security and defense in mind. A survival retreat minimizes many of these problems. A survival retreat should be in a suburban, or better yet, rural area in order to be able to do these things.

Most urban houses and all apartment buildings are designed to integrate with the public utilities, and are very difficult or impossible to convert - which makes them unsuitable for survival purposes. The first thing one should do is to make their survival residence independent of public utilities which may fail in an emergency situation. This includes electric, water, and heating service. To do this, one must have plenty of property space, which rules out most urban areas.

Heating is by far the easiest to accomplish. Wood-burning heating systems are readily available, and were the first heating systems used by man. Wood is also a renewable resource. Solar heating, used by greenhouses, is also a good possibility, altho it requires the presence of a decent amount of sunlight. And there are always tons of burnable trash around.

Another possibility is methane energy. I haven't heard much about this, but methane production is cheap and easy. Methane is a flammable gas produced as a by-product of decaying waste matter. It's also known as "poop power", and as far as production and renewability are concerned, it's as good as you can get. Similarly, alcohol is another renewable source that's easy to use, and can be made from the waste products of any decent-size farming operation.


THE DEVASTATOR BULLET
1
2
3
An aluminum canister containing lead azide, an explosive compound, and lacquer sealer is inserted into a small hole at the top of the bullet.
The "shock sensitive" lead azide can explode on impact...

Wind has been used by farms in the midwest, but in my opinion is too unreliable. If you live by a moving body of water, like a large stream, or on a seashore, then you can use water generation, and have a reliable, long term power source.

One good idea is building an underground house. Not only will it provide good protection against a nuclear attack, but it is also easily defendable, easy to add secret passageways, hiding places and access points to, easy to conceal by using terrain features to hide it, and very energy-efficient. When the house is being built, make plans for a good physical security layout, and large amounts of storage space. After it's built, add a decent security system.

TYPICAL SCENARIOS

City/Urban:

Depending on what type of disaster occurs, an urban area can be either the worse area to survive in or the best. An urban area is heavily built up, with a large population. To cover some common situations:

The main problem with urban survival situations is that in such areas, there are various laws against possession of weaponry, and the concept of self-defense is looked at with a jaded eye. While in the country, the citizens have no gripes about you keeping a rifle or shotgun on a rack in the rear-window of your vehicle, or packing a pistol while you go about your business, in the city, you might start scaring people and possibly get arrested on a weapons charge. Even to possess a weapon in your home requires a permit in most cities. So, even if you have no space constraints while living in the city, the fact that obtaining some basic survival essentials is illegal should have you seriously considering your choice of living area.

Another problem of urban living is the fact that cities are targets of weapons of mass destruction. You wouldn't want a nuke strike to ruin your survival planning by getting caught too close to where it hits.

Finally, the last problem is the high crime rate that naturally occurs in city areas due to the large population, and strict weapons laws. Because of this, there is a good chance that you might get killed by some junkie or mugger before you even have a chance to react, or get arrested for wasting your attacker. Because of this, the military is often called in to help provide order during emergencies. As a result, you could have your equipment confiscated, and be shot or detained just for what amounts to being prepared.

That is not to say that cities do have some advantages. If a disaster leaves a city mostly abandoned and somewhat intact, then one can have an easy time surviving on the supplies which were left behind. After such a scenario, provided the national guard didn't move in, one could live quite well by scrounging the large supermarkets and department stores, and finding a decent amount of living space.

Suburban:

A suburban environment offers many advantages over the city. It is far enough away from urban areas to allow you to prepare more easily than in the city, yet is close enough to enjoy the logistical advantages of urban life (ie: getting what you need easily). However, it is the suburban areas that will get the influx of gangs and refugees from the city when the shit hits the fan, as when they head for the hills, most will stop at the suburbs to rape and pillage wherever they can.

If you plan to keep a retreat in the suburbs, extra fortification on your survival residence will be necessary, as well as great preparations for siege-like conditions. Be prepared to be able to out-shoot and out- starve any invaders who might have you surrounded. I would also recommend lethal defense systems ready to be installed on your property to prepare for the disaster occurs. Better yet, relocate to the country.

Rural:

All in all, the rural environment is the best for survival purposes. By operating in a rural environment that you are extensively familiar with, you gain a major advantage over non-trained individuals or groups operating in unfamiliar terrain. While some street-gangs armed with chains, knives and cheap guns may rule their urban turf, they'll stand no chance against your group in the woods, hitting them with booby-traps, and sniping at them from 100+ yards away with deer rifles.

While the rural area will get its fair share of refugees, for the most part they will be unfamiliar with the area, and no problem to defend against. The rural environment, when properly handled, also precludes any siege situations that might be common in urban and suburban environments. Your base will be well-hidden, taking advantage of natural features and camouflage, and be equipped with booby-traps and early-warning systems. The only disadvantage to a rural environment is that it lacks the convenience of the urban and suburban areas, which in itself isn't all that bad.

MEXICAN BORDER:

If you live near the Mexican border, you are in for a special experience. The Mexican border is probably one of the worse places to be living near when the end comes. Today, Mexico is in economic and political crisis, and undergoing a quiet communist revolution. If you live near the Mexican border, I strongly advise that you clear out as soon as possible!

Illegals are coming across the border every day, and among those are "banditos", drug runners, Cuban agents. Living close to the border gives you a much better chance of getting robbed or killed. Also, due to all the illegal aliens and drug runners, conducting your group's training - even on your own property - is likely to get the attention of the DEA and the Border Patrol - not something you want!

Furthermore, when the shit hits the fan in Mexico, the number of illegals coming over the border will at least increase by a factor of 10, and if Mexico falls to the communists, an invasion could come straight up across the border - either of which would turn that entire area into a most harrowing experience.

CANADIAN BORDER:

The Canadian border is a mixed blessing. If a dictatorship were to take over in this country, or massive persecutions of your race, religion, ethnic group or creed were to take place, living close to the Canadian border would give you an opportunity to get across it, and seek at least temporary refuge provided our Northern neighbors didn't share in the same craziness that would be occurring down here. Canada still consists of vast stretches of wilderness, but the winters are awfully cold. On the flip side, a foreign power invasion could come down thru Canada much the same way as up thru Mexico - altho Mexico is by far the best of a foreign-invasion route.

COASTAL AREAS:

A coastal area is one of the best places to live. The sea provides an abundance of food, and if you own a good vessel, an easy way to escape the country if something goes wrong. And it provides a source of cheap, available energy, a guaranteed supply of water, and better year-round temperature regulation. Unless you have a sea-going ship, the only way you'll escape by boat is to head down into the Caribbean, which isn't a nice area even during peace with all the drug runners, pirates and the Coast Guard. If the shit hits the fan, that area might become hazardous to your survival if you stay there for any length of time, and at certain times of the year, hurricanes and other storms frequent the area. In any event though, if you're into survival, a coastal area will provide you with many benefits. If escape-by-sea is going to be one of your serious options, you not only better prepare your ship and supplies but also your seafaring skills and knowledge, as the sea can be very treacherous - particularly for the unprepared and the ignorant.

NUCLEAR, BIOLOGICAL, AND CHEMICAL WARFARE

The military's "big guns" are their stockpiles of nuclear, biological and chemical weapons. These weapons require some safety risks and little discovery risks to make, are easy to deploy and often deployable by secret means, and can be quite effective. Nuke/Bio/Chem weapons are also so misunderstood that even the mere threat of them can induce terror and panic.

The Geneva Convention prohibits the use of Chemical or Biological weaponry in a war, but in all honesty should a war break out, it is doubtful that this (voluntary) restriction would be adhered to. Chemical weapons were used by the U.S.S.R. in Afghanistan and a few other places, and by both sides in the IRAQ-IRAN WAR. It is also common knowledge that they were used by Saddam Hussein's troops against us during Desert Strom. However, they can be detected, and usually easily defended against.

While the manufacture of full-scale nuclear devices and nerve gas is beyond the capability of everyone except large corporations and governments, there are a few simple and basic techniques which one can make under primitive conditions. While in no way as powerful as the military stuff, they are usually effective enough.

NUCLEAR

While the actual process of making a nuclear device is not difficult, one does need to have a source of weapons-grade plutonium (difficult and expensive to obtain), and one must have access to a rather sophisticated lab setup to avoid accidents and getting radiation poisoning. As an alternative, there is the R.E.D. (Radiological Explosive Device) Bomb. This device is a fragmentation grenade or similar type explosive device which casing is made of radioactive materials. Radio active materials require a Federal license to possess, but small amounts are available from many scientific supply houses.

When detonated, the blast radius will be littered with radioactive shrapnel - effectively contaminating the area. The end result will most certainly be severely contaminated wounds for anyone caught in the blast radius. The contamination of the area for quite a while, making it unsafe to be around, and possibly the death penalty for you if you're caught. The U.S. Government has an organization called N.E.S.T. (Nuclear Emergency Search Team) whose entire job is to identify and deal with nuclear terrorist threats. They probably don't see much action, so if you are found doing something like that, they'll probably tackle the case with an unprecedented enthusiasm and major amounts of "inter-agency cooperation" and firepower.

Another more subtle method is to take radioactive dust or liquid and spray it into the target area thru its ventilation system, or contaminate the area's water supply. Quite nasty and undetectable (unless you have a Geiger Counter and it is ON when the contamination occurs).

NUCLEAR DEFENSE

There have been many books published about surviving a nuclear war. The best one I've seen is "Life After Doomsday" by Bruce D. Clayton (available from many survival book-sellers). It's an excellent and comprehensive work on the topic. Personally, I feel that a "classic", all-out nuclear war or even a "limited nuclear exchange" within this country, is unlikely, but the possibility always exists for some fanatical terrorist group to make a R.E.D. Bomb and possibly use it in some concentrated, urban area.

The best defense against a R.E.D. Bomb is to not be around one when it goes off. However, it's hard to avoid airports, major hotels and other highly public and visible places. The next best thing is to quickly get behind some solid, hard cover to avoid getting hit by the radioactive shrapnel, and then flee the area. The ideal thing for someone who might be able to do this is a hazardous materials suit and some major fragmentation clothing. Of course, you normally don't have this stuff readily available in most public places and most blasts that will affect you will be near enough to you that you can't react in time to stop or avoid the shrapnel.

Dealing against intentional radiological contamination is even worse. If you feel that you may be subject to those attacks, keep a Geiger Counter on at all times, and as soon as levels go up over background, flee the area. You should also secure your ventilation and water access points against the possibility of someone doing this. The idea here is prevention, as there's little you can do once it occurs. (see our SILKWOOD device plans).

BIOLOGICAL WARFARE

Biological Warfare has been with us ever since the Middle Ages when both sides of a conflict tossed waste matter, garbage and dead bodies at each other hoping they'd catch some disease, and put nasty things into each other's water supply to try to poison them. Today, biological warfare ranges from smearing shit on punji stakes and knives to give an enemy lockjaw, to the use of aerosol and insect vectors, to intention ally spreading diseases. The basic precautions are to keep your immunizations current and to keep your living conditions as clean as possible. Cook foods thoroughly and try to assure their sources are uninfected. Also, flee anywhere that's being sprayed by air, and keep the insect population under control with sprays and netting.

CHEMICAL

For starters, pick up a gas mask at a surplus store somewhere. The Israeli ones are best. This will protect you from tear gas and some of the more lethal ones. For expedient chemical protection, get some impermeable clothing, such as a rubber raincoat and hip waders. Close up any openings with duct tape. Then get out of the affected area and out of low lying areas. "Poison gas" is generated from a liquid or dust and usually seeks the lowest ground. Remember though, the best thing to do is to simply leave the area, and get washed off ASAP. The military deploys poison gas by either spraying it or by artillery. Spraying is pretty obvious. A gas round will sound underpowered, like a low whump instead of the usual bang. You'll probably also see lots of "smoke" when it impacts. Chlorine gas is a popular weapon. It is made by mixing ammonia with Chlorox, and it induces pneumonia of the lungs (often fatal).

URBAN SURVIVAL

The city is a place which due to your job or some other necessity, you could find yourself in when the "shit hits the fan". As dangerous as city living is, the greatest threat to you by far is from street crime - not from a foreign invasion or dictator takeover in Washington DC.

You could be accosted by muggers convinced that your wallet is their next source of income, or you could accidentally/unknowingly piss off some 14 year old turdball because the shirt you're wearing happens to be his gang's "color". You could also be walking down the street and be blown away because some rival gang member happened to walk by you when he was attacked in a drive-by shooting by some shithead who can't aim or used the shotgun approach.

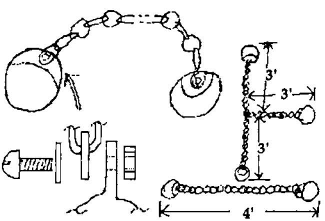
All of those are just the day-to-day dangers you face when you're in any urban area. There's always the possibility that some terrorist or foreign power might pick the place as the optimum target for a nuclear or chemical weapon; or think your office building, or restaurant would make the perfect place for a random bombing or hostage situation.

As you know from terrorist situations in Japan, the subway is a perfect setting for a chemical bomb. Bio and chem weapons are a cheap and easy means of mass destruction. Even piss-poor third-world countries have them. Just think if some religious fanatic who runs one of those places decides that using his stash would help defeat "The Great Satan"? Do you think a couple of million people living very close together would react in a calm manner when they realize that they've just been hit with the modern day version of the black plague or by a small nuclear device? Finally we have the general, overall tendency of city denizens and their respective law enforcement to randomly go absolutely apeshit.

All of this is complicated by the fact that the politicians and bureaucrats who lurk in these areas are usually more prone to pass laws limiting the citizens' right and means to defend themselves'. Criminals love this as it makes for easier business. A foreign invader loves it too, as it makes subjugating the place easier when they move in. Sheep are good for one thing only - to slaughter!

Surviving the Streets: There are a number of things you can do every day in the city to avoid becoming a victim of a mugging or similar antisocial encounter. The first is to dress discreetly and modestly. Try to avoid red or pastel blue clothing - common gang colors. Don't stand out because you look well off. When your walking, keep a confident, alert look on your face - don't shuffle around or hang your head in submission when you encounter or pass others. Look like you know where you're going and doing. Keep a hand concealed so it looks like you are holding a weapon in your pocket. For that matter, keep your hand on the weapon in your pocket. Stay closest to the street, away from alleys. Late at night, if traffic is light, walk in the middle of the street; it minimizes ambushes. And learn about what areas you should stay away from, and stay away from them.

Also, stay away from any teenagers or young adults who are wearing unusual decorative clothing, clothing which seems to proclaim some sort of unknown or dangerous organization, in easily recognizable colors such as red and blue - especially if their talk seems full of esoteric and cryptic sayings or jargon or body language. Those are indicators of street gangs. Most muggers and random-wilding wolfpacks are looking for what appears to be easy prey. Put forth an appearance that you are not the type to with, and 90% of the time, you will be left alone.



IMPROVISED BOLAS The nice thing about bolas is that they can be easily made from readily available materials. Bolas come primarily in 2-end (ie: ball) and 3-end types. The 2-end types are easier to control. Traditionally, the bola is thrown to entangle the feet of the enemy or his horse. However, particularly if the bola is made heavier, it can be handheld to flail the enemy with the balls or to entangle him with the chain or cable. The balls or weights can be any size, shape or mass, but should be ones that you can comfortably handle. Spiked or unspiked. Large fishing sinkers, lead tire weights and dumbbell plates are common. Also commonly used are plumbing parts, iron stock and scrap iron parts. The chain or cable must be flexible in all directions (avoid bike chains and thick, heavy steel cables). In lieu of chain or cable, hemp rope will also work. Soak it in salt water before throwing, or dust it with graphite first, or feed it thru braided cable shielding. Or use stranded cop per wire (0-12 gauge, remove at least 6" of insulation from each end). Another good alternative is piano wire. Used correctly, a piano wire bola will slice off the body part it wraps around. Piano wire is avail able from music supply stores. Still another is a carbide saw blade. The line can be attached to the weights with pinched-on or screwed-on collars, welded, brazed, soldered or tied. Try out several variations of weights and lines to find what suits you best. If you are concerned about getting caught, make an on-site assembly using heavy duty double-ended fishing swivels.

