Cybertek

Issue 9 — Technology, Security, Self-Reliance — January/February, 1995

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

Steps to Self Reliance and Preparedness

by Thomas Icom

Clearly, the bad times are upon us. When one examines the rising crime rate, record inflation, withering of young people's minds by an educational system more interested in promoting socialism than educating, totalitarian government policies being established, and the spin-control propaganda issuing forth from the mass media it becomes apparent that an epic disaster of unprecedented magnitude is due to happen shortly.

Some people disagree and state that the disaster has already occurred slowly over a period of time, and that the events we are witnessing today, the ones I stated earlier, are actually the beginning of a new dark ages. Whatever one believes, one thing is certain. Times are changing and the changes aren't for the better.

All is not lost however, for those who recognize society's downward spiral and take the time to make appropriate preparations for the survival of these perilous times. Those with the foresight to take the necessary measures to protect themselves and their family will weather the stormy days ahead, and leave a priceless legacy for their descendents.

As more people recognize the danger signs of what's to come, they realize that there is no help to be found from the mass media. When the media does recognize a real problem, the rising crime rate for example, the automatic response issued forth by the editors and anchormen is to cry for increasing legislation and restriction of the citizens' right to self-reliance and preparedness. Certain traitorous types in our government seem to be only too willing to accept their suggestions.

This situation does nothing to help those who desire to take control of their own lives regardless of what the future might throw at them. It has already resulted in the genocide of thousands of people in this country who were denied by various local and regional governments an adequate means to defend themselves against crime. It would seem that select people in the government and media are purposely trying to worsen this country's situation so that they might be able to institute a socialist totalitarian Amerika, and enslave the masses.

To take charge of your life, achieve true freedom, and maintain self-reliance from the establishment the following steps are recommended:

1) Acquire firearms of known reliability, common caliber and availability, along with sufficient parts and accessories (magazines, slings, scopes, etc.) Become competent with your weapons and learn about improvised weaponry and military tactics.
2) Maintain a reserve ammunition stockpile for your weapons. The minimum recommended amount would be at least 500 rounds per weapon, with 1000 rounds being preferable.
3) Purchase gas masks and learn about defense from nuclear, biological, and chemical hazards.
4) Form into groups of three to ten trustworthy and reliable people.
5) Keep your group's profile low and refrain from overt activity that would attract unwanted attention.
6) Develop alternate communications systems such as couriers, radio, or computer networks.
7) Gather as much intelligence as possible about the various factors affecting your survival in your area and surrounding regions. Make your group's plans according to information you receive.
8) Stockpile a minimum three month to two year food and water supply for your group.
9) Acquire communications equipment: CBs, scanners, ham radio equipment, shortwave receivers, modems, packet radio equipment. linemans' test-sets, etc.
10) Acquire a reliable, common, easily repaired vehicle. Collect spare parts and try to keep a minimum of 40-50 gallons of fuel on hand.
11) Learn about alcohol fuels. Be able to set up a still and convert your vehicle for alcohol fuel use.
12) Make at least five copies of this article and anonymously send them to people whom you feel will make use of it.
13) If you haven't already, learn a useful trade that will enable you to earn a living in a rural area. Stockpile tools and materials relating to your trade.

14) Move to a rural area if possible. Acquire a 1-2 acre (more if you desire and are able to do so) buildable (or already built on) plot of land near a small town/village.

15) Learn about first aid, wilderness medicine, herbal, radionic, and other alternative medical and health techniques, field sanitation, and communicable disease control. Study for and acquire an EMT/Paramedic certification and beyond that if possible, and you feel particularly drawn to the healing arts.

16) Learn at least the basics of producing/acquiring your own food. If you know how to do this, you'll be O.K. no matter what happens to the stores. Having a working knowledge of hunting, fishing, gardening (particularly small-scale hydroponics), trapping, homebrewing, and raising animals will save you money in food bills, and possibly save your life sometime.

17) Learn the basics of shelter building. As long as you know how to get a basic roof over your head under varying conditions, you'll be O.K.

18) Never stop learning. Knowledge equals freedom.

These steps represent a basic starting point for those readers interested in true self-reliance and preparedness; not the ramboesque bullshit that often passes for it.

The aim is to be a jack of all trades and master of a few that will help you live independently from "the system" as much as possible. Actually, it's not as isolationist as it sounds. You should be participating in the economy of the small, pleasant community where you live. The "system" you'll be independent of is the mess that's responsible for this country's decline.

While you are getting your ground level education in the various self-reliance fields, you will undoubtedly be drawn to particular ones. Those are the ones you should specialize in and master. This may seem a tall order. Some will say it's impossible. In the days before TV our ancestors did exactly what I am suggesting. Take out your 12 gauge. Put a round of 00 buckshot into that damned idiot box. Mail it to Dan Rather as a token of what you think of him. With that accursed distraction out of your way, you'll have plenty of time to learn what you need for the hard times ahead.

"A people who mean to be their own governors must arm themselves with the power knowledge gives."

- James Madison

Ψ

Citizen's Band Communications

by Thomas Icom

People looking for an inexpensive way to communicate via radio often choose Citizen's Band, or "CB" as their means. CB is probably the most widely used communications band in the U.S.

CB has a colorful history in the U.S. In the late 70's and early 80's it was the focus of a great fad in this country which resulted in several movies and popular songs of the era. Unfortunately, this publicity caused the band to lose it's reputation as millions of people "put their ears on" and used it to practice their southern accent.

While the "good buddy" era has passed, most people still have a CB in their car as it remains the best way to determine highway conditions and request assistance when stuck on the road. In any semi-populated area, a CB tuned to the right channel is an effective intelligence source of the jungle telegraph variety. When something happens "so-and-so" gets on the horn to "what's-his-name" and gives him all the details. After a disaster, the common availability of CB equipment will make monitoring the CB band a necessity to gather intelligence from individuals who will be transmitting real-time news from the disaster area. After the collapse it will help you determine the intentions of some of the many groups who will be roaming around. Hearing a marauder band five miles down the road heading towards your homestead will enable you to make special preparations for their arrival. (For more details, refer to the Claymore mine plans in Issue #8 of *Cybertek*.)