If you are ever find yourself alone at night in a dangerous neighborhood, one technique that works very well: Muss up your hair and clothes and dirty your face (as if you are homeless). Then take a piece of string and let about 3 inches of it to hang out of your mouth. If you have a red candy, chew it and let some of the spittle and foam run down the sides of your mouth. Believe me, nobody - I mean NOBODY - will mess with you!

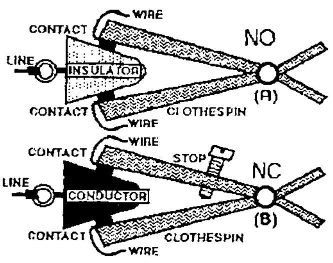
Another excellent el cheapo technique is one that your grandmother used to defend herself from mashers - the good ol' hatpin. A hatpin can be easily secreted in the hair, clothes, purse, wallet, shoe, etc. Weapons like stun guns and mace are much more difficult to access and apply in an emergency. When threatened, it is quickly retrieved and causes severe pain to the criminal. A stab in the eye, ear canal, throat, genitals or lower back (kidneys) will quickly end even the most determined assault. See our, "Mugger, Rapist - Diet" - manual for the ultimate non-firearm self defense weapon.

If you are confronted and have the slightest belief that you are in danger, react with full force and get the hell out of there. Wreck as much havoc, confusion and destruction you can in the shortest amount of time, and then leave quickly. Either your threat will be neutralized or it will be confused long enough for a clean getaway. There are many different kinds os self-protection weapons ranging from belt buckle knives to derringers. See Soldier of Fortune, American Survival Guide or similar for a plethora of such items.

Another excellent technique is to develop the need for a cane. Canes are not only useful for dealing with gangs but also with feral animals, and they help prevent falls. Canes can be outfitted with knives, electric shock circuitry, zip gun mechanisms, etc. Of course, those kinds of conversion could land you in jail, and they are costly and not always reliable or easy to use. What I prefer is to use is a golf putter - with a heavy head - as my "cane". I put some heatshrink tubing (available from electronic parts stores) on the top of the handle and pressed on a rubber chair tip. I use the head as the handle. It looks attractive, and is 100% legal everywhere.

If you are confronted by someone asking for money, quickly look the person over. Your average bum will look grungy and usually not threatening. You can either respond negatively or throw him a little pocket change. Throwing some pocket change is always a good idea, as it avoids a real confrontation. If the person appears to be threatening or a group is "asking" you for money, then you are probably about to be mugged if you don't have enough to offer. The way out if circumstances prevented you from carrying a weapon is to offer up a fake wallet with a minimal amount of sucker cash ($1 bills) as a "this is all I got" routine. Keep the other money and documents hidden on your person. If you have a weapon, the choice is up to you.

If you are seriously considering fighting back in an urban environment, make sure your skills are finely honed. You want maximum performance and precision when you get into a quick street fight. Most of the muggers are experienced and prepared for almost any reaction, and going out there without a high skill level could get you killed. Practice combat shooting, improvised weapons and unarmed combat. Act quick, strike hard, and leave.



TRIPWIRE: Tripwires are commonly used for burglar alarms, booby traps, perimeter alarms and tamperproofing (attach line to the protected object). When the fishing line is pulled, the wedge is pulled out, activating the circuit. You can make the circuit as simple or complex as you wish. A simple circuit would be one in which the wedge interrupts a line going from a 12 volt battery to a 12 volt buzzer. (A) Normally-Opened (NO) Configuration. Wedge is made of an insulator (ex: wood, plastic). When the wedge is pulled out, electric contact is made resulting in a closed circuit. (B) Normally-Closed (NC) Configuration. Wedge is made of a conductor (ex: NO wedge wrapped in aluminum foil, copper). When the wedge is removed, the stop prevents contact from being made and open-circuit condition result.

Living Free in the City: When it comes to disappearing and living out of the system, the city offers as many opportunities as the country. The starting point is to get the three basic essentials: Food, Shelter and Clothing.

There are three basic sources of food in the city. The first and easiest is to go to the soup kitchens that many philanthropic organizations run to provide a hot meal to the homeless. The Salvation Army and churches are good sources. The second is the fine art of Dumpster Diving - popular during the Great Depression. Many restaurants and food stores throw out perfectly good food, which is free for the picking. You will have to compete with other transients though, and you'll have to be careful in what you select. You don't want a case of food poisoning. Probably the safest thing to get from dumpsters is bread. When bread gets over 2 days old, it usually gets thrown out and is still safe and nutritious. Also sealed products with an expiration date are still perfectly good, and often suffer the same fate because they aren't "fresh". One trick that has been used with success is to call a place which does phone-in take out orders, and place an order with an assumed name and a phone number that's always busy or doesn't answer. The food is usually then thrown away when the nonexistent party doesn't pick it up. The problem with that trick is that it can only be used once in a while. The third sources of food is from hunting, foraging and agriculture. There are several urban dwelling animals such as squirrels which make good eating. Use an air rifle, sling, shot, trap or other silent means to bag them. Most cities are plagued with pigeons. People pay thousands of dollars to hunt dove, and a pigeon is nothing but a big dove. Often, they'll walk right up to you. Grab one by the neck, chuck him in a bag and take off. Their young (squabs) and eggs are also excellent. They usually nest in high buildings, bridges, etc.

Water is usually easier to get. You can stock up from public water fountains in stores and shopping malls. You can also tap into the city's water system at your usual place, and you can collect rain water. Distilling and boiling rain water would be a good idea. The public water supply is chlorinated and is usually all right.

For those looking for a quick place to live temporarily, there are plenty of "homeless shelters" available in any city which allow a roof over your head without having to resort to living in a cardboard box. However, they aren't exactly perfect for stockpiling, or conducting any sort of survivalist operation out of. They allow short term living, and altho they charge a minimal amount, the facilities are better and much safer than a shelter, and you can often go in there just to wash up for no charge.

A major problem with living in abandoned buildings are street gangs. Typically, they go building-to-building and room-to-room to rob, rape and pillage. Be prepared to flee or fight if so threatened. A good practice is to securely hide all of your valuables, leaving nothing worth stealing from your living area. Then disappear during the time that the gang is going thru your area.

Clothing is fairly easy to get, and very necessary to maintain a high living standard. Good used clothing can be had for free or nearly free at thrift shops, and via the Salvation Army and Goodwill. You can bargain with these people for even cheaper prices. Having a good set of clothing will make it easier to find a job, which is useful for you to buy the stuff you can't scrounge.

Looking thru dumpsters and garbage cans can net you some useful stuff. You'd be surprised at what people throw away.

SELF DEFENSE/OFFENSE

"A well-regulated militia being necessary to the security of a free state, the right of the people to keep and bear arms shall not be infringed" - U.S. CONSTITUTION, 2nd. Amendment

According to the Department of Justice, a violent crime is committed once every few minutes. Every 60-120 seconds, someone in the U.S. is murdered, raped or assaulted. Add to this fact that most of the subhuman scum that commit these heinous crimes usually aren't arrested, and if arrested, they are usually not charged, and if charged, they are usually plea-bargained and are never tried, and if tried, they are some times acquitted, and if convicted, they are usually given a light sentence, and if imprisoned, they are usually paroled long before their time or their victims recovery. I doubt if even 5% of all violent crimes result in the criminal serving a sentence anywhere near what he deserves.

This means several things: First, justice is obviously not served. Second, the threat of punishment is so remote that it is not a deterrent. Third, our streets, particularly in the urban areas that criminals prefer, are dangerous - often too dangerous for decent people to live.

A classic example of this is El Paso, TX. Most communities in Texas believe that the best way to fight crime and keep down jail populations at the same time is to put criminals on buses to the most distant parts of Texas - El Paso. It is a fact that out of every 7 paroled criminals found in El Paso, only one is from a jail in El Paso County. In fact, it is a very common practice these days of getting rid of criminals and mental defects by putting them on buses (and planes) to somewhere else with one-way tickets. In fact, a duel has resulted between Miami and Los Angeles. Each one now routinely sends its criminals and mental defects to each other's cities. It's gotten so bad that often when one arrives in one city, just the minute he is spotted in the bus terminal, they buy him a one-way ticket and send him right back. It's much cheaper than jail/ court/prison. It's also the reason why I very seldom take buses.

More self-defense information is found in the Urban Survival chapter. When considering the concept of "self-defense", you must take into account the fact that the "government" takes a dim view of citizens who take measures to protect themselves. Most states have laws against the carrying of protective weaponry. Personally, I feel that when law-abiding citizens are disarmed and violent criminals are set free, the time is right to take a close look at the way the government is working as some thing is obviously wrong. Of course, I don't recommend that anyone break any laws, but many people think and this author agrees, that IT'S BETTER TO BE JUDGED BY 12 THAN BURIED BY 6!

Before I delve any further into this topic, let me warn the more "sensitive" readers that they may be offended by the very frank nature of this discussion. Saving your life and those of your loved ones is very serious business, and should be treated as such. When your life is at stake, there are no rules. What counts is whatever works. This info has only one purpose - the quick and efficient stopping of an attack. I cannot stress enough that this information should only be used in a life- or limb-threatening situation, and then wisely.

Among certain circles, there is much talk of self-defense techniques which are able to be used by untrained, unarmed people and offer wonderfully effective results against attackers. These techniques are of minimal, if any, value in a truly dangerous situation, and are primarily extolled by liberal types who abhor the idea of violence to even defend themselves, but want to have some peace of mind.

Martial arts training is really the absolute last resort tactic that should be used to defend yourself. And even the greatest hand-to-hand combat abilities does not substitute for a weapon and just plain street smarts. For example, a third-degree Karate blackbelt was accosted by twos muggers on a New York subway platform. While one diverted his attention, the other got behind him and shoved an ice pick into his kidney. He died within minutes - his decades of training wasted.

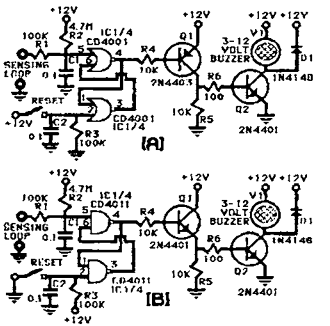
To be able to effectively defend yourself, you must at least have some training in the art of anti-personnel warfare, or as it is more informally called, "the art of doing others in". If that idea offends you, then you're reading the wrong book. Try "Lady's Home Journal" instead.

The two key concepts in defending yourself are to use any available means to aid you and to attack your aggressor in the most effective manner possible. While this offensive (tactically speaking) policy is opposite of what many martial arts schools teach, it is the best policy. By attacking rather than defending yourself, you remove an attitudinal disadvantage to yourself and give one to your attacker. Your attacker is looking for a frightened and submissive target. Attacks directed at him will not only catch him off guard, but make him wonder if you're worth the effort to tangle with at all.

If you are attacked by a group, a quick and efficient attack that incapacitates the biggest/baddest member of the group will make the others think twice before they act against you. Also, an aggressive mood on your part will increase your confidence. By "getting mad", your body will release more adrenaline, which will give you an edge, and a better chance at survival. Of course we don't recommend mindless combat, but making it look mindless, and that you are crazy/disturbed/psychotic does help by adding to the effect.

THE RIGHT TACTICS

It is RIGHT to say that, in most cases, a violent criminal wants to rob or rape you *AND GET AWAY WITH IT.* Except in cases where the criminal is a mental case, the Number 1 concern of the criminal is to get away with his crime.



ALARM CIRCUITS: These neat burglar alarm circuits use one IC and are powered by 6-18 VDC. Sensing Loop to (A) is hooked-up to a Normally-Closed (NC) switch while (B) is hooked-up to a Normally-Opened (NO) switch. Note design differences (circuits are complements of each other). Both circuits are high-input impedance and thus conservative with battery power (quiescent currents in microamps), permit very long input leads and permit many NC/NO input circuits (all wired in parallel). The input capacitors, C1 and C2, are required for noise decoupling. If the alarm false triggers a lot and the problem is not due to an inadvertent open/short, then the input leads are probably acting like antennas, and you should increase the C1 and C2 values accordingly (up to about 1 uF max). The IC inputs to these circuits make great debouncers -something that comes in very handy when any switch must operate in a less-than-ideal environment. *OPERATION OF (A)*: The NC sensing loop puts a 0 at Pin 5 of IC1. This results in a 1 at Pin 4 and Pin 1, a 0 at Pin 3 and Pin 6 (Pin 2 is pegged to 0). The 1 at Pin 4 turns OFF Q1, thus Q2 is also OFF and the alarm doesn't sound. If the sensing loop breaks, R2 forces Pin 5 to 1, and thus Pin 4 to 0. The 0 at Pin 1 and Pin 2 causes Pin 3 and thus Pin 6 to go to 1. The 0 at Pin 4 turns ON Q1, which turns ON Q2 and the buzzer sounds. If the transgressor tries to reconnect the break, the buzzer remains ON because Pin 6 is latched at 1 forcing Pin 4 to 0. The Reset causes Pin 3, and thus Pin 6, to go to 0, and Pin 3 to go to 1, turning OFF the buzzer. *OPERATION OF (B):* The NO sensing loop puts a 1 at Pin 5 (IC1), thru R2, resulting in a 0 at Pin 4 and Pin 1 and a 1 at Pin 3 (Pin 2 is pegged to 1). The 0 at Pin 4 turns OFF Q1, Q2 and the buzzer as before. If the sensing loop shorts, 0 is put at Pin 5, forcing Pin 4 and thus Pin 1 to 1 and Pin 3 to 0 and Pin 6 to 0. The 1 at Pin 4 turns ON Q1, Q2 and the buzzer as before. If the transgressor tries to reconnect the break, the buzzer remains ON because Pin 6 is latched at 0. The Reset causes Pin 3, and thus Pin 6, to go to 1, and Pin 3 to go to 0, turning OFF the buzzer.

Mental cases are almost always clearly identifiable: Property is of little or no concern, the criminal has/had a close or intimate relationship with his intended victim, the criminal is experiencing drug withdrawal, or the criminal is hallucinating or spacing out. If the criminal is a mental case, it is usually best to resist as little as possible, and try very hard to create and take advantage of flight and fight opportunities. Altho most mental cases are somewhat unpredictable in their actions, all humans are habitual creatures in at least some respects, and many mental cases suffer from obsessive/ compulsive behavior and tics. By sensing the behavior patterns of the mental case, you can usually scheme your way into effective defenses.

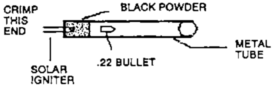
However, if the criminal is not a mental case (most cases), then you must vigorously resist his every attempt to isolate you to increase the chances that his crime won't be witnessed or reported:

(1) NEVER allow the criminal to take you to an isolated spot. You are much better off taking your chances in a public place than out in the desert or forest. When you resist, the criminal may then (try to) shoot or stab you, but if he does, he will likely try only a few very rushed times and then flee. However, once in a secluded spot, the criminal can leisurely tie you up and shoot/stab you many times and at point blank range.

(2) Resist the criminal as loudly and as rowdily as possible when he tries to isolate you. Resist all attempts to be tied up or gagged (where he can then physically force or take you to a secluded spot).

(3) If property is involved, give him all that he wants. Property can always be replaced - your life and health cannot.

SIMPLE IMPROVISED FIREARM



This weapon can be mounted on a pistol-shaped block of wood, or even strapped under your arm. Use a push-button switch and a 9-volt battery to set off the solar igniter.

(4) Try to talk the criminal out of his intentions. If he intends to rape you, you might tell him, "I have AIDS", or "I'm in my period." You might tell him, "My uncle is a bureau chief for the FBI." I've always taught my children to say. The important thing is to be firm - look the criminal straight in the eye. NEVER beg.

(5) Leave evidence. If you can tie your attacker to the crime - and he knows it - he'll be reluctant to risk a death sentence by killing you. Scratch his face, pull his hair, run into his car, yell out his name -anything that ties him to the crime.

(6) If he attacks you, attack back! For example, if he tries to strangle you, try to gouge out his eyeballs instead of trying to pull his hands off. Look for and create flight/fight opportunities.

UNARMED COMBAT

Rule Number #1 in unarmed combat is that if there is a weapon available use it. And if not, try anything to improvise a weapon - car keys, belt, pick comb, brick, rock, broken glass, pipe, board, stick, dirt - anything. Unarmed combat is generally considered the worst case combat scenario.

However, training to fight with nothing but your bare hands is very useful as you will have the peace of mind knowing that even if you are in a worst case situation, you at least have something to rely upon. One of the best styles of unarmed combat is the U.S. Marine Corps Hand-to-Hand Combat Course. The Marines teach a style which is quick-and-dirty but does the job. It works very well because, unlike the popular martial arts, the Marines teach only one thing: How to kill someone with your bare hands.

Despite media hype, most martial arts are somewhat unsuitable for serious combat, and the ones that are, usually take 10 or more years to master enough to be considered effective for combat. This is because of their defensive nature. Ignore media BS about how martial arts practitioners are mystically-trained combat machines with special psychic powers. In their PR efforts, most martial arts have toned-down the aggressiveness that prompted them to be developed in the first place.

However, there are still some martial arts which are combat oriented. One good example is Jujitsu. Jujitsu is a pragmatic style where all common martial arts techniques are taught, from punches and kicks, to takedowns, to pressure points. Another martial art which is very effective, altho defensive in nature is Akido. Akido's defensive concept lies in using an attacker's momentum against him to bring him down. While it isn't an offensive art, it still is very effective. There are probably many other martial arts suitable for no-nonsense combat. When looking for one make sure it covers a wide range of techniques, particularly pressure points and take downs (the primary method used in Akido), as these techniques produce the most effect with the least effort. The art should also emphasize a flexible response to fighting. Many don't. Finally the martial art should have an offensive philosophy rather than a defensive one.

No matter what style of unarmed (or armed for that matter) combat you choose, a general fitness training program to further develop your strength and agility is an often critical requirement. While one can develop your physical fitness by the martial art's training alone, a general supplement will enable one to advance quicker and with better results.

In a self-defense or offense situation it would be wise to attack these areas and protect them on your own person:

HEAD: There are several spots on the head which are worth going for. The first is the nose. Hit it with enough force and you'll break the tar get's nose and put him out of action (unless he's on PCP). Hit it even harder and you may kill him. Hitting is done by jamming the palm of your hand forcibly upward into the nose. The eyes are another excellent spot. You can blind your target and thus eliminate him as a threat and leave him open for a finishing blow. The best method is to forcibly poke him in the eyes, Three Stooges style, with your fingers, or to dig your fingers into his eyes to gouge them out. Or throw sand, boiling water, just about any spray, or some other substance into the eyes. Particularly if you are held in a bear hug, the ears are also vulnerable. The ears are attacked by cuffing your hands and then slamming them violently and simultaneously against the ears. The base of the skull is also another good target, if you can get at it. A forceful karate-chop blow can cause spinal injury and even death. An other vulnerable area is the temple. A karate-chop blow here can cause brain damage, hemorrhaging and even death. Finally there is the adam's apple area. A karate-chop blow here will collapse his windpipe, causing death, or at least stun him, enabling you to do something more effective.

SOLAR PLEXUS: A powerful enough blow here will stun your enemy.

GROIN: Suffice it to say that a knee, foot or fist here works very well. However, the groin is a small, well-protected area. One effective tactic is to fake a blow to the groin, then follow with a head or other blow.

STOMACH: This one will also stun your enemy.

FLOATING RIBS: A hit here can drive them into the kidney(s) and liver, causing great damage. Even if you don't kill him, he'll be on dialysis for life.

FINGERS: can be grabbed and twisted, causing sprains, dislocations and major pain.

ARM: If you can put your target in a hammerlock (where you have his arm twisted behind his back police style) feel free to keep twisting until his elbow is by the base of his neck. This will either break his arm or dislocate it. In any event it hurts like hell and will definitely put him out of action for the next month or forever, depending on what you do next.

KNEE: A powerful blow to the back of the knee will bring an enemy down very quickly. If in front, a powerful blow to the side of the knee has been known to dislocate it - besides bringing him down quickly, it hurts like hell.

FOOT: Slamming your foot down on someone's instep will quickly disable him. If you can't reach the instep, then go on top of the toes. How ever, with combat or steel-tipped boots, the feet may be only marginally vulnerable.

ARMED COMBAT

Before I discuss armed combat weaponry, let me state that a weapon is only as good as your training and experience using it. Most weapons require some practice in order to use them effectively. While this practice is easy to accomplish and not usually difficult or demanding, it is still needed. Without it, a weapon just encumbers your hand, and worse, it could be turned on you.

There are various types of effective melee weaponry which are easy to obtain or improvise, and are effectively used with little practice. Note that some of the weapons described herein may be illegal to possess, not to mention to use, in your area. Therefore, I advise you to discreetly check your area's laws or refer yourself to the 11th. Commandment, "Thou shall not get caught". Generally, weapons laws are much more lenient in the South, West (except California) and Southwest than they are elsewhere, so where you live can affect your, "right to defend yourself".

An interesting experience happened to a business associate and friend of mine who started their own business in New York State selling edged weaponry. To not break any laws, they contacted several law enforcement and judicial personnel to find out the laws regarding edged weaponry. Except for the obvious restrictions on switchblades, stilletos and the like, each person gave a different explanation of what was illegal. Even if the actual laws are consulted, the interpretation of them can change daily.

Usually, it's better not even to ask. The morale of a joke told by an Israeli comic underscores this. He was pulling into a parking area in Tel Aviv, when he spotted a policeman standing nearby. He called the policeman over and asked, "Can I park here?" The policeman responded, "No!". He then asked, "Well then why is it that these other cars are parked here?" The policeman chimed, "They never asked."

SURVIVAL & COMBAT KNIVES

The cutting edge is one of man's earliest tools and has withstood the ultimate test of time by not having been replaced by anything better for its purpose. Of course, there have been many enhancements made since early man wielded a piece of sharpened flint. Generally speaking, the best knives used for survival and combat are the ones issued by the various military forces of the world. They are also the least expensive to obtain. There are also commercially made knives which are up to these standards and are even unofficially used by the world's military forces.

One of the major complaints I've heard is that combat and survival knives are expensive. While this is true, particularly of the Gerber and Cold Steel line, the product you are buying is very high quality, rugged, and will last a lifetime if properly cared for. Unless you lose or destroy them, a set of knives is a one-time purchase that you will probably hand down to your descendants.

There are several inexpensive civilian knife brands which are just as good as the expensive military style stuff, and look less noticeable hanging from your belt. From my experiences, I have found that I get less stares from people when I have a Buck sheath knife hanging from my belt than I get when my Cold Steel Tanto or Gerber BMF is in the same place. They also have a less threatening image which can make life easier in many respects.

There are several civilian brands which offer good quality sheath and folding knives. They are, but not limited to, Camillus, Schrade, Buck, Frost, Kershaw, Parker-Eagle, Ka-Bar, Ontario, and Solingen. Camillus, Ka-Bar, and Ontario also make knives for the U.S. military, discussed later. The top price you would expect to pay for a sheath knife or large folding lockblade from these companies is $40-$50. Smaller lockblades and pocket knives are less, top price averaging between $40-$60.

A serviceable knife can be had at a reasonable price from any department store and is probably in your own home. These are kitchen knife sets which are used for preparing meals. They are designed to cut thru thick flesh and bone and would make a suitable combat knife in a pinch. Some also have a fearsome appearance, which helps you win battles without even fighting. While not as rugged as a knife designed for the purpose, a good kitchen knife, preferable a large (8") butcher knife would at least work until better equipment is available or the job is completed.

Some of the most functional combat knives come from a company called Cold Steel. Cold Steel made their debut when they introduced a series of push daggers for combat use. These two weapons were called The Urban Pal and The Urban Skinner. These knives featured a special metal grinding technique which made them nearly indestructible. Since then they also released another push dagger called The Terminator, which is even more combat-oriented than their others, featuring a longer double-edged blade. They then introduced a modern version of the Japanese Tanto Dagger in various variations.

All of Cold Steel's knives are razor sharp, and in my several months of regularly using my Tanto, the edge never dulled. They also make a folding version of the Tanto called the Shinobu. Both the Tantos and Shino bus come in various sizes with the Tanto available in an all stainless steel version called the Special Ops Tanto (the other ones use brass for the guard and pommel), and a non-reflective finish version called the Recon Tanto.

Available as standard equipment with the Special Ops Tanto, and as an option on the other standard sized models, is a Kydex plastic quick-draw sheath. This is a friction fit sheath designed to be easier to wear, and quicker to draw a knife from. From my experiences with this sheath I found while it may be easier to attach to a belt or web equipment, it required some amount of force to pull out the knife, and the knife could not be pulled out slowly, but rather wrenched from the sheath. Because of this, the act of drawing the knife was clumsy, leading to the potential of accidentally cutting oneself or otherwise losing control of the knife. I also determined that the time it took to yank the knife from the quick-draw sheath was the same as the time it took to undo the velcro retaining strap and draw the knife from the standard sheath. Drawing from the standard sheath also allows for more control and safety. The retail cost of the quick draw sheath is about $20, which I feel could be better spent elsewhere.

With the exception of the quick-draw sheath, all of Cold Steel's products represent a good value for the price. The Urban Pal, Urban Skinner and Terminator are designed for easy concealment for a combat situation, and function admirably in that role. The Tanto is also primarily designed for combat, but is rugged enough to use as a very good utility knife. The Outdoorsman, Trailmaster and Clipmate are very good general-purpose blades.

Gerber Legendary Blades is one of the older makers of combat/survival knives. Their Mark II sheath knife was the edged weapon of choice for many servicemen in the Vietnam War. Gerber makes a wide range of knives, ranging from lockback folders to small concealable "boot knives", to sheath knives such as the Mark and Guardian series, to their large BMF and LMF series bowie knives. Within each series of knives Gerber makes, they offer different options such as single/double edged blades, different blade styles, sawteeth on the back of the blade, etc, for the varying individual tastes. Gerber knives are, in my opinion, a better value for the dollar than Cold Steel as Gerber knives are more suited for a wider variety of tasks than are Cold Steel's. I personally carry a Gerber Command II, which is the larger (7" blade) discontinued version of the Command I as well as the small Guardian, and can attest to their quality.

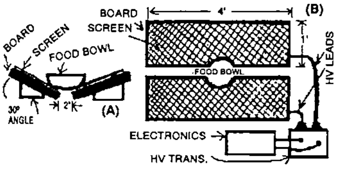
For sheath knives, there are their Guardian, Mark, and Command series. These are basically the same knives in different designs and blade lengths/styles. The Mark I and Mark II are the original Gerber design from the Vietnam War. Both are double-edged, with the current Mark II having a "wasp waisted" blade with serrations near the hilt. The blade lengths are 6-1/2" for the Mark II, and 5" for the Mark I. The Guardian series are the later version of the Mark series. There are three different varieties - each having a double-edged blade. The knife known as the Guardian is a small easily concealable knife with a 3-3/8" blade (7-1/4" overall length). Their large version is the Guardian II with a 7" blade. The Guardian and Guardian II are also sold in a camouflage version, as well as the standard black.

The standard issue combat knife for the U.S. Marine Corps is a 12" long bowie knife with a 7" blade and a black finish. The hilt and sheath are made of leather which is chemically treated to resist moisture and its related effects. This has been the standard issue knife for the U.S.M.C. since before World War II. The Marine Corps bowie knife is suitable for both combat and survival. Earlier versions of the knife were made by Ka-Bar and are collectors items, altho Ka-Bar makes a functional reproduction of the original knife. Current knives are made by either Ontario or Camillus. The quality is the same between the two brands. This is a good knife and was my first blade.

One old design is the British Commando dagger made by Sheffield. This is a one-piece steel, slender, black double-edged knife with a 6" blade. This knife presents a very slim profile and could be concealed very easily. It is designed as a combat knife, specifically for thrusting. There fore, the blade itself isn't too sharp and it makes a mediocre general-purpose/survival knife. However, it is well suited for its intended combat role. Just don't try to slit the enemy's throat with it.

For raw shock power at a reasonable price, your best bet is a Gurkha Kukri. This is a large combat knife that verges on being a sword. It was originated by and is today the mainstay of Great Britian's legendary Indian Gurkha Troops. Traditionally, these blades are never re-sheathed without drawing blood. In fact, each one has a blood-letting notch that permits the bearer to honorably re-sheath his knife without having to kill somebody/something first. Granted, if you can carry one concealed and pull it on a mugger, you will likely not have to use it - even if you aren't Crocodile Dundee. The only way to describe this knife is wicked and definitely no-nonsense.

Kukris come in two sizes. The sturdier officer's version is 17" long, has a 12" blade and weighs 25 oz. The enlisted man's version is 16" long, has a 11-3/4" blade and weighs 15 oz. The blade is curved forward and wasp-shaped, with the edge on the concave side. The knife is very well balanced, with the blade ideally designed and weighted for decapitation purposes. You can be effective even if you hit the target with minimal force or with a glancing blow - the momentum of the blade will do the rest. The Kukri is ideally used with slashing/chopping motions (altho it also thrusts very well), and is probably one of the easiest knives to use with little training. A well placed shot with a sharp Kukri will easily take off someone's head or limb. Clearly, the Kukri is best suited for combat -particularly slashing and chopping - and as a general utility tool like a hatchet, cleaver or machete. Several companies (including Cold Steel) are marketing modernized versions of this fine blade.



RODENT ZAPPER: This is an easy way to take care of rodents, other marauding or dangerous small animals, and small game. It draws very little current except when electrocuting. (A) is the end view. (B) is the top view. Place trough on level ground but elevate electronics and HV transformer. Don't use in wet weather, and limit current drawn by the transformer.

KNIFE FIGHTING

More than anything else, your ability to win a knife fight depends upon your quickness, agility, deception, reach, hand and arm strength, and the type of knife that you use. Since knife fights are usually short-lived, endurance plays a critical part mostly in military operations. Clearly, much practice and experience are required.

You should NOT be overly carried away by knife sizes. Altho knife size and combat effectiveness are directly related because size directly relates to reach, if the knife is too large or heavy for the bearer to properly handle and can be parried or bypassed by the opponent, then the large size is self-defeating. Also note that combat knife fights usually occur in the worse conditions: The surface is slippery, muddy, rocky, brushy, unlevel and-or unstable, and-or you are in a confined area. If your knife is unwieldly, your chances of slipping and mishitting are much greater. And since quickness is the most decisive factor in knife fights, it is usually better to be faster with a smaller knife.

The types of motions used with a knife in fighting depend upon the size, shape and balance of the knife. Limited knives, like the British commando dagger, are effective in thrusting or stabbing motions only. How ever, most other knives can be used for slashing as well. And some, like the Kukri, can chop. In virtually all cases, the knife is held so that the blade faces forward (and not where it faces behind as in the horror movies) and the edge faces down. This is because, when the blade faces forward edge down, you have much more mobility and versatility with it, and that creates uncertainty in the mind of your opponent. The knife should also be held only moderately firmly in the hand - about as hard as a tennis racket - if you hold it tighter, your hand and wrist muscles will freeze up.

When your opponent approaches, the knife is held behind the lower back, and is returned there whenever the opponent is at least a couple of steps away. This is done so that the opponent can only guess how you are holding the knife, giving you the advantage of surprise. If your opponent doesn't know you or you are known to be effective with both hands, then both hands should be behind the back at those times. The opponent then has to guess which hand will come up with the knife. Flash the empty hand first - he'll be forced to respond to it and be distracted - then quickly follow thru with a thrust/slash/chop with the bladed hand.