The CB band consists of 40 channels between 26.965 Mhz. and 27.185 Mhz. Power output is limited to 5 watts using AM transmission and 12 watts using Single Side Band (SSB) transmission. The typical range for reliable CB communications is 5 to 20 miles; although when atmospheric conditions are right, worldwide communications is possible.

The main advantage and disadvantage to CB is its wide availability and broad usage. As paradoxical as this sounds, it is true. These characteristics of CB enable you to accomplish several important things. CB gear is inexpensive and widely available. You will be able to buy your rigs at Radio Shack or a department store and assemble a sizable communications network easily and for relatively little money. Since CB is in very common use, your group's communications will be go unnoticed among the thousands of other people who are using CB in your area.

Having CB gear in your possession will not call attention to you any more than it would for everyone else who owns it. CB will also probably be the ideal inter-community party-line and "hailing frequency".

However, the same characteristics also cause problems. The sheer number of users causes interference which hampers your range. Everybody with a CB (meaning everybody) would be able to listen to your group's operations, and know that you were in the area. Those same listeners would be able to disrupt your communications just as easily as they are able to listen in; with a variety of means ranging from simply keeping their microphone keyed to recording and playing back your previous transmissions to confuse you. While this is true to a certain extent with all forms of radio communications, electronic countermeasures is most

easily conducted against CB communications. Your group should have a CB rig in its commo shack and in every vehicle for use as an intelligence collection aid, means of communications with the outside world, and alternate communications network for your group. Any base or mobile CB acquired should have SSB capability, as SSB gives more range for the power used, due to it's narrower, more efficient signal. To the best of my knowledge, there are no walkie-talkie CBs that have SSB.

The rigs you buy should be capable of being modified for extra output power and extended frequency coverage. The higher output power will extend your communications range, and the extended frequency coverage will give you extra channels that offer a little more privacy. Several books are available via mail order that provide details on such modifications. Note however that modifying CB radios for extra power output and frequency coverage is against FCC regulations unless you are an amateur radio operator modifying them for 10 meter band (28 Mhz. to 29.7 Mhz.) operation. Should you get caught violating FCC regulations you're equipment will be seized, and you will most likely get hit with a sizable fine.

Since you really have better things to do with your money, I suggest you play it safe and obey FCC regulations. After the collapse occurs however, whatever works to help you survive will be the order of the day, and I think there will be worse things to worry about when the balloon finally goes up than the FCC.

Whenever possible, you should use SSB for intra-group communications. Most CBs used by the general public only feature AM mode as that form of transmission requires less operator expertise to use; especially in a vehicular setting where the driver is also the radio operator. In addition to providing better range, SSB transmissions will sound "garbled" on an AM-only rig. This will provide communications security against low-end CB users (the majority of people who use CB). For those of you who are wondering, a properly tuned SSB rig will be capable of receiving AM transmissions so you'll be able to hear AM CBers on the same channel while in SSB mode.

When using a communications mode as popular as CB, some form of communications encryption is a necessity. Design a code system for use with your CB gear and change it on a frequent basis. Design it so that it makes your group's communications sound like typical CBer activity; such as a few fishermen chatting about lake/stream conditions or local residents catching up on gossip. A system like that is superior to a code system that sounds military because listeners will assume that innocuous sounding conversation is what it appears to be; whereas if you sound high-speed people will know something's up even if they can't understand what you're saying.

Those of you interested in learning more about Citizen's Band communications and CB modifications should refer to the following:

Recommended technical manuals for CB equipment; repairs and modifications for better performance and 10 meter ham band usage:

The CB Radio Hacker's Guide, by Kevin Ross
CB Tricks of the Trade, by J.L. Richardson
CB Tricks II, by J. L. Richardson
The "Screwdriver Expert's" Guide To Do-It-Yourself CB Repairs and Modifications, by Lee Franklin

Good general guide to CB radio; history and operations:

Tomcat's BIG CB Handbook, by Tom Kneitel

All of the above are available from:

CRB Research Books, Inc.
P.O. Box 56
Commack, NY 11725
(Catalog: $1.00)

An excellent source for CB technical information, parts, services, repair books, and high performance accessories is:

CBC International
P.O. Box 31500PC
Phoenix, AZ 85046
(Catalog: $2.00)

Popular Communications is a general radio communications / radio monitoring magazine that covers CB as part of its focus. It's available at any decent book store (Barnes & Noble, Borders, even Waldenbooks) or news stand.

Ψ

Survival Notes (# 1)

by Wildflower

DRYING WET BOOKS: Can be a long messy process of taking apart the books, separating the pages, and waiting for a long drying period, which rot & mold can still destroy the book permanently. At least that is the old process, for many years. Nowadays, whole books can be slowly dried faster at low power setting in a microwave oven. This process eliminates separating the pages, restoring the whole book at the same time, without major water damage, even eliminating insects & mold in the drying process.

CACHE STORAGE OF BOOKS: Utilizing a $50 vacuum & heat sealer, sold in most major department store chains, a book can be stored in a plastic bag, which has been vacuumed of air content, then heat sealed. Then the bagged books are stored in a waterproof container, such as a surplus ammo boxes, and then buried in walls, or ground.

If a book is zapped at low setting for 10 minutes in a microwave oven, this would eliminate excess water content, insect eggs, and any mold spores; before bagging the book. The vacuum & heat sealer machine can also be used to prepare moisture & mold sensitive articles, for safer storage. For example: clothing items, bandages, matches, toilet paper, ammo, etc. A good rule is to cache away items

essential for survival, essential to make other items with, or items hard to make or find later on. Examples: matches, magnet wire, transistors, primers, thermometers, etc.

I can build my own resistors, capacitors, even relays, but a transistor be damn near impossible. Can grind my own gunpowder, but harder to make a decent primer for the shell. Taps & dies, which I can make nuts & bolts with, are just as necessary as a hammer for my shop. It's easy to make candles & soap, yet easier if I lay in a few years worth now, before being forced to, create them.

AFTER THE COLLAPSE: Within ten years, most fuels will be either used up, or have deteriorated beyond usability. Most people then would have to depend upon "homemade" fuels: methane, alcohol, wood gas, wood, hydrogen, and possibly methanol. these fuels, expensive to make in any great quantity (in terms of man-hours), all be used carefully in whatever surviving or homebuilt machines then in use.