Club-Type Weapons: When early man decided to do in one of his neighbors, he probably picked up a stick or rock to help him and thus the club was born. There are many varieties of the club around and all work on the same principle - using blunt trauma to cause injury. Strangely, clubs are considered "non-lethal" weaponry, probably due to the fact that they are used in riot situations by the police when people are to be controlled with the least amount of injury, and the fact that their use often doesn't draw blood. The truth is, if you hit someone in the right place with a modern aluminum or polycarbonate nightstick, you stand a good chance of severely injuring or killing him. Even if you're using an older style hardwood nightstick, he'll FEEL it when you break it over his head.

Nightsticks and billy clubs are the classic club-type weapon - proven by the fact that most police departments still use them. The difference between them is that billy clubs are about a foot long while nightsticks are about two feet long. They are made from a variety of materials: Wood, polycarbonate and aluminum are most common.

A step up from the nightstick is the Tonfa. Formerly a martial arts weapon, the tonfa is now commonly used by police and security personnel, and is slowly replacing the nightstick. A tonfa is about as long as a nightstick, but has a handle extending perpendicular from the main stick about a third of the way down. This enables the device to be held in a more natural position and also opens it up for a more defensive role than a nightclub. The standard police tonfa is the Monadnock PR-24S. This is a 24" long tonfa made of polycarbonate plastic and is virtually indestructible (it comes with an unconditional guarantee against breakage). Monadnock also makes an aluminum version of the PR-24S. The tonfa is a much superior weapon than the standard nightstick. The perpendicular handle enables one to accomplish all sorts of defensive and offensive maneuvers that aren't possible with a nightstick. The tonfa is also, when practiced with, faster to deploy than a nightstick.

The yawara or kubotan is a small stick which fits in the hand with the ends sticking out. It has been very popular as a "keychain defense weapon". It's very easily made, yet very effective. However, it does require some training to use effectively. The kubotan is designed as a stealth/ quick reaction weapon for use against pressure points and other vulnerable areas of the body. To use a kubotan properly, you must take the offensive, quickly bringing the kubotan into play and attacking the attacker, and preferably hitting him in a pressure point. When used like this, the kubotan is very effective. The problem is that most of the people who carry one don't know how to use it properly, and thus the weapon loses it's effectiveness. I recommend carrying a kubotan as a back-up weapon. If you decide to do so, learn how to use it.

The de-facto club weapon in the middle-ages was the quarterstaff. It still remains one of the most effective melee weapons today. This is a wooden staff, usually made of oak or some other tough hardwood, about 6 feet or so long. For added stopping power, the ends are usually drilled out, filled with lead and wrapped in wire and black tape. Of all the club-type weapons the quarterstaff has the longest reach, and is the easiest to improvise. It is also a quick weapon when practiced with and is quite capable of taking someone out very efficiently. It's one major disadvantage is its length. It cannot be concealed or used in crowded/enclosed areas, as one needs the room to swing it around. However, there are no laws against carrying a 6 foot long "walking stick".

An example of an overrated weapon is the sap or blackjack. This is a type of beanbag filled with some type of weight, usually lead shot. There are many variations ranging from strips of leather sewn together and filled with lead to a sock full of quarters. Despite it's infamous reputation, it's an offensive first-strike weapon, the attack of which is usually limited to the back of the head, kneecaps or temples, depending upon what's open. The most disabling is the head shot. Blackjacks/saps are easy and inexpensive to improvise.

More effective than the standard sap are sap gloves, which are leather gloves with lead sewn into the knuckle area. The effect is similar to brass knuckles but is more easily concealed.

A favorite weapon of the Ninja of ancient Japan was the Manriki-Gusari. This was a length of chain about 3 feet long, with weights on both ends. This weapon was easily concealed, versatile and very effective. Besides its obvious offensive uses, it was used in defense against swords and as an entangling weapon. It is also very easy to make from commonly available materials. It also can be used as a blackjack/sap but is more versatile and powerful.

Another Ninja favorite was the Nunchaku. This device consists of two hardwood clubs or lead pipes connected together by a short length of rope of chain. One club is grasped and swung around, allowing the other one to move freely and gain momentum. The Nunchaku can be deployed with great speed, confusing an enemy. It also packs a severe punch, due to the centrifugal force resulting when the free end swings around at high speeds. The free end of a pair of Nunchaku hits with up to 1600 lbs of force at its impact point. The Nunchaku requires consider able practice to master; a heavily-padded version is used for practices.

Swords: For times when you can engage in out-and-out brazen melee combat in the open, the choice may be the sword. Under these circumstances, its large size is of less disadvantage. Of all the melee weapons discussed, none have the visual impact that a sword has, particularly an exotic-shaped one. Most swords made today are purely for decorative and ornamental purposes, made of cheap metal and lack a decent cutting edge. However, if you look around, there are still some modern-made swords which can be used as weapons. The two I like most are the Samurai sword and the machete.

A Machete is a small sword about 2 feet long. Its primary purpose is to hack thru dense foliage and to chop wood, etc, and is popular in Latin and South America. The machete also functions well as an inexpensive and rugged combat weapon, and as a handy garden and camp tool. Strangely, most people don't feel as threatened by a machete lying around (or an axe for that matter) as they do by a hunting knife, as most people regard the machete more as a tool than a weapon. If you are serious about combat and survival machete uses, stay away from the el cheapo K-Mart varieties with the fragile plastic handles and sheet metal blades, and buy a real one from military surplus or a cutlery dealer.

Garrotes: A garrote is a highly-specialized weapon used to kill sentries. It consists of a 2' to 2-1/2' length of strong thin wire (ex: piano wire), leather cord, chain or other material. This wire is quietly dropped over the target's neck and quickly tightened. The result is either strangulation or decapitation depending upon the material and method used.

Once one probes further for info about the garrote, things become hazy. Altho many people swear by them, there is not much hard data on garrotes. Most of what you hear about them are anecdotes picked up from combat vets, or movie accounts. The advantages that garrotes have over knives are: The target's silence is almost assured, you don't have to worry about body armor, and the garrote is very easy to improvise, carry and conceal. Its disadvantage is that your target may hear you and turn around and shoot you before you get the chance to use it on him.

There are several ways I have been told to use a garrote. The first involves the strangle variety: Cross your arms, drop the cord over the target's head and twist it to tighten it. The decapitation variety can also be used in this manner, but instead of twisting the wire, you just pull the wire hard. You can also drop the cord over the target's head and then turn around, going under your crossed arm, and lift the target up on your back. It appears that the piano-wire variety is the more effective, as strangling someone takes at least 3 minutes. And even if you don't decapitate the person, you will still probably slit his throat, accomplishing the same thing.

IMPROVISED WEAPONS

Improvised weaponry of all kinds can be made from just about anything:

1. Any awl or icepick can be devastating when used against a vital area. One can also use a long, sharpened nail to the same effect. A common trick is to take a ball point pen, like a Bic or Papermate, remove the guts and use epoxy to cement the business end of an awl, compass point or sharpened nail in it. The result will be an effective stabbing implement that looks like a pen until it is brought into use. Screwdrivers can also be sharpened, or even left unsharpened, for much of the same effect. The world is full of sharp implements: Scissors, knives, cutters,...
2. An improvised Manriki-Gusari can be made from a piece of chain and two heavy fishing weights. Attach the fishing weights to an end of the chain.
3. Kubotans can be improvised out of any piece of hardwood or metal which fits into your hand and sticks out 1/2" - 1" on each side of your fist.
4. Circular saw blades can be thrown with nasty effect like giant Chinese stars. But protect your hands first.
5. Garden implements, such as hedge clippers (electric or manual), hoes, shovels, rakes, etc, can be used as effective weapons. Manual garden shears can be unbolted to provide a pair of small swords or large knives depending upon size. Other common tools make great weapons: Chainsaws, axes, hatchets, hammers, handles,... Even a power drill can be swung by its cord in a pinch.
6. As a rule, anything that looks fearsome and wicked enough can often be used to discourage an attack, altho it is a wise idea to brandish some thing that is effective if you have to use it.

The above list is just a small sample of the great numbers of improvised weaponry available to you if you use your imagination. Unless you're in empty room, there will be something there which can be used as a weapon. Get in the habit of looking, because one day you may be surprised by an armed intruder in your home or business and you will have to react in warp speed.

REMOTE WEAPONS

The best weapon for defending yourself is a gun. With a gun, you have the edge over anyone trained with any other weapon in unarmed combat, provided you are far enough away. And you have at least an even chance against someone armed with a gun, provided you know how to use yours.

However, there is one exception. If you are highly trained in hand-to-hand combat, exceedingly quick and close enough to your attacker to reach him or his gun, then you may feel that you could succeed in resolving the threat with a quick action. The decision is yours. If you do so and the attacker has a gun with an exposed hammer, a common tactic is to run your hand along the top of the gun and then jam the webbing of your hand between the hammer and the frame, thus preventing the attacker from shooting you. You'll likely lose some skin but you'll also save your life if you succeed.

Black Powder Guns: There are several alternatives to modern guns. The best is probably black powder firearms. While not having the firepower or ease of reloading that more modern guns have, the advantage of black powder weaponry is that the laws regarding them are more relaxed while they are just as lethal as modern guns. There is quite a variety of black powder guns available, ranging from very accurate Kentucky long rifles, to shotguns, to concealable black powder revolvers which feature 6-shot capacity (as many as a revolver). For those into home-brew weaponry, black powder guns are easier and safer to make as there is less stress involved when a black powder charge is fired as opposed to conventional smokeless powder.

Airguns: Another good alternative to conventional guns are airguns. Despite their reputations of being "kids toys", there are many modern airguns that are quite powerful. I once got shot in the side with a "standard" single-pump, spring-fired .177 cal. Daisy BB gun. I was wearing a t-shirt, and I was hit from about 100 feet away. It stung quite badly for a half hour, and my previous fighting mood was remarkably changed. There was also the story, printed in a survival magazine, of a woman who was ALMOST assaulted in her home. She prevented the assault by grabbing a full-automatic BB gun, the only "gun" that she knew how to use, and showered (literally) her attacker with 1000s of BBs as he came towards her. The attacker spent a long time in intensive care recovering before he was well enough to stand trial.

There are also several kid's toys that fire ping pong balls. With these, or any air gun that fires a large projectile or water the projectile can be modified to carry explosives and-or other chemicals.

Bows: Besides guns, there is also one remote weapon used extensively by sportsmen and often by military special operations units, but generally ignored by everyone else. This device is the simple bow and arrow. Of particular interest to the survivalist/freedom fighter are the compound bow and crossbow. Each has enough power to down a deer with one shot, so they are adequate to use against humans. They are fairly silent - why they are used in special operations by the military and intelligence agencies. They are also legal, except in major cities where everything is illegal or regulated. I know of no area that has any restrictions regarding possession of a bow.

When choosing a bow for survival/defense use, get a bow with at least a 50-pound pull. In most states, this is the minimum pull weight allowed for hunting. Anything less is only good for target practice. I prefer the compound bow to the longbow because the pulley arrangement permits greater power with a lesser difficulty in pulling back the bowstring (ex: a 75-pound pull bow would only have a 50-pound apparent pull). If you have difficulty pulling back a conventional compound bow, then select a crossbow, preferred by the military for their operations.

When choosing arrows for your bow, get the hunting points. These have multi-edged razors on them and are designed to produce maximum trauma. One of these can take down a deer when hit in the right spot. I'd hate to see what they'd do to a human. Note that when nocked in a bow, hunting arrowheads are vertically oriented because the ribs on animals are vertical, so the arrow can slip between the ribs for penetration into the vitals. A human's ribs are horizontal, so the orientation of the arrowheads should be horizontal for anti-personnel uses.

In the "Rambo" movies, Stallone used exploding arrowheads. While it is virtually impossible to make an arrowhead with the explosive power shown in the movies, a lesser powered version has been made before, and is easily made. Take a hollow aluminum arrow and remove the arrow head. If hollow aluminum arrows are unavailable, a thin length of aluminum or other metal tubing with vanes attached to one end will also do. Fill the arrow with FFF black powder, tamp and replace the arrow-head with a primer cap.

Flare Guns: Flare guns are commonly used in James Bond movies, as well as on TV. While not very accurate, they are accurate enough at close ranges, fire a very large incendiary round and have no or few restrictions with their sale or possession. There are many different configurations, ranging from the classic break-open pistol design, to a pen design, to a one-shot tube. The best unit for survival/defense purposes is the pistol design. It fires the most powerful flare cartridges and is in a pistol design to make its use easier. A flare pistol also has other uses. Besides signaling, you can use it to set flammable material aflame from a distance. It also has a psychological shock-value when used to defend yourself. Imagine what would go thru a mugger's mind when a potential victim shoots a "fireball" across his path. Even if it doesn't terrify him altogether, he should be stopped in his tracks long enough for you to reload and nail him with the second shot.

Other Distance Weapons: While primarily a "distraction" weapon, blowguns are silent and can be used with poisoned darts as an effective weapon. The same holds true for regular throwing darts. Blowguns can be made out of any type of tubing from a soda straw to a length of thin copper pipe. Range and power depend upon ammo used, tube length and tube inner-wall smoothness (that's why it's much better to get a commercial model). As with any dart, bow or throwing weapon, poisoning the tip optimizes weapons properties. Slingshots can also be used as an effective distraction weapon, with the more powerful "wrist rocket" models somewhat more dangerous. One can also fire cherry-bombs or a similar explosive device with them for an added distraction. Spear guns are one of those exotic weapons that are 100% legal when kept or used as intended. Used on an intruder, they tend to cause an embarrassing amount of blood, gore and screaming. Spears can be made from many common items. If you live near a recreational water area, you can buy gig points, and easily secure them to a wooden broom handle. Else, you can cement/solder/weld/braze/tape/wire any sharp point to any wood/plastic/metal shaft of appropriate length.

FIREARMS

Many folks live in urban and suburban environments, and even after the "shit hits the fan", many will choose to survive in their familiar surroundings. Even many of those who plan to "head for the hills" will find themselves trapped in place because of gridlock when the panic sets in. Unless you live next to a primary nuclear target, a toxic waste dump or a gang- infested area, you should plan to survive "the day after" right where you live - even if on only a Plan B basis.

And as dangerous as cities and suburbs have become, surviving BEFORE the shit hits the fan is much more of a problem today than it ever was. The truth is that many of our cities are self-destructing before our eyes, and chances are that most of them will launch into chaos without ever having been "attacked" by anyone.

There are several different types of guns to be considered. This diversity often causes confusion when a person with a limited budget tries to buy the one gun that will serve all of his needs. Unfortunately, no one gun is capable of handling every situation. That is why the professionals (ex: Military Special Operations and police SWAT teams) have each member carry a different gun. This is to enable the team to handle many different situations on the spot and still not be bogged down with four or five guns per man. You will seldom see the SWAT guy with the sniper rifle kick down the door or the SWAT guy with the shotgun or SMG (sub-machine gun) up on the roof across the street. Each weapon serves a certain functional span well, and is mediocre - even dangerous - for all others.

AMMUNITION

There are several types of ammo which can improve the effectiveness of gun usage, as the gun optimizes the stopping power or penetration of ammo optimally suited for it, and the design of the ammo itself can optimize these factors. Penetration is easily measured. "Stopping Power" is defined as the capability of the ammo to stop the action of whatever it is shot into, to some extent an ethereal property.

For people with body armor or behind armor, stopping power and penetration are directly related. For unprotected people, stopping power and penetration are inversely related because even a .22 cal. bullet will frequently completely pass thru the body part. For unprotected people, blunt trauma usually stops better than penetration: Low-speed, high-crossection bullets have much greater stopping power than high-speed, low-crossection bullets. For example, a slow .45 ACP bullet has greater stopping power than a zippy .357 magnum bullet for an unprotected human. The opposite is true for bear and human targets with body armor.

Stopping power levels off at the bigger calibres. For example, a .44 magnum has little more close range stopping power against an unprotected person as does the much less powerful .45 ACP. If an attacker is hit by either of these bullets at close range in the head, torso or limbs, the attack will stop, so the stopping powers are closely equal.