For travel, most would be: on foot, bicycle, horse, by sail boats, by canoe & paddle, or rarely a motorcycle of even a moped, and even rarer by automobile (As years go by, what roads will be left?).

But there is another mode of travel ignored by most post-collapse planners. This is travel by aircraft, of many sorts!

Take for instance, microlite aircraft, able to take off and land from afield, cruise about on very little fuel, while covering many miles of travel. And for heavier craft, bush pilots for years have flown one and two engine craft, equipped with pontoons and wheel combination for land/water takeoff/landings. During WWII, Japanese aircraft flew on alcohol, even local homebrew!

Or how about hydrogen/helium balloons or dirigibles for travel. If properly constructed, they can be used for world-wide travel, and even carry their own fleet of aircraft along for fast reconnaissance/defense or ground to air shuttling of passengers and cargo! Yes, hydrogen is very flammable, but until you find enough helium to replace it (by salvaging from welders's supply or recovering from natural gas wells), can be used safely. Heck the Germans did it for awhile!

For heavier cargo, probably be moved by restored rail service, rebuilt canal barge systems, or by steam tractor road trains. As for major highways, only those maintained by private road companies will still be used.

And no doubt, various technical survivors will utilize cellular phones, shortwave communications, fax machines, and computers, either from salvaged systems and parts, or if possible locally manufactured!

This means of course, just how well prepared you have made your "survival" library. Yes, one is going to have to include whatever books cover the design & manufacturing of the high tech items you will need, along with the tools or information on constructing those tools, necessary to build hydrogen proof fabrics, helium recovery systems, or cutting silicon wafers into integrated circuits!

Also be good now to prelocate by using maps and phonebooks, various industrial manufacturers and suppliers for future salvaging after the collapse. This will safe many man-hours and fuel supplies for your recon & salvage scavengers later on.

Same can be said for any local welder's suppliers or natural gas wells in your area.

ALTERNATIVE ENERGY: If you can afford to buy your solar cell panels, hydroelectric generators, even wind generators now, do so. If possible, invest in all usable alternative systems practical for your area and needs.

As for the cost, do remember even a solar cell panel of 1 amp production, will be well worth having when your local utility dies for good, someday! Or how much would you pay just to switch on a light, especially when the power is gone forever.

LAST: After the collapse, it would be nice to hold a convention for all you fellow survivors, whom made it! And for those whom didn't a mass pee-off on their common grave site (after the homebrew beer festival)!

All for now.....

LIVE LONG & FREE!

*Wildflower*94*

Ψ

Deciphering the Radio Sticker Code

by Thomas Icom

To make things easier on customers and salesmen, radio manufacturers place little star or circle (dot) shaped stickers of various colors or with various letters on their low-end radios and packaging which have been configured for operation on popular low-power and itinerant frequencies. This sticker indicates what frequency the radios operate on.

Knowing this code will help you when you're purchasing surplus or used equipment at hamfests and auctions. Even if the radio's batteries are dead/missing or you don't have your frequency counter handy, you'll know if it's compatible with the rest of your equipment. Knowledge of the code will also aid in doing SIGINT (Signals Intelligence) work if you have no frequency counter or scanner handy. If you can get a decent glance at the radio being used by the target, you'll be able to determine the frequency for later interception. This sticker is usually on the lower front or back of the radio. This enables you to see the sticker when it's either resting in it's belt carrier, or when it's being held up to the operators head while being used.

Blue Dot - 154.57 MHz Green Dot - 154.60 MHz

Red Dot - 151.625 MHz Purple Dot - 151.955 MHz
Brown Dot - 464.50 MHz Yellow Dot - 464.55 MHz
J Dot - 467.7625 MHz K Dot - 467.8125 MHz
Silver Star - 467.90 MHz Gold Star - 467.875 MHz
Blue Star - 467.925 MHz

Ψ

One-Time Cipher

by Nick Halflinger

This is a one-time cipher. The formula used is sin(x^3). The program asks if you are encoding or decoding the data. Type E or D. The program asks you for the PLAINTEXT file name. This is the english (or binary) data when it is not coded. The program asks you for the CIPHERTEXT file name. This is the encrypted data.

The program asks you for the starting value of X. This is one of the two parameters that are special. The program asks you for the step value of X. This is the other special parameter.

To decipher a message, you need both the START and STEP values. If someone else finds these values, then the data can be read. You must find a way to decide these values so that nobody else can figure them out. You might want to use things like the file date/size, or something. They can be any real number.

If you don't know what a one-time cipher is, or why it is secure, find a good book on ciphers or security and find out. This is not the place for a description. You don't need to understand what makes this secure, but it does help.

I've tried about 1/2 meg of sample data, including executable files and text files. There has not been one single error in encryption/decryption in that time. However, I can't guarantee that there aren't any bugs. If you put the wrong filenames in the wrong places, you may overwrite your source data. The program is very basic and doesn't check.

```
{prototypical one-time cypher system}
PROGRAM one_time_cipher (input, output);

USES crt;

TYPE
  datafile = FILE OF BYTE;

VAR
  plain : datafile;
  cipher : datafile;
  start : REAL;
  step  : REAL;
  user  : CHAR;
  fname : string;

{our function, which could be anything we want it
to be}
FUNCTION pseudo (x : REAL) : BYTE;
BEGIN {pseudo}
  pseudo := ROUND (200 * SIN ( (PI * x * x * x) /
180) );
END; {pseudo}

FUNCTION encipher (orig : BYTE; value : REAL) :
BYTE;
BEGIN {encipher}
  IF ( (orig + pseudo (value) ) > 255) THEN
     encipher := orig + pseudo (value) - 256
  ELSE
     encipher := orig + pseudo (value);
END; {encipher}

FUNCTION decipher (orig : BYTE; value : REAL) :
BYTE;
BEGIN {decipher}
  IF ( (orig - pseudo (value) ) < 0) THEN
     decipher := orig - pseudo (value) + 256
  ELSE
     decipher := orig - pseudo (value);
END; {decipher}

PROCEDURE encode;
VAR where   : byte;
    current : real;
    tempval : byte;
BEGIN {encode}
  REWRITE (cipher);
  RESET (plain);
  current := start;
  WHILE NOT EOF (plain) DO
        BEGIN {while}
        READ (plain, where);
        tempval := encipher(where, current);
        WRITE (cipher, tempval);
        current := current + step;
        END; {while}
END; {encode}

PROCEDURE decode;
VAR where   : byte;
    current : real;
    tempval : byte;
BEGIN {decode}
  REWRITE (plain);
  RESET (cipher);
  current := start;
  WHILE NOT EOF (cipher) DO
        BEGIN {while}
        READ (cipher, where);
        tempval := decipher(where, current);
        WRITE (plain, tempval);
        current := current + step;
        END; {while}
END; {decode}

BEGIN {main}
     clrscr;
     writeln('One-Time Cipher 1.00');
     writeln;
     write('(E)ncrypt or (D)ecrypt');
     user:=readkey;
     writeln;
     write('Plaintext file name: ');
     readln(fname);
     assign(plain, fname);
     write('Ciphertext file name: ');
     readln(fname);
     assign(cipher, fname);
     write('Start value: ');
     readln(start);
     write('Step value: ');
     readln(step);
     IF upcase(USER)='E' then encode;
     IF upcase(USER)='D' then decode;
     close(plain);
     close(cipher);
END. {main}
```

Ψ

Memetic Engineering - PsyOps and Viruses for the Wetware

by Atreides

Managing Director, The Nemesis Group

Bunbu Itchi - Japanese phrase meaning 'Pen and Sword in accord'

Most practitioners of the 'hard' sciences look down their noses at what they refer to as the 'fuzzy' sciences-those domains that are limited to passive observation, with no or only limited application to the real world. This is an understandable chauvinism; when they look around them, they see bridges, skyscrapers, automobiles, airplanes, cellular phones, CAT scanners, synthetic fibers, all the fruits of their labors. What could compete with all that?

Because of this chauvinism (by definition, in fact), a fusion, synthesis, or synergy, take your pick of terms, combining very powerful aspects of certain hard (mathematically malleable) sciences and soft (non-quantifiable), has been seriously overlooked. This may in fact be a good thing; if the repercussions of such a blend of domains are as powerful as they seem, the practitioners of such a new field will, quite literally, wield considerable influence.

Think of this new domain as 'applied sociology' or 'cultural engineering.' Neither name is sufficient description to a field that encompasses: information theory, general semantics, semiotics, cybernetics, neurolinguistics, statistical theory, advertising / propaganda, conditioning, epistemology, epidemiology, game theory, cognitive psychology, sociology, and evolutionary biology. If your eyes have glazed over, or you have already decided that you shouldn't be reading such 'trash' as this, then resign yourself to being one of the sheep. Careful study of Nazism (and Goebbels), Marxism, or Scientology (and Hubbard) give clear indications that the concepts work; from there, it is simply a matter of analysis of the phenomenon to build a new form of engineering, which in deference to its roots, can be referred to as memetic engineering.

1.0 Background

Evolutionary biologist Richard Dawkins, in his book *The Selfish Gene*, proposed a concept he termed *memetics*, a corollary to genetics, but in the domain of the mind rather than molecular biology. A *meme* is a basic unit of memory, but like a gene, can be transferred (via replication); better than a gene, memes can be reproduced by a variety of mechanisms beyond those of conventional biology.

For Dawkins and other biologists, this would function similarly to the discredited principles of Lamarckian evolution, where acquired traits can be passed on to off-spring. On a practical biological level, this is absurd; removing the tails from lizards will not cause the offspring to be born without tails. While physical characteristics are in no way transferable in such a convenient method, psychological characteristics do indeed seem to be. The young of most any species that has parents present through infancy, childhood, and adulthood appear to have a mechanism built in that is geared to learn through imitation; this provides education to the young in a cost-efficient manner for the parent, and so seems to have won out in the natural selection process. In human beings, both behavior and language appear to transfer through this mimicry process; part of our brain, operating independently of conscious will, acts as a 'self programming' computer.

In a typical moment of whimsy, Dawkins wonders if it is possible that Nature views the mind as a whole different eco-system, where memes compete via natural selection for control of a 'host.' Dawkins further speculates that, if true, memes are spreading, mutating, and evolving exponentially faster than their biological brethren; it seems that the human mind is a fertile ground for expansion. Given a cross-divisional background and a cynical view of Humankind, one quickly wonders if this mechanism in the human mind is deliberately accessible and if a specifically engineered meme could be introduced through it, intentionally beneficial to the engineer rather than host. To get to that point, a brief discussion of other relevant areas is called for.

2.0 Mind as Ecology, Mind as Ecosystem

[The material for these sections derives from the works of Shannon, Korzybski, Eco, Wiener, Jung, Kuhn, Hume, Bateson, McLuhan, Von Neumann, Turing, Pavlov, Skinner, and Pareto; I highly recommend their works as a concrete starting place for an avid student to pursue.]

You are an expert on the human mind; after all, you are in possession of one. Unfortunately, you never received a user's manual. However, you have managed to get this far in life, so obviously your mind seems to be able to take care of itself; just like a top of the line automobile, it automagically takes care of the details and leaves the larger issues up to you (extrapolation of this analogy further, implying that the human brain seems merely a tool for the human mind, and further implications from that, are left to the reader). If you think about how you think, you will find your mind is made of memories, facts, and that sort of thing; you picked these up through continual reinforcement and having been there for it (some things can be taught, others need to be learned). Using a computer metaphor, your mind is hardware (the grey matter, providing you with senses, nerve endings, neurons) and software (combined from that odd core of your being that is doing the reflecting, and the material it is reflecting upon, kind of like a computer program

and its data). That isn't the whole story, of course; there is an unidentified extra component, the 'wetware', that gives you free will, volition, self-awareness. We know next to nothing about how this piece works; it appears to be an odd combination of chaotic and stochastic processes, transcending both. About the only thing we know for certain about the human mind is that we haven't even begun to utilize it to its full potential.

3.0 Language, the Building Blocks of the Mind

Very little of what we think of as 'conscious' thought goes on without language. Language seems not so much an expression of thought, but the basic assembly materials of it; as such, it is also the limiting factor to a peoples' thought process (for an instructive example, track the historical tendency in the New World for English speakers to favor free markets and democracy, while Spanish speakers favored controlled markets and oppressive governments). Language has its limitations; for instance, there are some things that can't be represented, only evoked, such as emotions. Communication is thus limited to the realm of dogma, where the symbols passing back and forth between people are just second-hand slices of someone else's point of view. The amazing thing is that it is capable of occurring at all.