The .44 magnum has much greater penetration and range, and thus stopping power at a distance and against protected targets. However, most handgun uses occur within 100 feet of an unprotected target. Also, regarding magnum rounds: They are little better than standard rounds in handguns with barrels shorter than 5 inches as the powder requires a barrel of at least 6 inches to become mostly burned (8-12 inches preferred). Therefore, don't buy a 4-inch .44 magnum.

For .22 cal. long rifle ammo there are hyper-velocity slugs in both solid and hollow point configuration. The most commonly known brands are CCI Stingers, which are hyper-velocity hollow points and far more effective than standard .22 ammo. Besides CCI, both Winchester and Remington make their own brand of hyper-velocity ammo. Remington makes hyper-velocity ammo in both solid (Viper) and hollow point (Yellow Jacket). For an effective comparison of hyper-velocity to regular ammo, use a tin can or apple for a target, fire some standard .22LR into it and then fire some CCI Stingers. You'll see a big difference. Some weapons, particularity the Ruger 10/22, function better with hyper- velocity ammo for some reason.

"Arcane" ammo were brought to my attention by a friend of mine. I haven't shot arcane ammo yet, but the concept behind their design seems valid. An arcane round is made by taking a standard solid-point round, and filing the tip to a 70 degree cone. When done on rounds larger than .30 cal., the round creates a shock-wave in front of it when fired. This much increase blunt trauma.

Explosive bullets are easy to make, but matching explosives with bullets is a dangerous task to attempt. This type of ammo should only be used in revolvers as using them in an automatics could cause the gun to jam, exploding the ammo prematurely, and the extreme set-back force of rifle ammo doesn't agree well with the impact explosives used in exploding ammo. A safer, less powerful version of exploding ammo can be made by drilling a hole in a standard round, putting a drop of mercury in the hole, and topping it with a primer cap. When the bullet hits, the inertia makes the mercury slam into the primer cap, setting it off.

"Regular" exploding bullets are made by simply filling the drilled hole with an impact-sensitive explosive, and sealing the tip with wax. These are also a lot more dangerous than the first kind. When properly made, an exploding bullet will detonate just after it hits it's target, exploding in the body, creating a large wound cavity and massive amounts of trauma. Improperly made exploding bullets will likely not explode or explode inside your gun, wrecking it if you're lucky (turning your hand/face/life into road kill if you're not).

Teflon-coated bullets, also known as KTWs, were outlawed years ago because of their ability to penetrate kevlar body armor. The way they work is that the teflon acts as a super lubricant and enables the bullet to slip thru the weave of the kevlar like a watermelon seed between your fingers. They also did a good job of ruining the barrel of the gun if too many were fired.

In my opinion, teflon bullets are unnecessary. If I find a target is wearing body armor, I just aim for a part of the body which isn't protected, such as the head. To make similar bullets, melt down the plastic from a child's toy or other plastic object, and coat the tip of the bullet with it. Another way is to spray Rustoleum Wood-Paint (which contains teflon), or pipe joint sealer containing teflon on the bullet's tip. Or cement on strips of teflon plumbing tape. Just don't blame me when you ruin your gun. Or coat the bullet with a thin layer of silicone rubber sealant.

One way that I know to be effective, is to cover the bullet with graphite. This can be done using a graphite lubricant, or by taking a soft lead pencil (#2 or #1) and heavily shading the bullet with it. Actually, graphite works about as good as teflon when it comes to penetrating kevlar.

The armor penetration ability of a gun's ammo can also be increased by simply using something other than lead for the bullets. Many types of hard metals will suffice. A quick and dirty way of doing this is to simply saw the head off of a case-hardened bolt, and replace the lead bullet with the bolt. Additionally, you may also want to file down the tip of the bolt so it resembles a bullet for greater accuracy, range and penetration. This technique is also used by unconventional warfare forces in improvised reloading'techniques. You can also drill a hole in a solid bullet, and put a BB on it. Not only does this help penetration, it also increases expansion of the slug when it hits a soft target (flesh).

Well-known in spy-novels are "ice rounds", which are used for assassinations. A person is shot and killed with an ice bullet, leaving no evidence, as the round simply melts away. While they do work, there are obvious limitations to their uses: They melt, to be effective they must be fired at near point-blank range, and they work well only in 12 or 10 gauge shotgun rounds. The latter is true because the heat and wind resulting from the firing quickly dissipates the bullet

To make an ice round, take a shotgun shell and remove the shot and some wadding. Put in some wax, rubber cement, shellac or vaseline for water proofing. Fill the rest of the round with water, and freeze. For added strength you could embed wool, hair, chicken bone or some other natural substance in the water before freezing. The same effect can also be had with rock salt, again loading a shell with it after removing the shot. Rock salt dissolves in the body as a saline solution, removing the evidence.

URBAN SCENARIOS

The urban scenario is the most difficult one to select guns for, due primarily to the wide variety of terrain encountered in an urban environment. Usually, in a rural environment, terrain variation is limited and thus it's easier to determine your gun needs. However, in an urban environment, you can encounter everything from wide open spaces, to city parks, to cramped enclosed spaces, to roof tops - all within a very short distance from each other - each having different gun needs.

For survival purposes, the handgun is usually considered a defensive weapon due to its limited ammo capacity and range. However, with the advent of large capacity magazines and diversity of ammo, automatics (ie: semiautomatic pistols) have become viable offensive weapons for urban combat. It's small size enables the automatic to be easily wielded in enclosed spaces, and certain weapons (ex: the Heckler & Koch VP70) have as much magazine capacity as SMGs. Also note that the automatic was the weapon of choice for many "tunnel-rats" (underground combat experts in the Vietnam War).

The riot shotgun remains one of the best weapons for short-range urban combat, and in enclosed areas. My definition of a riot shotgun is a pump or semiautomatic shotgun with an 18"-20" barrel having a cylinder bore choke. For added versatility it is usually equipped with a folding stock with a pistol grip. This is one of the few effective weapons which is still available without major restrictions. It is also capable of the same fire power as a SMG when used by a person trained properly in its use. Its only disadvantage is that its a short-range weapon, but that disadvantage can also be somewhat taken care of with proper training.

SMGs are somewhat better than riot shotguns as short-range weapons. Their range is better, they carry more rounds and have greater penetration. On the other hand, the riot shotgun handles ambushes much better as aiming is not as critical and one blast can wipe out several assailants. True SMGs are illegal in the U.S. Their legal equivalents are semiautomatic only and have their barrels lengthened to meet legal requirements. Because of these changes, their effectiveness is reduced as they become little more than M1 carbines firing pistol ammo.

A small, concealable and silenced SMG, such as an Ingram MAC10 or MAC11, does have its use as a covert operations/ assassination short-range weapon. To paraphrase one covert ops expert, you could use a silenced MAC10/11 to wipe out an entire room filled with people without anyone waiting outside of the room realizing anything wrong. The MAC10/11 is not much larger than a .45 automatic, and can be concealed in clothing, briefcases, hollowed-out books, etc.

THE SURVIVAL ARSENAL

With all of the guns on the market, it's often difficult to select exactly what you need in your survival arsenal. The weapons you'll need will depend mostly on your home terrain, and possible situations you'll run into associated with that terrain. As your operational area increases, and your aims shift from that of simply survival to freedom fighting, your weapon needs will increase. At that point your weapons needs will shift from self-defense and hunting, to guerilla warfare, to more sophisticated military actions.

Clearly, you can make due with more primitive and less militarized weapons if that's all that's available to you at the time. For the cost of a VCR you can acquire one to several quality guns. Regardless of which gun is optimum for which situation, about the most guns that anyone can carry at any one time are three (if at least one is a handgun). So when someone tells you that they have 50 guns, clearly they have far more guns than they can ever expect to need or use in a survival situation. And as things go along, other guns will become available to you (ex: off of dead bodies, abandoned or in storage).

Now that you made a list of your operational requirements, you should figure out exactly what you need. When doing this, the major things to consider are: Gun price, the survival niche that the gun fills, the gun's availability, and your capability to effectively use it. What I mean by capability is that while a .44 magnum might be one of the most effective handgun rounds to use, it'll be worthless to you if you can't handle the recoil. You can't kill an attacker with a loud sound.

HANDGUNS

The handgun is primarily a defensive weapon. There are solid arguments for both revolvers and automatics. Automatics handle more rounds, reload easier and faster, and you can fire them more quickly. But automatics also jam more, have more moving parts, are less accurate at distance, have less range, and are limited to far fewer calibers than revolvers. Revolver reloading problems are somewhat overcome with speed-reloaders.

My rural choice is a .357 magnum double-action revolver, like the Dan Wesson (heavy barrel). With enough practice you can effectively hunt big game with it, and it's ability to also use .38 special rounds make it one of the most versatile handguns. While it may not be as quick as an automatic, it's double action will still let loose 6 large high speed bullets in a relatively short time, which suits most purposes. And being a revolver, it'll stand up to abuse in a survival situation better than any automatic.

My urban choice is the .45 ACP automatic based upon the Colt M1911 design. The .45 ACP isn't a recommended hunting round, but will serve well for personal defense and offense, and has far greater stopping power than the inexplicably more popular 9mm automatics. 9mm automatics have only been proven to be more effective against blocks of gelatin. When the earth becomes invaded by gelatin space monsters, I'll get a 9mm. In the meantime, I'll snuggle up to my trusty Colt .45.

If I couldn't handle the recoil of the bigger calibers, I would resort to the 9mm (urban) or a .38 special (rural). Altho both rounds are marginally suitable for defensive purposes and for hunting, if you can't properly handle the larger calibers, it makes no sense to use them. The 9mm higher capacity magazines are also more forgiving if you aren't as practiced or steady.

The .380 ACP is a little under the 9mm in stopping power, and is more or less ideal for children and the elderly, altho its ammo is not that common. For the more anemic calibers like 9mm and .380 ACP, I would buy/ modify ammo to maximize its stopping power. Never be lulled into thinking that a low stopping power slug is going to stop a highly deter mined/spaced-out attacker. The 38 special has greater stopping power than the 9mm and .380. Yet, several years ago, two police officers pumped 13, 38 special slugs into an attacker. The attacker survived to stand trial for their murders!

In all cases, I would also be backed up by a .22 revolver (rural) or automatic (urban). Altho the stopping power of the .22 is zilch compared to the larger calibers, it is ideal for small game, pests and feral dogs, and the gun can be easily carried and hidden in case I lost or jammed the bigger one. Even a .22 is far better than having to flip the attacker off. Stay away from .25 and .32 cals. as they are about as effective as a bean bag.

Pocket pistols are intended for very short range firing. 30 feet is about the practical maximum. If you get into this situation, aim for the chest (unless he is likely to have body armor, then aim for the head), and then empty the magazine into him as you step closer. If you hit a vital area, he's either dead or severely wounded, and you've stopped the attack. Whether you finish him off or get the hell out of there is up to you. If he isn't (badly) hit and just an average scumbag, then he'll probably be scared shitless, which will give you enough time to get out of harm's way before he can react. If he is an above average scumbag, then you will clearly be in a very embarrassing situation.

RIFLES

The choice of a rifle is even more varied than is for a handgun. That is because there are more different types of rifles. The first is the basic .22 LR Rimfire, commonly used for target shooting and small game hunting.

The second is the high-power rifle, which is a large caliber (.308/7.62mm NATO, .30-06, 7mm Magnum, etc) weapon used for hunting big game, and also for sniping. These guns are usually bolt actions, and occasionally are semiautomatic. The third is the "rifle carbine" (most people incorrectly refer to as the "assault rifle"). I don't like the term, "assault rifle", for several reasons: They are not true "assault rifles" (as they are semiautomatic at best), the term implies that the user intends to assault people with it, and the term is used as a catchall to describe any gun that some liberal doesn't want to see available to the public.

In any event, my term "rifle carbine" is used to indicate any shortened rifle that uses one of the smaller rifle cartridges (.223/ 5.56mm NATO, .30-30 Winchester). Most of these guns are semiautomatic, but lever- actions are also included in this category.

The forth category is what I call the "pistol carbine", as they are carbine-length weapons which fire a pistol round (ex: 9mm, .45 ACP). These weapons are basically civilian, semiautomatic versions of SMGs that have had their barrel lengths lengthened to meet the specs for a "long gun", as defined by the BATF.

Each type of rifle has different uses. Due to varied types of rifles and their various uses, rifle selection isn't as easy as pistol selection. Urban rifle selection was explained earlier in the "Urban Scenarios" chapter, which leaves us with the rural and suburban scenarios.

If I were in a forest with heavy underbrush, the rifle carbine would be best for its maneuverability. The intermediate cartridge would also serve well at the short ranges you'd be encountering your targets at. Traditionally, the 30-30 lever-action (ex: Marlin and Winchester) was preferred here because its heavy bullet could crash thru the underbrush with minimal deflection. However, any 5.56mm semiautomatic would probably do OK, particularly if your were shooting into trees or across ridges. Don't worry about range too much, as you probably aren't going to engage your target at any more than 100 yards.

If I were in the Great Plains or a similarly clear area, I would choose a good .30-06 or .308 semiautomatic as my combat rifle. Weapons like the M1 Garand, FN-FAL, and HK91 are good choices. These can also be used as sniper rifles. If I wanted a real accurate sniper rifle, I would go with a bolt-action with a scope. The Springfield M1903 is a classic example, and bolt-actions by Remington, Ruger and Winchester are excellent as well.

In a wide-open situations (ex: temperate forests), you'll need something with great range, the 7mm magnum is most preferred (if you can get the ammo) for its flat trajectory and very high velocity and range. Altho average ranges in temperate forests are less than those of the Great Plains, on ridges the ranges are in terms of miles.

For suburban areas, my general purpose rifle would be a 5.56mm semi automatic. It has good firepower at the range you require. For a "sniper rifle", I'd stick with a 7.62mm, and make it very accurate. In a suburban scenario, it's difficult to find the range you need to be safe, altho the range is longer than in an urban scenario.

.22 RIMFIRES: .22 Long Rifle (LR) Rimfire weaponry deserves a section all it's own due to it's unique and versatile nature, and its extremely wide availability and high affordability. It's probably the most versatile gun around - indispensable for hunting small game, eliminating pests, and for gun practice. A .22 rifle shooting high velocity ammo zips a 50-grain bullet along at 1,000+ feet per second. When hyper velocity rounds are used, the bullet shoots even faster. While the bullet's stopping power pales when compared to anything larger, it's high speed, high accuracy and decent penetration make it very effective. With hyper-velocity (CCI Stinger) ammo, you can effectively use a .22 to over 200 yards - more than adequate for most survival and self-defense uses.

A .22 has little recoil, making rapid fire easier, and effective use by weaker people possible. The innate lighiness of the .22 rifle and handgun makes their wheeling-and-aiming response times much faster than those of the larger calibers - ideal for use against small game and pests, and often the difference in a gun fight.

The velocity of the .22 rifle bullet is just under the speed of sound. This makes the .22 rifle invaluable as a silenceable rifle (Note: some larger handgun calibers fired from "assault rifles" - 9mm, 45 ACP, etc - are also subsonic and silenceable). When silenced, the .22 rifle report is less than that of a .177 cal. BB rifle. .22 handguns come in small and lightweight sizes, making them backup guns of choice.

Keep in mind that .22 ammo is much more susceptible to environmental conditions than other rifle ammos, and after being stored several years in a garage or shed, tend to experience many misfires. I've seen other (military) rifle ammo stored 40+ years in bunkers with better reliability.

For the .22's advantages, it is essential to outfit yourself with at least one .22 gun for any survival situation.

My favorite .22 rifle is the Charter Arms AR-7 Explorer. This is a true "Survival Rifle". You know this right off because the Government has tried to ban it. It's semiautomatic, clip-fed and can be taken apart with no tools and stored in the rifle's nylon stock (which happens to be waterproof and will float). Disassambled, the entire package is 2-1/2 feet long and weighs a little over 2 lbs. The standard clip contains 8 rounds, and is quite small so one can carry quite a few ready for action. If one desires more firepower, 25-round clips are available (at this writing). For a back-up and survival rifle, I recommend it most.

For a general-purpose hunting/utility rifle in .22LR, my preferance is the Ruger 10/22. This rifle features a highly reliable rotary magazine action which is less prone to jamming than other .22s. It also has the usual range of accessories such as folding stocks and high capacity clips. Another good brand is Marlin. Marlin makes excellent quality, inexpensive .22s which, from my experience, are reliable and very accurate.

SHOTGUNS: For short range combat, your best bet is a shotgun. A .12-gauge pump shotgun loaded with 00 buckshot is equal in firepower to a 9mm sub-machine gun, and you can LEGALLY buy the shotgun without special registration or fee. Shotguns are common and readily available guns. Despite their fearsome reputation, their possession doesn't raise eyebrows (even of those of liberals), as they have a legit hunting use. If you live in a rural area, few will pay undue attention if you have a shotgun (or deer rifle) in your pickup truck (because many people do), whereas many would certainly take a second look if you had an AR-15 on the gun rack.

For close combat, the best is a 12- or 20-gauge (16 is marginal) pump or semiautomatic shotgun with an 18" - 20" barrel, and preferably with a folding stock with pistol grip. Sawed-off shotguns are of limited value (they are illegal), and can be replaced for most uses by a legal riot shotgun. One real foreseeable use for a sawed-off shotgun would be as self- defense in a highly-intense and closed-in combat situation (mostly urban). Most sawed-off shotguns are made from break-open shotguns because the barrels can be cut down more easily than you can with others. However, this limits the number of rounds to one or two, defeating most survival purposes. Furthermore, when the barrel is really cut-down, the shot-spread makes it usable only out to about 20 feet. For utility use, go with a full-length barrel and a variable choke.

Break-open shotguns do have one outstanding advantage. They can be easily converted into improvised mortars (about the ultimate in improvised mortars are made from tennis ball or baseball ball throwers). The double-barrel 10- or 12-gauge with a medium length barrel is also effective for home/office defense against burglars and prowlers, as both barrels going off at once (if you can handle the recoil) releases a large shot pattern that much improves your chances of hitting your target - as well as everything else in front of you (suggested only if you live/work alone). It also makes a LOUD noise.

HARASSMENT AND REVENGE

This chapter contains much miscellaneous information that falls into the category of "soft" guerrilla warfare. Use this chapter when some scumbag screws you over, and you don't want to blow up his house, or shoot him in the kneecaps.

THE S.H.I.T. BOMB

This one is so nasty, I wouldn't use it on my worst enemy. S.H.I.T. stands for Special High-Intensity Terror, as well as its main ingredient. Take a sandwich bag, and fill it with, ahem, feces. Then stick in an M-80. (*see our FIREWORKS manual on how to make M-80's as well as other fun toys*) When the M-80 is lit, and goes off everything within 50 feet will be "fragged" with excrement. Now you know why it's called S.H.I.T. bomb!

The best way to rig it is to take a light-bulb, break the glass without damaging the filament, and then screw the device into a ceiling light socket THAT IS OFF! This way you can be out of the area when it goes off, make sure the target is within the blast area, and you get a greater blast radius from being high-up. Another safe way to activate it is by lighting a cigarette, and placing the fuse at the base of the cigarette. One can get a 5-10 minute delay this way, and it is most effective for deployment in public places.

GAS TANK TRICK

Everyone's heard about putting sugar in the gas tank of a mark's car. For something even more nasty, but less damaging, pop in a ping-pong ball. When your mark starts driving, the ping-pong ball will be sucked to the bottom of the gas tank, and block the fuel line. The car then dies due to lack of gas. The ping-pong ball then floats to the surface, and the car can be driven another couple of miles until the whole routine repeats itself. Unlike sugar, no evidence whatsoever results. Eventually, the ball will dissolve in his gas tank (usually after about $400 in car repairs).

Stuffing a potato in the tailpipe is another way to seriously disable a vehicle. Want to make a car backfire? It's easy. All you do is (when the car engine is cold) take a handful of 22 cartridges and throw them up the tailpipe. Then take a pair of pliars and bend up the bottom of its exhaust port so that the ammo doesn't roll out. After about a half mile, the tailpipe will be plenty hot to set off the 22s - don't be nearby!

IMAGINATIVE BUSINESSES

Thanks to the wonderful world of desk-top publishing, you can create limited runs of professional-looking flyers, catalogs, newsletters, business cards, and the like without the hassle of dealing with the minimum amounts, high cost, delays and high exposure that using a commercial printer entails. I know, six years ago, I turned in some work to a local scumbag printer, and he turned it over to the FBI! Nothing happened but I was really pissed!

Besides the practical aspects of that, how about making up some business literature for your favorite mark? Some of the ideas I was considering around one depraved evening included doing some free advertising for his new business I invented for him called "Pederasts' Procural Services." Include a few blurbs in the ad such as "professionally trained catamites," or "bestiality and necrophilia our specialty." Include the mark's name, home/business addresses and home/business phone numbers. Not only will every weirdo and deviant call him/her at odd hours, but chances are quite a few people will be stupid enough to believe the ad, and possibly bring legal and-or other action against him. At a minimum, his reputation is shot and his life may be in danger.

A variation of this theme is to get a hold of a phone line, preferably the marks, and do a little telemarketing off of it for the mark's business. Ask people if they have a young son, and if so would they be interested in sending him to catamite school. Act serious and professional, like "Pederasts' Procural Service" has been training young boys to become catamites for 69 years. If you act serious, most people will take you seriously, which leads to major trouble for the mark. Hopefully some people will complain to the phone company, and they might investigate - especially if they get an "anonymous tip" that so-and-so is running a boiler-room operation out of his basement.

And while we're on the subject...

With all the stuff going on about child molestation, a well-placed rumor to that effect will have a devastating effect on your mark, especially if he/she works with kids. Make it as disgusting as you wish. You could also take a trip to 42nd St. and pick up some kiddie porn to send to your mark at work, or plant in your mark's office.

If you're really into sick stuff, get two adults who are very open-minded. One should look like your mark, the other should look real young, like way under 18. Take a few pictures of them in various interesting positions, and make sure his/her spouse, boss, minister, friends, etc get copies. You could also use some of that desktop publishing equipment, along with some video digitizers, and merge pictures of your mark with the porno.

PASSING THE BUCK

A good practice is that when you apply revenge techniques to your mark, leave evidence to implicate a second mark, or some organization like the KKK, JDL, American Nazis, Earth First, or NOW. The best thing to do is to blame some organization that you never could have any affiliation with, such as the KKK if you're Jewish or Black, or the Black Panthers if you're a WASP.

WRITING ON THE WALL!

It's always been my belief that once you've identified a scumbag or crook, you should let the whole world know! The best way of course to do that is to publish. Unfortunately, since most scumbags you run into in this life have far more money than you do, he can beat up on you by using his shyster attorney and the corrupt judicial system. To avoid that, you have to find a way of publishing the person both in a way that makes it impossible for him to prove that you did it and that will maximally damage him. The best way to do this is by using a small scratch awl, nail, ice pick or similar, and carve his name into places like toilet stall walls in seedy bars, bus stations and parks. Don't use ink as ink can be removed or painted over. The device should have a good handle so that your engraving is as deep as you can get it - you want something to really last! And make it seem very worthwhile for the reader to contact the mark. For example:

"I need anal sex! $100 plus $100 per inch above 8. I also pay extra for big balls, whippings and chains. Call 555-1234 (his wife's number or the boss' number) or stop by any time at 321 Big-Shot Heights (mark's home address if married, else his work address) and ask for Bob 'Sweet Cheeks' Simpson."

Or you might say:

"Local chapter of the ... now recruiting! Apply by calling ... or in person at ... " Follow this by his name, home/business phone number and home/business address as above. The group mentioned should be one in which the people that will read it are highly pissed at (ex: "KKK" in a black ghetto bus stop), or will tend to be very supportive of. This type of advertisement works particularly well in communities with very high racial and ethnic tensions.

Another excellent tactic is to produce half-page flyers advertising the mark's suspected pedophile activities and surreptitiously insert them in children and teen books at libraries (particularly church libraries), scout huts, etc (leave no fingerprints). For example:

"*Hi! Boys and young men wanted. Must be open-minded, keep secrets, and are well-developed. I have lots of money and stuff that will make you feel great...*". Follow this by his name, home/business phone number and home/business address as above. Sound really sincere, and don't be too obvious. This works particularly well if you've got a serial killer or rapist prowling your community.

THE #1 RULE OF REVENGE

The #1 Rule of Revenge is to NEVER take credit for your actions! The important thing is to effect the revenge. That means that you tell no one - not even relatives or close friends! And you use as few people as possible to help you execute your scheme.

Another very important rule is that unless you expect only a limited window of opportunity, you should take your time to plan and execute your actions from the time that you've had the problem with the mark. For example, if your mark rips you off in a business deal and two weeks later his neighbors are getting anonymous letters about how much of a pervert he is, not only will the credibility of the letters likely be questioned but the finger will obviously point to you (unless he's such a scumbag that he has many known enemies). On the other hand, if you wait 1, 5 or even 10 years, particularly at an opportune time (ex: the mark is running for office, plans to get married, is being considered for something important, etc), not only will the effectiveness of your attack increase many fold, but the finger won't point to you. Also by waiting, you can often gather more information on the mark to hone your attack better.

Personally, I have the policy of never forgetting, never forgiving and always getting even. ALWAYS!! For example, when I was in high school, I showed a classmate (who I thought was a friend) some of my Dad's coins. He stole them and I got into big trouble. Fortunately, I knew something about his family. 15 years later, I collected with big, big interest.

VEHICLE MODIFICATIONS

THE BASIC CAR

This mostly depends on what you want to do. Each vehicle type has certain tradeoffs in different areas. Van's make great surveillance posts, but lack performance. Sportscars, while high in performance, are a bit flashy for undercover work. Your basic family sedans are great for undercover work, but lack performance, and the list goes on. Your best bet is to figure out what you want to do and how much money you have. Then shop around. *Here are a couple examples of vehicle types and their advantages/disadvantages:*

Smaller Family Size Station Wagon: Great combination of size, and unobtrusiveness. Preferable with a large hatchback. There are plenty of used ones around at reasonable prices. Being a common vehicle, they're inconspicuous, and the extra room allows for plenty of modifications and extra equipment. Performance is a bit lacking, altho gas mileage is good, as well as usable space.

Small (but not too small) Sports Cars (like the Ford Mustang): My favorite high-performance vehicle modification car. It is the pursuit interceptor of choice for many police departments. It's less flashy than some other sports cars, but anyone who is slightly familiar with cars will know its reputation. Overall a very nice car for a James Bond special, but its reputation can be a hassle.

Plymouth Type Family Vehicles: Your basic four door-family sedan. Probably the most innocuous-looking car around which is its biggest advantage. Very reliable; also available in high-performance versions with a V8 engine. Widely available at reasonable prices.

Family Vans: As stated before, excellent for surveillance ops, but can be obtrusive and attention grabbing. You don't want that. Very important: do not use a van with no windows. Everyone knows that a van with no windows means only one thing: trouble. Use very dark window tinting to obscure vision into the van. If using in night ops, cover insides of windows with black tarp.

So you want to be like James Bond and drive around in a souped-up car full of gadgets? Well for starters we aren't going to show you how to convert your Geo into an amphibious, all-terrain assault vehicle, but we will tell you about a few interesting things which might come in handy in certain situations. Be advised that certain modifications might be illegal in your area., or at least piss a lot of people off.

COMMUNICATIONS

For communications between your home base an other mobile units, your best bet is to install a CB (Preferably with SSB and modified for extra channels), and a secondary communications unit (ex: a business band mobile radio or modified ham set). The CB will enable you to go public for information such as traffic reports, and for communicating with outside parties (since everyone owns a CB these days). Mean while, you have something more secure to use for your group. Option ally, you might want a scrambler for your private net, and possibly a "mobile relay" which makes your vehicle's radio act like a repeater between a handheld and your base for when you're away from the car.

In the realm of receiving equipment, install a good scanner and radar detector. Both of these should be hidden, as their use is illegal in some areas. You might also want to get a radar jammer, although they are illegal, and not necessary to avoid tickets.

WEAPONS SYSTEMS

"SHOCKWAVE" DEFENSE SYSTEM: Use an audio sweep generator set between 1-25 KHZ, putting out about 120 decibels. When exposed to this sound of this frequency range, humans and animals react with headaches, disorientation, nausea and a general feeling to get the hell out of the area. The sound level itself, 120 decibels causes major pain and discomfort.

ANTI- PURSUIT SYSTEMS: Just like James Bond, there's the well known oil-slick sprayer. The easiest way to do this is to get a solenoid-opened box, and fill it with oil, or better yet, an oil/teflon mixture. Mount this in your trunk, or under your car just behind the bumper, with a switch going up to the dashboard. As an alternate one could also drop caltrops. During the night, you can also "flash" someone. Mount a high-power (minimum 100,000 candle power) spotlight facing behind you. When someone gets on your tail at night, let them get close in, and turn the light on. Your pursuer will be temporally blinded, and unable to follow you.

FIREARMS: In many areas, mounting firearms on your vehicle is illegal, but if you desire to do so, a shotgun or semiautomatic rifle could have the barrel cut down, and stock removed for easy mounting in the trunk or under the hood, and hooked up to a motor-driven BMF activator or solenoid. Accuracy won't be great, but it could save you in a tight situation.

BETTER LIVING THRU CHEMISTRY

Knowledge of basic chemistry is essential for the technological survivalist/freedom fighter. A basic chemistry knowledge makes the safe manufacture and use of explosives and other chemical warfare weaponry easier. This section will deal with the nonexplosive/nonmilitary aspects of chemistry. In particular: Poisons and "revenge" chemicals. For those looking for explosives, and Nuclear/Biological/Chemical warfare information, consult the respective chapters in this book. (for more information on poisons, see our **DEADLIEST TOXINS** manual).

NON-LETHAL MIXTURES

There are a couple of chemicals and chemical mixtures which have applications in the non-lethal "revenge" department. A classic group are the laxatives. Not surprisingly, laxatives were used in certain covert ops. by the CIA in the past as a very effective psychological warfare attack. Many different types of laxatives can be mixed with food and will escape detection. My two favorites are Metamucil and Chocolate Ex-Lax. Chocolate Ex-Lax mixes great with candy and Metamucil is a powder which dissolves in just about anything. Add as much as you desire, the most you can get away with - you want to keep your opponent very regular!

Another old favorite which isn't too well known is Ferrous Sulfate. This is sold as a dietary supplement. When too much is taken, two very interesting things happen: The first is that it turns the color of urine to green. The second is that it causes various types of intestinal distress. In some respects, this stuff works even better than laxatives. We also have Tabasco or "hot sauce." When injected just below the surface of the skin it causes terrible rashes with plenty of swelling, itching and burning. The classic method of injection was just to coat a small amount on the tip of a sewing needle dart.

There is also Saltpeter or Potassium Nitrate. Also required to make black powder explosives and usable as a rocket oxidizer. When administered orally over a period of time, it causes the pleasure centers of the reproductive system to shut down. It has been placed into food at military bases to keep soldiers from getting horny. It also acts as a diuretic.

A wonderful classic guaranteed to be the laugh at any restaurant, or social gathering is good old Syrup of Ipecac. In case you didn't know this stuff is used to cause vomiting in cases of "poisoning". It's wonderful stuff.

POISONS

Poisons are considered the Sunday punch of warfare as they allow small wounds to be just as deadly as bigger ones. Granted, all one has to do is just get the stuff in the target's body in a large enough concentration and it'll do the job. The #1 rule when working with poisons is to keep that in mind and don't accidentally ingest the stuff, or accidentally cut yourself with a contaminated blade or needle. If you're not extremely careful, you may end up accidentally doing yourself in first.