When very young, and with the mind acting continually to acquire patterns to imitate and mimic, the basic building blocks of communication become programmed. View them as precursors, primitives, or archetypes, they are critical pieces necessary to interaction with the environment for the rest of your life. When someone tells you something is 'blue,' you are forced back into the original foundation of your language skills; the same for most anything we view as 'baby talk,' those simple one-syllable words that form the least common denominator of all other concepts. Obviously, access to this primal mechanism in the human mind would be quite powerful; access, however, becomes more complicated over time. It appears that without constant use, the capability atrophies, much like a muscle; as we grow and become more sophisticated, higher reasoning centers and capabilities of abstraction come into play, leaving the more basic and powerful 'store and repeat' functions alone. We also tend to create a center of disbelief; while young, it is statistically likely that most of the behavior and language acquired is pro-survival, while later in life this probability radically decreases. Any adult with exposure to children will note how easy it is to convince them of things; soon though, children stop believing in the Easter Bunny or Santa Claus, and other spurious bits that are easy to 'root out.' We gain an ability to be more selective in our beliefs, at the cost of an amazingly robust learning process that is native to the human mind. That is not to say that the faculty goes away, it does not; it is only harder to get to.

Humans develop 'blinders,' a functional inability to recognize or process certain symbols or concepts that do not agree with the operational psychology of the resident wetware. Kuhn, when examining scientific progress, coined the term 'paradigm' to explain the issue; people wear rose-colored glasses that causes them to see or interpret the world around them in a way consistent with that which they already believe. Oddly enough, this seems an odd corollary of the Copenhagen interpretation of quantum reality, or the bane of the professional intelligence gatherer, which is 'you get what you look for,' and in many cases, only what you look for. The human mind has a unique ability to take a large body of data, or an unknown situation, and put whatever interpretation upon it suits them the most, ignoring everything else. Take as given this level of uncertainty as to the underlying 'truth' of things, and sure enough, you come around to 'tell them enough times, and they come to believe it,' the operational philosophy of both Goebbels and Madison Avenue.

4.0 An Expanded Model of Communication

Review of a communication model may be helpful at this point, so a walk-through is in order.

Party Able of the communication begins with an intent, a purpose for wishing to communicate. A channel for communication is chosen by Able; the channel and medium of communication has certain traits which effect the message. There are throughput, how fast you can communicate; bandwidth, how much you can communicate; and interactivity, the degree and frequency with which there is contact with the other party. Proper choice of channel is critical to the ability to successfully communicate the message; a picture can be worth a thousand words, and vice versa. Additional choices, some not consciously, are made - the initial conditions of and for communication, handshaking to confirm that there is a dialog possible, and the basic building blocks to be used to assemble the message, the primitives, precursors, and archetypes. Able then frames the message. This message intends to impart some informational value to the recipient; there is a fine line as to whether such intention is value-neutral communication or manipulation in varying degrees of subtly (a game theory expansion of evolutionary benefits of communication as a tool concretely supports that manipulation of others and their resources is the primary intent of the faculty). The message will contain a variable degree of explicit and implied data points. Explicit hard points are the standard 'who, what, where, when, how, and why'; soft points are 'relative' concepts commonly exchanged in absence of quantification (such as "I'm in pain." which can describe a paper cut or amputation, unknown without referents); and there are also 'null' points such as the format or level of politeness. Implied content to a message can come from traffic analysis (given a statistically significant base to work from) as well as the intentional and unintentional inclusions and omissions in the content (which implies the receiver has at least equivalent or greater knowledge of the content topics to gauge properly).

Able's message may be sent in many forms, many times, via many channels and media types to increase the probability of successfully achieving the intent; variably the intent may require continual reinforcement, thus benefiting from the 'signal saturation,' or this may cause overload in the recipient, to the detriment of Able's purpose.

Party Baker is the receiving party of the message; Baker may or may not be a willing party to such communication. Baker's motivation is to remain integrated and maintain equilibrium; to do this, Baker passes the message (already having potentially suffered loss and noise related to the channel) through a variety of automatic cognitive filters, such as Baker's perception, operational paradigms, interpretations, and frame of reference. What such mechanisms do is strip the message down so that it can be rendered into its useful component parts; the results may be complete acceptance of all content, or total filtration of the message until there is no content. This is a product of the layers built initially by the 'mimicry' mechanism and compounded by later cognitive faculties. Depending upon the medium and channel, Baker may give feedback, reply, ask for clarification, etc. The message may initiate actions or reactions in Baker based upon an accurate match-up of releasers, gestalts, and concepts that evoke a response.

Baker may initiate a message, becoming the Able party in the model, but the message must be reviewed in the light of the initial trigger. Is the content of the initial message continuing on (thus successfully causing replication or transmission, being a meme with contagion)? Has the content changed? If so, was it done poorly (bad replication, a decay, like the game of 'telephone')? Oddly (mutation)? Improved upon and added to (aggregation)? Did it spur new content (offshoots)?

Taken in its entirety, even basic communication is incredibly complex; as stated earlier, it's amazing it occurs at all. As is evident in the model, however, is just how closely communication of ideas seems congruent with the spread of infection; review of some basics on disease will help clarify this further.

5.0 Diseases and Other Automata

No matter what else may be an apparent effect, the only purpose of a disease (and automata) is that of reproduction and metabolism. Everything else is secondary; most flu symptoms are caused by a virus intent on replicating itself into additional hosts; the potential eventual fatality of the host is meaningless to an unreasoning reproduction mechanism that cannot foresee the results in the event of it actually succeeding (a game theory expansion on this with 'rational' players requires the use of new positions "don't lose" and "don't win" and is highly educational).

Infection, regardless of the source (bacterial, viral, fungal), is opportunistic; all it 'wants' is access to the resources necessary to continue on its quest for expansion. The vectors of contagion, via which the automata reproduce and replicate to additional hosts, are varied channels; all require that some representative sample of the automata, suspended in a mechanism that can support its meager claim to 'life,' be exchanged.

Limits to the growth and spread of such automata are many; the diversity of the domain of potential hosts itself is a barrier, since such variation is beyond the capabilities of automata to reproduce and be transmitted in; the 'yeast growth law,' where the most limited resource constrains the system, also works to the automata's detriment, commonly through limiting the number of new and available hosts in a brownian motion-type expansion.

Certain potential hosts have a susceptibility to being infected, some through genetic or hereditary predisposition, or because of age, with a young, 'inexperienced' immune system, or an old 'tired' one. The host's immune system will commonly recognize the infection for what it is and begin an immune response, an attempt to repel the invader or integrate it into the system. While the host deals with the automata on a 'micro' level, there are 'macro' level actions as well; there are processes of containment, the control and suppression of vectors, 'firefighting' with specific treatments, and 'firebreaks' intended to prevent the spread.

There is an aftermath to dealing with the automata, related to the survival enhancement (value added) or detraction (value subtracted) effects, which may vary from the benefits of E.coli or mitochondria, or an improved immune response, or the damage of an impaired or weakened immune response, or the loss of some resource in the fight for control with the automata. It takes no great stretch of the imagination to draw the parallels between disease-automata and message-automata. Memetics, the study of language-communication-informational automata, will become a generally recognized field of increasing importance. At one point in time, historically, we had no biological or 'germ' theory of disease; because of this, we were late to cope with the effects of widespread access of automata to improved disease vectors (as simple as fleas on rats spreading the plague to the effects of air travel on modern, yet primitive, epidemiology); we are suffering greatly now because such poor understanding has allowed such automata as AIDS to gain a statistically significant foothold, and other 'dead' diseases are returning.

There are now similar vectors in place for memetic type automata: witness the media explosion of telephone, television, cable, fax machines, computer and computer networks, movies, books, magazines, posters, billboards, radio, whisper nets; it is endless. And while naturally occurring biological diseases are simply opportunistic and have no such mechanism, memes can be very accurately targeted, aimed at self-selecting affinity groups that will make 'ideal' hosts.

6.0 Memetics as an Applied Science

Plato banned music from his 'Republic' because of his primitive natural understanding of memetic engineering; the notion of an 'idea' coming along and literally rewriting the nature of a culture is obviously an old one. Examples of memes are instructive case studies and merit examination.

6.1 Primitive and Not-So-Primitive Attempts

Santa Claus is a meme that parents deliberately infect their children with; the purpose for it is quite unfathomable, and seems to run along two paths - it didn't seem to hurt the parent when they had it, and it helps to explain the odd behavior that people go through once a year. The Claus meme in a child helps the way cowpox helped with smallpox; part of growing up is the 'trauma' of learning, once old enough, that Santa is a myth, and that people, including one's own parents, have systematically lied to you. This may seem a callous way to view it, but from the viewpoint of building cognitive mechanisms, this is one of the earliest we gain that fosters the ability of disbelief.

Nazism, the myth of Germanic racial superiority, is an interesting look at a common historical occurrence. Hitler provided the skeleton, but Goebbels and the Propaganda Ministry put flesh on the bones. Use of constant reinforcement, triggering an amazing number of cultural responses such as 'noble sacrifice' and 'total commitment,' use of the 'elite chosen by God' metaphor, indoctrination of the young, all were a masterful implementation by a natural talent. The meme, however, had the roots of its destruction built in, with non-tolerance, the inability to conceive of losing, and the perpetration of unspeakable acts as side effects that combined to kill off those infected. Nazism also gives an example in recent history of a successful meme actually managing to become an operational paradigm for continuing generations.

Religion and cults are understandable when one realizes that a cult is a meme that spreads throughout a population, but once it becomes the operational paradigm in a significant number, it acts as a religion. Judaism is specifically interesting for its exceptions, such as the lack of the ability to convert into the system, and the requirement that the Talmud be exactly duplicated, with no changes or interpretation. These have acted to give the followers a solid cultural identity that has resisted schism and other, not inconsiderable, attacks. The odd beast known as 'Scientology' is another clear example of natural talent at work. Hubbard, a failed science fiction author, created Dianetics on a wager, freely plagiarizing critical concepts from an older 'mystical' group he monitored when younger. Scientology was deliberately engineered to give power and wealth to its creator, while providing an operational 'philosophy of living' to the followers; certain 'religious' functions such as 'clearing' with a pseudo-polygraph device create additional opportunities for control through blackmail. A comparative study of religions and religious history is an instructive lesson in memetics and cultural manipulation.

Finally, the military provides another view of memetics. Military training and indoctrination are a factory for memetic implantation; such training strips the individuals down to their basic core personality and rebuilds them in the image desired by the service. Such training uses many of the accepted tactics of 'brainwashing': de-individualization, sleep deprivation, exhaustion, control of the means of support, immersion into chaos and personal incompetence, and the creation through reinforcement of a new doctrine and identity. It is suspicious, in fact, that military personnel have a unique susceptibility to brainwashing attacks, as it has already been done once; such indoctrination techniques wear down an individual's resistance, but do not necessarily build it back up properly to act as an immunity. Additionally instructive is the lack of success of military sponsored 'hearts and minds' campaigns, where memes are never crafted to become the operational paradigm of the targeted people, and so have instead fostered hostility or resentment through the oversaturation of what the target's view as 'noise.'

6.2 Mechanisms

As the Noble Prize winning physicist Richard Feynman stated, you can't predict the actions of a single thing at a single time because there is no math-prediction is a rough adherence to an average, which requires a statistical body. Use of memetics to manipulate individuals would seem to be out of the question, but the large scale use to manipulate large bodies or cultures is not. Anyone familiar with systems operations is aware that, in rough terms, 20 percent of the members of any average set will produce 80 percent of the effects of the set (for example, 20 percent of the scientific researchers in a given domain will produce 80 percent of the discoveries, or publish 80 percent of the papers). It does not, then, require an unwieldy number of 'converts' to manipulate a large body, as controlling a small number gives the apparent effect of controlling the statistic majority. What is important is the correct identification of those who will be susceptible, reaching them, and doing it with the correctly fashioned message to evoke the desired response.

It is important to remember at this time that the mechanism that can be relied upon for replication of a meme into a host is a primitive one; it is not susceptible to reasoned arguments, or sophisticated ones. This is more of a case of life imitating art; people don't perceive reality, only their perceptions of reality - everything is second hand; people live their myths and only tolerate their reality.