There are four basic ways a poison gets into a targets body. They are injection, ingestion, inhalation and skin-absorption. Of the four, the easiest and most common are injection and ingestion. The hardest to detect when properly done are skin-absorption and ingestion, followed by injection and inhalation. However, evading detection is only really needed with long term poisons. For a quick one-shot affair such as Cyanide, detection becomes less important. The most dangerous (for the user) method is skin-absorption. If this method is used one must be extremely careful not to get the mixture on one's skin for obvious reasons.

Cyanide: is considered the "classic" poison. It seems that every movie poison victim is killed off with cyanide. Cyanide is fairly quick-acting, and can be delivered in various ways. And it can be field-made by taking a handful of Apple, Peach or Apricot seeds (with the hull removed), drying them out and grinding them up. While not the purest form of cyanide, this field expedient is easy to make and gets the job done.

Nicotine: A drop of pure Nicotine will kill someone in 15 minutes, and is also fairly easy to make. Nicotine can be ingested, injected, or absorbed through the skin (see DMSO). A close to pure form of nicotine can be made by taking a can of chewing tobacco or "snuff", wrapping it in a handkerchief and soaking it in water for a day. After you soak the tobacco, remove it from the water, wring well to remove any water, and dispose of it. You then slowly boil the water until a dark syrupy liquid remains, which is your finished product. This can then be mixed with a few drops of water to the desired consistency for ease of use in certain situations, such as injections. It can also be mixed with drinks, but is somewhat detectable unless the drink's taste masks the taste of the nicotine.

Asbestos: can be obtained from the furnace areas of old, abandoned buildings or areas having it removed. Asbestos causes cancer in even minute amounts, and it makes a good long-term poison. Asbestos is best inhaled, altho ingestion also works, but not as well. The best way to deploy this poison would be to stick it in a bag or envelope with an adequate explosive (ex: a large M-80) or pressurized release (ex: in a balloon), and explode it near your target. This will throw the asbestos in the air where it will be inhaled, and thus most effective. In an enclosed space, such as an office, the exploding asbestos will go everywhere and be very difficult to thoroughly clean up. Just don't be anywhere around your device when it goes off.

LSD: while not poisonous in itself, causes hallucinations which can effectively disable your target, making the killing process by other means much easier. Also, in large doses, it could cause a bad enough "trip" that the target will kill himself, leaving no evidence of foul play.

People also tend to do dangerous things when they're on LSD, like believe that they can fly, and try to jump off of a tall building to try out their new found ability. Be careful with hallucinogenic drugs, as some types like PCP can cause extreme psychosis, making your target harder to kill and/or making your target turn on you. The results could be very unpredictable.

There are various types of psychedelic drugs out on the black market which are fairly cheap. LSD is a common one and comes in various forms. The common method of administering LSD is by placing it on the tongue. It could be mixed with food and given to your victim. There is also a variety kicking around called "blotter," or "blue star" which is on a piece of paper and absorbed through the skin. While this brings up some interesting possibilities, one should be extremely careful with this type as it's too easy to get it absorbed thru your skin, causing you to have some quite disconcerting experiences. Just don't stare at lightbulbs or chessboards.

Chlorine Gas: causes Leumonia (Phneumonia of the lungs) which can be fatal. This is some nasty stuff so I don't recommend playing with it as it's real easy to get yourself put in the hospital with it. Chlorine gas is made by mixing ammonia or Drano with a chlorine solution, such as Chlorox Bleach. This is usually done by putting the two chemicals in separate glass bottles, taping them together and then throwing them at the target. Chlorine gas is released upon impact.

Poisonous Animals: If one captures a poisonous animal, like a spider, snake, gila monster or whatever, and sticks it in bed or somewhere similar with his target, then chances are it will bite him and poison him. Of course antidotes for animal poisons are readily available, limiting the effectiveness of such a technique, but if he's sleeping or otherwise "occupied," then it just might work effectively. To safely deal with a live animal takes some knowledge and experience, and results can be unpredictable. But even experienced snake handlers get bit now and then.

Plant Poisons

There are various plants which are poisonous and readily available in the United States. Some of the most deadly poisons come from plants. Others will just cause some discomfort and inconvenience. Note that even if a poison is described as being non-Fatal, the injection or ingestion of that poison and-or when taken in large enough quantities, and- or depending upon the health condition, allergic reaction and age of the target, can easily become Fatal. Thus, the terms "Fatal" and "Non- Fatal" should be regarded more in the vein of relativity to each other as opposed to some absolute concept. Some examples:

AUTUMN CROCUS: Bulbs cause vomiting and produce a nervous state.

ASH: Poisonous.

ATROPA BELLDONNA: Fatal.

AZALEAS: Produces nausea, vomiting, depression, respiratory problems and coma. Fatal.

BE STILL TREE: Produces low pulse, vomiting and shock. (Fatal.)

BLEEDING HEARTS: Foliage & roots are fatal in large amounts.

CAMARA: Green berries affect lungs, kidneys, heart, & nervous system. (Fatal.)

CAMOTILLO: Contains solanine. Fatal.

CASTOR BEANS: Contains Ricin - one of the most deadly poisons known to man! Causes vomiting, delirium, & coma. Fatal.

COMMON OLEANDER: Causes heart problems. Fatal.

CHERRIES: Wild and domestic twigs & foliage contain cyanide. Fatal.

CHINA BERRY TREE: Fruit affects nervous system. (Narcotic.)

CHINA TREE: Seeds must be injected. Fatal within 4 hours.

CROW FIG: Seeds contain strychine.

DAPHNE: Berries. Fatal.

DEATH-CUP MUSHROOMS: Fatal.

DIEFENBACHIA: Produces burning, irritation, and swelling to mouth.

DIVINE MUSHROOM: Produces hallucinations. Psychedelic drug.

DUTCHMAN'S BREECHES: See Bleeding Hearts.

DUMB CANE: See Difenbachia.

DWALE: See Atropa Belldonna.

EAST INDIAN SNAKEWOOD: Contains strychine.

ELDERBERRY: Causes vomiting and digestive problems.

ELEPHANT EAR: See Difenbachia.

FALSE UPAS TREE: Contains strychine.

FOXGLOVE: Contains digitalis. Affects circulatory system.

GARLIC: Must be injected.

GOLDEN CHAIN: Seeds cause convulsions and coma.

HOLLY: Poisonous.

HYACINTH: Causes vomiting.

JACK-IN-THE-PULPIT: Causes irritation to mouth & tongue.

JASMINE: Berries affect nervous and digestive system. Fatal.

JIMSON WEED: Causes halucinations. Fatal.

LARKSPUR: Seeds affects nervous and digestive system.

MAYAPPLE: Roots are highly toxic. Fruit causes diarrhea.

MISTLETOE: Berries are fatal.

MONKSHOOD: Roots affect digestive and nervous system.
NARCISSUS: See Hyacinth.
NIGHTSHADE: Unripe berries affect nervous system. Fatal.
OAKS: Foliage and acorns affect kidneys. Non-Fatal.
OLEANDER: Leaves and branches affect heart. Fatal.
OLOLIUQUI: See Jimson Weed.
POINSETTIA: Leaves are fatal.
HEMLOCK: All parts are fatal. What did Socrates in.
POISON IVY: Causes irritation. Non-fatal.
POISON OAK: Similar to Poison Ivy.
POISON TANGHIN: Causes vomiting and paralysis. Fatal.
POTATO: Vines and foliage affect nervous and digestive system.
PSYCHIC NUT: Seeds cause vomiting. Fatal.
RED SAGE: See Camara.
RHUBARD: Leaves produce convulsions and coma in large amounts.
ROSARY PEA: See Castor Bean.
ST. IGNATIUS' BEAN: Causes convulsions.
STAR OF BETHLEHEM: Vomiting and nervous system problems.
TOMATO: Vines and foliage affect nervous and digestive system.
WOLFSBANE: Poisonous.
YEW: Foliage is Fatal.

Miscellaneous Poisons: Pesticides, herbicides and many other common chemicals are poisonous - some of the more powerful pesticides are very deadly. The fact that the poison control centers deal with hundreds of accidental cases a day attest to that fact. While some of the things may not be all to easy to get into the person by ingestion. One can still inject them or use DMSO. One of the nastier chemicals is Methyl Alcohol, or "Wood Alcohol," which is a common chemical used in many different consumer products, particularly in regards to auto supplies where it is used in Anti-Freeze, Dry-Gas and Windshield Washer Fluid. This stuff causes blindness and is also deadly.

Battery acid is another commonly available deadly chemical, capable of causing severe burns, which will at least disable your enemy permanently if thrown at the eyes.

Most spray-type chemicals will cause blindness if sprayed in the eyes. Take a look around the housewares and the automotive section of your local department store. They offer a myriad of chemicals with field- expedient uses. For information on deadly toxins, see our DEADLY TOXINS manual.

AIR

If you have a needle and syringe handy and nothing right at hand, you can always inject air into your target's bloodstream. This will cause an air embolism, which can be fatal. Cause of death is hard to detect and even harder to prove. Maybe I shouldn't have included this section. Surely, some hand-wringing liberal in Congress will now feel required to register or confiscate everyone's air. If that happens, only the police and criminals will have air. Remember air doesn't kill people - people kill people.

TRANQUILIZERS

This method has been used by many people to commit suicide and could be used as a weapon. However, to get someone to drink a toxic amount of tranquilizers requires some trick. In some cases, the target will get too drowsy too fast to voluntarily ingest a toxic amount. In other cases, your target might get sick and vomit.

MAKING KNOCK-OUT DROPS

The term, "Knock-Out Drops", usually refers to chloral hydrate. I cross-referenced this file with some chemistry books, and this procedure is a field-expedient that works, altho famillarity with basic chemistry is helpful.

CHEMICALS: Clorox Bleach, Sani-Flush, Sulfuric Acid, Calcium Oxide Distilled Water, Alcohol. And a Basting Syringe.

(1) You will need pure alcohol so buy some 100 proof vodka and distill it until you have about 12 ozs. Put the alcohol in a flask (Flask A).

(2) Put a small quantity of bleach and a teaspoon of Sani-Flush in another flask (Flask B). This will generate the chlorine gas that you will need. Aerate the chlorine thru the alcohol (Flask A). When the alcohol stops absorbing the chlorine, place a heat source under Flask A. Keep the heat source on at a low level until the alcohol stops absorbing again. Raise the level of the heat source and repeat. Continue this until the alcohol is boiling. Some of the alcohol will distill off into the collection bottle of the still. Several times during the process, pour this back into Flask A to obtain greater purity.

(3) When the alcohol is totally chlorinated, the flask is poured into a porcelain dish and allowed to cool. If you have done this right, the cooled product should be a crystalline mass of unrefined Chloral Hydrate. Now, pour sulfuric acid, three times the volume of the Chloral Hydrate, into the pan. Place this pan on your stove over gentle heat. When the Chloral Hydrate is melted, it and the sulfuric acid are stirred thoroughly. Pour this into the flask and heat again, but this time use a thermometer and don't let it get over 200 F. As the mixture heats up, the still impure Chloral Hydrate will rise to the surface. When it stops rising, use the basting syringe and draw the top off of the sulfuric acid. Repeat this until the pan is empty of Chloral Hydrate.

(4) Put the Chloral Hydrate (you drew it off in the last step) into a beaker and heat at about 190 F for 20 minutes. This will get rid of any alcohol or acid still in it. Pour this back into the flask and add an equal amount of sulfuric acid. Swirl this around to mix it.

(5) Once again you must distill the mixture, but this time it is easy since the Chloral Hydrate will boil at 210 F and the sulfuric acid boils at 722 F. When finished pour out the acid, then wash and dry the flask.

(6) Now, put the powered Calcium Oxide, equal in volume to the Chloral Hydrate into the flask, add the Chloral Hydrate and distill again. Stop as soon as the surface of the oxide is dry.

To use, add one part water to two parts by volume of the finished product. The dose is 1/28th of an oz (1 gram). The best way to use this is to put it into a mixed drink, because it has a bitter taste. In about 15 minutes, it takes effect.

EXPLOSIVES

There is much information on explosives. Many different books provide some interesting and useful information. For demolitions information, pick up a copy of the "U.S. Army Explosives and Demolitions Manual". Both of these are available via mailorder from several publishers, and occasionally at Military Surplus Stores. A few hacker BBS also have a lot of explosives information on them because of the information-hungry nature of their hobby. However, much of this information is inaccurate and very dangerous (ex: mixing chlorates with sulfur).

For related information, CONSUMERTRONICS publishes "Rocket's Red Glare" (solid-propellant rocketry), and "Fireworks" "Rocket's Red Glare" is highly recommended for its description of many propellant formulations -many of which can be modified to make explosives.

LEGAL EXPLOSIVES

The following two explosives are legal in that they have legit purposes, and can be bought over the counter. However, their legality becomes moot when they find out you've made a couple of grenades with the stuff. Both of these can be bought at gun stores, altho their purchase implies that you know what they're used for, and if you're not familiar with black-powder guns or reloading, you could get into a situation where you're asked a question and won't know the answer. The solution is obvious, acquire some knowledge in those fields. Reloading and black powder knowledge is practically required knowledge for the Survivalist.

PYRODEX/BLACK POWDER: This is the most common explosive, and is used in muzzleloaders. Black powder can be made at home by mixing Potassium Nitrate (Saltpeter) (75%), Sulfur (10%), and Charcoal (15%), or you can buy Pryodex, which is a synthetic form of it and 30% more powerful. The best to use for explosive devices is FFF black powder - it burns fastest, altho we've also seen decent results by tightly packing FF as well. Black Powder requires some care when being used as sparks and excessive heat will set it off. This makes it great as an initial trigger for detonating high explosives - it detonates easily when used with many improvised actuators. Pyrodex is a little harder to set off and thus safer. To be quite honest, it's easier at this time to simply go out and buy Pyrodex instead of making it. It's legal to buy now, and since the ingredients are harder to get, they're better used for other things.

SMOKELESS POWDER: The nitrocelluose-based propellant used in modern guns. This stuff is legal as it's used by reloaders, and is more powerful than black powder. Available in many different types.

DEVICES

"THE JOHNNY CAMPO BOMB": This formulation was downloaded from a hacker BBS with a solid reputation for accuracy. It's an excellent harassment device, and is also effective for clearing out crowds.

<u>Materials</u>: M-80. A large cylindrical cardboard container. Several cans of Comet cleanser. Roll of electrical tape.

<u>Procedure</u>: Fill the container half-full of Comet. Poke a 1/8 inch hole in the side of the container at the halfway point. Insert the explosive in the center of the container, running the fuse thru the hole. Pour more Comet over the explosive to the top of the container. Tamp down the Comet well. Put the lid back on the container, and reinforce the lid and base with tape. When this goes off, it sends out a large green, persistent and toxic cloud.

GRENADES: Fragmentation grenades can be made simply by taking high-explosive, putting it in a container, and adding BBs, screws, nails or metal scrap to the outside. Or you can take a metal pipe, heavily score it around the outside, and use that as the casing. For authenticity, get a couple of dummy grenades from a military surplus store, and use them as a casing. A small-scale (relatively speaking) grenade can be made by taking a M-80 size firework, dipping it in glue and then rolling it around in a plate of BBs.

CLAYMORE MINES: A claymore mine is basically a directional grenade. You take your high-explosive, put it in a casing that will only blow out one way and then add some shrapnel to the weak side. Claymore mines are very useful in guerrilla warfare for boobytraps and ambushes. If the Claymore is activated electronically, proximity circuitry should be added so that if the Clay more is tampered with once set (ex: turned around), it becomes a dud.

SHORT TOPICS

Smaller articles are presented in this section.

SURVIVAL INVESTMENTS

When the collapse occurs, it is far better to have stores of dehydrated or freeze-dried foods than precious metals and rare collections. Why?

(1) You can't eat precious commodities. Therefore, you will be forced to leave your protected area and make yourself vulnerable to trade your precious commodities for the necessities of life - food, water, clothing, medicine, weaponry, etc. What would stop the person you are dealing with from simply killing you outright and taking it all from you? Remember, he knows that time is on his side and that you must deal with him on his terms and on his turf because you're need must be fulfilled.