6.2.1 Target Hosts

Proper identification of the target hosts conserves resources, and so should be done carefully. Individuals who

have recently undergone 'crisis events' are particularly susceptible to most any message; this group are the most likely to undergo a religious conversion or complete change of life behavior. The uneducated, inexperienced, or unsophisticated lack the more advanced cognitive mechanisms for manipulation of language and for 'filtering' it, acting like an immune system. Individuals who need to fill a void, such as college students away from home, commonly for the first time, are ripe targets for more than an education, as numerous cults have found. The Jesuit belief that if you 'catch them early, and they are yours for life' seems true for more than religion; such identifications as 'brand loyalty' are also fixed while subjects are young.

For more sophisticated hosts, the messages must be more diffuse, but that in fact seems to aid in transmission; just as people strain harder to hear a whisper, concepts that they 'absorb' or receive through extrapolation seem to by-pass filters better. This seems to be akin to 'tweening' in motion pictures, where an eye will smooth the actual jerky motions into smooth action; people fill in cracks, they categorize, and these tendencies can be put to good use.

6.2.2 Crafting the Meme

A robust meme needs good, thoughtful design, like a well laid out house or city. Many memes suffer from 'organic growth' problems, where they are undirected, unmanaged, and soon die under their own weight. Creation of a meme requires that the engineer frame the correct intent for best performance value; just as with a military mission, if you can't state the objective, you aren't likely to succeed. It is important to identify the right 'buttons to push,' the releasers or triggers for behavior that are desired; note that a target subject can act or react based upon a meme, and a clearly directed outlet should be built in.

Unlike with a biological automata, the meme should not unnecessarily impair the host and their ability to function; making certain that the meme and host fits into the system is critical to the spread and overall influence of the meme.

The memetic engineer will likely want direct unaltered transmission of the meme from host to host, as that gives a uniform basis for prediction of actions and reactions. A well crafted meme encourages replication and transmission (the 'preaching' factor) to others; it should also allow a 'group identification' communication to give hosts a feeling of 'belonging' to something larger than themselves. Intent is likely that the meme alters or becomes the host's operational paradigm (a 'conversion'); this provides the longest lasting effect of the meme, rather than being just a 'fad.' It would be useful if it helped impart a resistance to further reprogramming (the strength of 'faith'), and shouldn't require continual reinforcement (which, to prevent overload, would require signal variation, which may then cause schisms). A meme should be resistant to schisms and interpretation by encouraging 'dogma,' acceptance of the communicated experience rather than a direct one, and enforce a desire for external, 'wiser' guidance.

Effects can also be seen through the use of aggregation, alterations, expansion, and improvements off of existing memes; in many ways, this is an easier task to accomplish, since the engineer can 'hijack' a proven operational meme with similar or shortfall effects to their desired intent and have a solid likelihood of success.

6.2.3 Starting the Fire

The engineer or sponsoring group will need to have access to the necessary vector channel for distribution. Research will also likely provide leverage points, where the effort invested gives back considerable return. It will be important to maintain a sense of realism, however, and focus efforts based on the needs of the intended goal; is it necessary to have a significant number of people over a short period of time, or a few, dedicated people over a longer period of time? The engineer should follow the communication model and maintain the proper role and actions based on it.

7.0 Operational Uses of Memetic Engineering

Manipulation of this sort occurs all the time, albeit primitive and directed at such things as 'Drink Coke' or 'Vote <Whomever>.' There are a great number of areas that memetic engineering could have large scale effect.

7.1 Jungian Economics

Since most people don't know the difference between real worth and perceived value, they get them very confused. What makes a certain stock on the market worth more than another? What causes a bank run? People's perceptions do; two stocks can have the same real worth and yet sell for wildly different amounts; a perception of bank instability triggering a run becomes a self fulfilling prophecy. It is all popular delusions and the madness of crowds. Deliberate manipulation of perceived values can have extreme effects on a market and economy.

7.2 Cover Stories

Careful use of memetic concepts can provide the intelligence community with the ideal process for cover stories. Crafting a set of memes that take into account various perceptions of events can create an impenetrable chaos; the 'actual' facts are wrapped, like successive layers of an onion around the core. Each layer of the onion is yet another plausible interpretation of events mixed with 'red herrings'; use of multiple layers insures that if one or a few get peeled off, the truth still remains covered. Interestingly, tailoring a few layers of the memetic cover story for specific types of 'probers' can send them off with their expectations properly met, but with the truth still secure.

7.3 Cultural Manipulation & Cultural Warfare

As a tool of covert intelligence and operations, memetic engineering has considerable potential. Politics by its nature lies (pun intended) on perceptions, and so becomes an easy target for this sort of operation.

There are other uses for the practice that are more indirect yet beneficial. For instance, the region of the former Soviet Union is in chaos, the operational paradigm under which they have been operating having been completely shattered. Some want to return to the old ways because it is familiar, it fits with their paradigm. Yet all those people have had their myths shattered; this makes them dangerously susceptible to any chance meme that happens along. Taking advantage of this ready-made target group should be done as soon as possible, instilling a new myth that is beneficial to the West. Introduction of a quasi-religious semi-political movement with a charismatic leader, preaching how the collapse of 'Socialist Realism' should have killed them off, but how they are a strong people, able to 'conquer' any obstacles, would be quite effective. Free market values and the upheaval necessary to make them a reality are made palatable by pointing out that even with active opposition, and with a waste of considerable resources, they had never been 'beaten'; then the message that they can turn this energy and their resources to winning in the market can be introduced. Current reform process is proceeding at far too lofty an intellectual level and is doomed for failure; a resurgence of hostile forces to the West in the region are not desirable.

This is just one example of the covert political use of memetics; it will grow to be a considerable tool for operations that may not use more coercive forms of manipulation.