(2) The people who sold you the precious commodities will know who you are and where you are at, or at least have a good idea. This information is of big survival value to them. When the collapse occurs, they can either attack you directly or sell or trade that information to someone for something they need. Your possessions aren't secret from Day 1. You are far less likely to be noticed by those you buy food, clothing and medical supplies from before the collapse, and you can easily buy them anonymously with cash. The people who sell you guns and ammo know who you are but that information is of less value to them because they sold you the very means to defend your guns and ammo with and many people own weaponry.

(3) Your precious commodities have to be assayed or otherwise evaluated at each trade. The necessities of life have easily demonstratable qualities and quantities. There are few experts who can knowledgeably and trustworthy appraise precious commodities even during stable times. Even if you were very lucky to find such a person after the collapse, on what basis could he sensibly price your items?

(4) Altho when compared to the necessities of life, precious commodities have little comparative value, some have much less value than others. For example, gold and silver will retain some value because there are utilitarian uses for these metals and they preserve very well, while rare paintings and stamp collections will have little value.

The premise for hoarding precious commodities during hard times has its roots in the immigrants who escaped oppressive regimes with the clothes on their backs and whatever valuables they could sew into their linings. Precious commodities take the smallest space for the greatest value. But always remember that they are valuable only where friendly, unthreatened and comfortable people live who enjoy a strong economy and a well-established market for these items.

Be careful in the investments you make in dehydrated and freeze-dried foods. Many firms selling these items are grossly overpricing them and misrepresent their quality and quantity.

URBAN SURVIVAL RULES

If you don't want to become the next violent crime statistic of your gotham, it pays to follow a few rules. These rules much reduce the probability that you will be robbed or raped:

RULE #1: All strangers should be considered as potential threats. Don't allow yourself to be distracted, isolated or simply stopped on the street by any stranger. Criminals prefer victims who have stopped moving. That makes it easy for them to finalize their plans. Keep going and don't slow down for any disturbance you see on the streets. And don't move about or necessarily react in predictable ways.

RULE #2: Walk down the sidewalk nearest its street edge. Walk in the middle of the street if there is no traffic (watch for traffic anyway). Be particularly careful of corners, doorways, between cars and all shadowy areas. Cross the street frequently and randomly.

RULE #3: Always be alert. Look ahead up the street to anticipate any problems. Turn around one complete turn at least once every city block, but in a random way. If you spot people loitering or moving about suspiciously, abruptly change your direction, and always be on the lookout for escapes and police. Avoid confrontations - even with bums. Always keep out in the open with many escape options.

RULE #4: Avoid places where gangs of juveniles or members of other races, ethnic groups or economic classes (that you feel may be hostile to you for that reason) congregate. Juveniles are particularly dangerous because, in recent years, they have tended towards violent, brutal and senseless crimes.

RULE #5: Never show money in public. Criminals are constantly on the look out for this.

RULE #6: If possible, avoid conditions so crowded that you could be pickpocketed. A simple nudge from someone could actually be them taking your money/valuables.

RULE #7: Never bring out a weapon just to warn off a potential assailant or a weapon you are not familiar with, as it can be turned against you. If you brandish a weapon - use it!

RULE #8: Elevators are particularly dangerous. There, you can be trapped by a criminal with no witnesses and no hope of immediate help. Never allow any elevator you are in to go either to the basement or the top floor (can be a maintenance facility). Observe the elevator indicator. If you are on the first floor and the arrow points down, don't get in unless you know what's in the basement. If you are in an elevator and a dangerous-looking character gets in at a subsequent floor, immediately get off. If no one else is in the elevator, push the top floor button, but don't get in. Watch the indicator as it goes up. If it stops on any floor on the way up or back down, chances are a criminal is waiting.

RULE #9: If someone approaches you on foot while you are walking, do not let him get too close. Say something like, "I can hear you from there, don't come any closer." If he still approaches, warn him again much louder and angrier. If he still approaches, immediately prepare to fight or flee. If a person approaches you in a car, always maintain a minimum distance of at least 25 feet from the car, and don't approach the car if beckoned.

RULE #10: When you leave your hotel or motel room, wedge a small piece of folded paper or match stick close to the bottom of the door between the door and the jam. If it isn't there when you return, someone has entered your room. If this happens, go back and get security personnel to enter your room FIRST. This is also a very good technique to use on your home's doors when you go to work, on a trip or just to run errands.

RULE #11: Never open your door to strangers for any reason without first verifying thru a satisfactory identification that the person is a service person you called, police officer, delivery man, etc. Any crook can buy an authentic looking badge and uniform - depend upon a verifiable ID only.

RULE #12: Avoid habitual and ritualistic behavior. You may not think anyone notices, but criminals make a habit of picking up on behavioral patterns. Elderly people and college students in particular tend to develop habits. Criminals look out for these habits, and victimize you accordingly. Always vary your behavior outside of your home. For example, if you use an outdoor laundry, try to use several and randomly vary your visit times for each.

RULE #13: Be stingy with the personal information you divulge, whether on an application form or in chit-chat with your local grocer. Keep a low profile, and don't do anything that will bring attention to you.

HOW TO NEUTRALIZE BUREAUCRATS

I know of no one who hasn't had at least one very upsetting encounter with a bureaucrat. I know of some who must deal with this problem daily. Bureaucrats are often rude, cavalier, insulting, intimidating, ignorant, lazy, irrational and incompetent. Fortunately, tried and true methods have been developed for obtaining justice from these jerks.

One method, called the Psychopathic Killer Method, is used to place the bureaucrat in some state between a deep uneasiness and abject fear. No open threats are ever made because they have a strong mechanism in place to deal with threats. None need be made. The answer is psychological warfare - by using an appearance and subtle, ominous remarks. This puts the bureaucrat in a situation he can't deal with without incurring a substantial lawsuit for false arrest and harassment. Any panic on the part of the bureaucrat immediately puts you in the driver's seat. Most will simply quit screwing with you and treat you with the respect you deserve - since you are paying their salary.

Consider these approaches:

APPROACH #1: THE MOTORCYCLE GANG MEMBER

(1) Dress like a motorcycle gang member. Spread a little grease and dirt on as appropriate.

(2) Motorcyclists are perceived to be crude and unwashed. Don't bathe or shave for at least three days prior to your appointment. Wash down some garlic with some whiskey prior to going in (but don't drink). Muss up your hair (which should be long and stringy).

(3) Leave a chain dangling from your pocket like the kind used to secure motorcycles with.

(4) Wear silvered glasses. These are the types of glasses associated with psychotic killers and motorcycle cops. The bureaucrat feels very uneasy staring at himself in your glasses. Further, it makes it difficult for him to pick up on your reactions (that he can exploit). It makes him wonder just where you are coming from. What he doesn't understand, he will fear.

(5) Never take your eyes off the bureaucrat. Keep a fixed sneer on your face.

(6) Invade the bureaucrat's space as much as possible. Project your face and body as close to his as you can without actually making contact or appearing threatening. Position your body between him and any escape route he may be contemplating.

(7) Say as little as possible. Grunt when that suffices - it has a wonderfully communicative effect. Use minimal gestures and be completely devoid of pleasantries.

(8) When you do speak, do so slowly and deliberately (with long pauses) and use subtle threats. For example (upon seeing a family photo), say, "Is that picture of your wife? She looks real pretty right now." Remember, many bureaucrats will not hesitate to ruthlessly destroy you and your loved ones and have left a long, bloody trail of destroyed lives. You must fight evil with evil. In most cases, the purpose of this approach is purely bluff and is used simply as a means to gain an end. How much realism is involved is solely up to you.

(9) Well before your appointment date, find out who you will be meeting with and investigate him. The Freedom of Information Act will net you his salary, GS level, education, experience and work history, but may be too obvious to use and alert him about you (usually resulting in a last minute switch). Phone directories, contacts with the bureaucrat's co- workers and associates are usually helpful. Accessing his credit bureau records is about optimum, and there are many ways of getting them. Or follow him home, preferably using a bumper beeper on his car. If you can get dirt on him, all the better - you might convert an impending bad decision to something very favorable to you.

(10) Make the bureaucrat spend a lot of time with you. Don't rush the interview. You want to extend the pain to its maximum amount so that the bureaucrat caves into your every demand and will not likely bother you again.

(11) Start the interview with a hard hand squeeze, then thru the interview, pick your nose (wipe the proceeds on the bureaucrat's desk), and then scratch your armpits, genitals. Burp and fart to your heart's delight. Remember, if you have not left the impression that you have 10 strains of VD plus jock rot and lice, you have miserably failed. You have the advantage as long as you keep him guessing.

There are other possible approaches: Mafia Hit Man, Terrorist, Street Gang Member, Drug Cartel Member, Mad Scientist, Survivalist and Lunatic are some other possibilities. The approach you choose depends largely upon which role is most comfortable and believable to you. If you are a large, hairy, tattooed and tough looking, the motorcycle gang member role is about ideal for you. However, if you are thin, pale and delicate looking, the organized crime hit man or mad scientist is a good approach. If you look like your from the Middle East, the terrorist image might be most convincing. If you are a member of a racial/ethnic minority, the street gang member is a convincing choice. The important thing is to be convincing. You'll be most convincing if you play on the prejudices of the bureaucrat.

IMPORTANT MATERIALS

Your ability to improvise is probably one of the most important skills you must learn as a Survivalist. Improvisation requires considerable knowledge and experience. And a supply of useful materials. I have found, over the years, that it pays to browse thru electronic, hardware, plumbing, automotive and hobbyist stores and shops to learn about new materials and methods to aid in my improvisations. This knowledge not only helps tremendously in the field, but when properly applied, can save your family $ Thousands each year because it results in do-it-yourself activities that are much cheaper and more effective and efficient. To get them even cheaper, I keep a keen eye open for them in garage sales, flea markets, etc. The products listed below are largely found in electronic stores:

(1) SILICONE RUBBER CEMENT/ SEALANT: Of all of the cements and sealants, I find that Silicone Rubber Cement/Sealant (ie: RTV) is one of the most useful. While epoxies dry very hard, they are also brittle and refuse to stick over periods of time, thus limiting their usefulness in the field. And crazy glue is primarily best for small jobs.

In the cement style, the cured RTV is harder and quicker drying than in the sealant style, however, the sealant has much better flow and adhesion. RTV also works very well as a filler, mechanical isolation against shock and vibration, and as a potting substance. And you can get RTV for special applications (ex: gasketing, high-temp, etc).

One area where RTV works surprisingly well is to seal against gasoline, solvent and other hydrocarbon leaks.

Another area where RTV (sealant) works surprisingly well is clothes. It can be used to seal seams that are coming apart, to mend tears and to apply patches. And it won't come off in the laundry.

RTV does stink, but its smell is due to acetic acid (same stuff in vinegar) and is not known to be harmful. The cure time for RTV largely depends upon its exposure to air. The greater ventilation of the site, the faster the cure. However, if you use it as a filler or potter, the inner part of the RTV mass may take weeks - even months to properly cure.

(2) CABLE TIES: Cable ties are nylon strips 1" to about 2' long and 1/16" to about 1/2" wide. They are normally used to permanently secure bundles of wires and cables. They have serrations on one end and a slot on the other end containing a tiny slanted piece of metal or plastic. You insert the cable tie's tail into the slot, pulling it thru, thus reducing the loop's diameter until in squeezes down on the material to be secured. The slanted piece ratchets on the serrations to provide a very strong grip that can only be broken by cutting the tie. Some non- electronic uses include:

(A) To securely bundle multiple items of virtually any description that you can find a large enough cable tie to encompass (ex: matches, ammo, gun parts, tools, etc).

(B) To secure one item to another when normal mechanical attachment is not practical. For example, they can be used to secure a scope to a rifle or improvised parts together, etc.

(C) To bundle soft items into compact bundles, such as clothes, rope, wire, etc.

(D) To keep related or paired items together, such as shoes, socks, gun parts, etc.

(E) To seal containers by securing lose tops. And to latch boxes, cages, etc. To replace other types of clamps, such as vehicle hose clamps, etc.

(F) For handcuffs. The strength of 1/4" wide cable tie exceeds that of the strongest man on earth.

(3) HEAT SHRINK TUBING: (HST) and Tape are about the greatest thing invented since sex, integrated circuits and silicone rubber cement. HST is made from a special plastic that, when heated, doesn't burn or melt but shrinks to about 50% of original diameter. It was originally intended to splice wires together in harsh environments - still one of its greatest uses.

HST uses are virtually unlimited. It can be used to insulate the handles or shafts on tools, athletic equipment, etc. To insulated electrical parts. To join any pair or group of mechanical parts together. To protect a surface from corrosion or wear. To protect a part from mechanical damage. To increase the diameter of a part so that it fits properly with another part not exactly made for it.

I have found HST's best uses lie with any mechanical problem that defies normal solutions. A good example is eyeglasses. I used to have an expensive pair of gold-plated metal eyeglass frames. The plastic earpieces developed cracks and the metal began to rust inside of them. I tried every cement known to man and couldn't stop the process. I finally shrunk on a 6" segment of HST tubing on both earpieces. The frames lasted me for another six years.

WILLIAMS' COMBAT PRINCIPLE

Have you ever wondered why some guys get shot in combat while those around them escape death? Purely a case of luck? I don't think so. Of course, some luck is involved. But after talking to a number of combat veterans (as is myself), I have confirmed a long held belief that I call the **WILLIAMS' COMBAT PRINCIPLE.**

The major factor that determines who gets shot at (and thus wounded or killed) has more to do with human nature than anything else. Have you ever walked into a room with several bugs on the floor. Instantly, you spot one bug and relentlessly chase and stalk it until you've killed it or it escapes - altho other bugs may be easier targets. Why did you pick THAT particular bug? Proximity? Yes, partly. Or was it some characteristic - even a subtle one - that compelled you to attack THAT bug? Yes, mostly.

Infantry combat is similar. You are with a group of soldiers opposing an enemy group of soldiers. You see a number of the enemy approaching. Unless they are closely bunched together, you tend to single out one or a few individuals and then to relentlessly try to kill them over the other targets. For brief periods, your obsessed mind blocks out the entire world except the narrow focus of your target. Why did you pick that particular target? You fixated on THAT target due mostly to one of its personal attributes. Those attributes might be behavioral and-or physical. They may make perfect sense (ex: the target looks like a leader). Or they may not. The human mind is designed to be highly discriminating. Recognizing patterns has been clearly demonstrated in psychological tests (ex: Rorschach Test). Have you ever gone to a dance filled with people, and after eyeballing the place, you suddenly zoom in on a particular person across the room? That's because your brain carries clearly defined and sometimes highly complex patterns in it that relate to other people and things. The closer that a person resembles that pattern the more that you will automatically notice him. You almost can't help it.

In combat, you definitely don't want to become such a target. The moral of the PRINCIPLE is that you much lessen the chances of that happening if you do not have any dress, mannerism, action or other appearance that makes you "stand out" on the battle field. Don't act like a leader. And don't be loud, cocky, overly confident or even cowardly (no matter what army is involved - everyone instinctively hates the coward). Don't wear your clothes or gear differently than others or anything that is unusual or flashy (ex: badge, medallion, watch, red scarf, etc). A different appearance helps the enemy to focus onto you, and anything eyecatching acts as a convenient target to place into the crosshairs. Make as little noise and motion as possible. Don't be in a position where you are either in the center of things or on an end or perimeter. And avoid areas better lit than others.

And analyze the other casualties. When they were shot, what were they wearing, what were their physical characteristics, how were they acting and what were their positions? Keep in mind that some people get shot simply because of bad luck. However, given a good enough sample, do you observe statistically significant common charactertstics? And if so, how do they compare to your characteristcs? This effort is worth it because your life depends upon it. *End of manual.*

THANK YOU FOR ORDERING "BY AN ORDER OF THE MAGNETUDE". The best of successes in all that you do!

--- *The Authors*