8.0 Spread and Control of Memes

There are many unanswered questions that will only receive answers with time and study. Among them are many critical points, such as how do you deal with information once it is released? You can't take it back, so you had better get it right the first time. How do you fight an idea? Such things as gun control can't work as long as there is the basic idea of a gun, and the know-how to assemble one. Even more important is dealing with a meme like 'Marxism,' which was correctly seen as spreading uncontrollably; the accompanying paradigm shift was a simple concept (as opposed to explaining a complicated democracy to illiterate and uneducated peasants) and attractive to the majority of those it infected - that they should have control, a steady supply of food, an education, freedom from 'the oppression of the ruling class.' Without instituting a careful study and science of memetics, we'll never know how to deal with such things in the future (although it might be suspected that introduction of another primitive meme to counter it would work, if only through the perpetuation of a chaotic state of affairs and the subsequent susceptibility of the population, then taken advantage of that with another meme; see the rise of Napoleon as an example).

9.0 Protecting Yourself

The best way to protect oneself, knowing that this sort of thing is possible, is the Delphic oracle's comment to 'know thyself.' Understanding the rudiments of what is going on allows for considerable self programming and self control; a sophisticated person in fact will have a number of paradigms and shift them at will. It is interesting to note that prophylactic measures against this sort of thing have considerable history; for example, Speculative Freemasonry, in an attempt to counteract the rise of superstition and the power of the Church, used various rituals and initiations (kept secret to increase the 'shock value' to the participant) to invoke and evoke a state of mind and being through 'gnosis,' direct experience. The influence, historically, of such groups is still debated, yet the influence of the practitioners still remains; we view them as the most significant free thinkers, artists, and scientists of their age. Clearly, the ability to continually integrate the signals one receives and choose one's own actions and reactions is a beneficial capability.

10.0 Conclusion

An old Eskimo proverb states that to 'give a man a fish is to feed him for a day, to teach a man to fish is to feed him for life.' The discovery or invention of concepts and memes and subsequent transmission of them is the story of Man. Yet many other historical pressures, once given careful analysis, have yielded useful, beneficial engineering practices and sciences.

It is only a matter of time before a practice of memetics, called something that will make it palatable and believable, comes into formal existence. Hopefully, it will be soon, as there are a number of areas for study and implementation immediately.

Meanwhile, just as diseases cut down humanity before we understood about germs, memes are cutting through and having their effect. American 'culture' is particularly susceptible, having become highly sensitized to it. Culture is, in fact, simply a statistical aggregate of the reinforced signals available in a body of people. European and Asian cultures, with considerable tradition and what could be termed 'cultural inertia,' are harder to manipulate 'against the grain.' Aberrations such as Nazism are not influences that run contrary to a cultural bias - they are, in fact, a tight feedback loop of the primitive cultural identity symbols transmitted back into the culture continually, much like feedback in a sound system.

The U.S. has no culture anymore - rapid adoption of high-throughput, high-bandwidth signals channels, from cellular phones through MTV, have completely eroded

what culture there was and replaced it with 'instant gratification,' 'pop culture,' and 'sound bites.' Culture is a statistical average of the signals, and Americans are subjected to continual bombardment of ever-changing and inconsistent signals; cultural schizophrenia is the least resultant problem, yet causes splinters of the culture of retreat into more insular cultural identifications. Studies of violence, drugs use, and other behavior are incomplete without an accompanying memetic investigation.

Control of the signals and messages presents the ultimate tool for defining, shaping, and controlling a people, American or otherwise. What of the considerable investment by the Japanese in American media organizations, or the fact that more children recognize Super Mario or Sonic the Hedgehog than Mickey Mouse? Memetics can be a powerful tool, and can be seen as a culmination of the Japanese sentiment that the pen and sword should be used together (to think and act are one) and can even be the same weapon.

This document is an attempt at memetic manipulation as well. You the reader now have a spawn of new memes, not to mention the meme of memes, in your personal wetware. The difference is that my intent is to turn you the reader into a player rather than a pawn. You trust me, don't you?

Ψ

A Look at Business Data Security Measures

by Thomas Icom

I've received some information from our readers regarding the data processing security guidelines set by various companies, and how they are presented to their "rank & file" (ie. non information systems department) employees. I've taken the 10 most common guidelines and presented them in this article; so as better give the 'zine's readers an idea about business data security measures. If you run a business that makes use of computers and are interested in how to protect your data, you will find this information useful.

The nice thing about these measures is that they cost next to nothing to implement, and if conscientiously applied, will do a great deal to increase your level of data security.

1) Account (user ID and password) information for remote systems should not be resident in a PC or it's software. They should also not be written down in any documentation, or otherwise be easily accessible by unauthorized personnel.
2) Remote system passwords should be changed every 7-60 days. (Each company had a different time period specified in that range.)
3) Telephone numbers to remote systems should be supplied on a "need-to-know" basis. The numbers should not be easily accessible by unauthorized personnel.
4) Accounts belonging to transferred or terminated employees should deleted immediately.
5) Information copied from a remote system to a workstation should be assigned the same level of protection that it had on the remote system.
6) Users should logoff a remote system before leaving their terminal.
7) Computers and related material (diskettes, software, manuals, modems, et. al.) should be given the same protection as any other highly portable and valuable property. When possible, they should be secured when not in use.
8) Personal Computer users should make use of the system's keyboard lock when not in use. The key's serial number should be recorded.
9) Data on a hard disk or floppy diskettes should be backed-up, with the floppies being stored in a secure, preferably remote, location.
10) Proprietary or Confidential information should be stored on floppy diskettes, rather than on a system's fixed disk.

Ψ

Doing a Radio!

(reprinted from Full Disclosure #30)

I have found a way of receiving your great radio program, which I feel will help others receive Full Disclosure Live. (Ed Note: Full Disclosure Live is on WWCR 5065 Khz. Sundays at 7-8 PM Central Time). Since I am in prison, you have to find new ways of getting to hear the truth.

This does work, as I regularly listen to Full Disclosure Live, VOA, RCI, CBC-Canada, BBC, France, Germany, Netherlands, R.O.C., Cuba, Time Signals -- WWV - CHU, and morse code, all this on a modified Sony walkman bought here at the prison. I modified the radio to receive up to 10 Mhz.

Sony FM/AM Walkman Model #SRF-29

Modifying a walkman to receive shortwave

1) Open the back of the radio, removing the two screws -- one in the battery holder -- one under the belt clip.
2) After the back of the radio is removed, look for a small copper wire wrapped iron bar at the top of the radio. This is the AM antenna.
3) You will see four small wires soldered to the antenna.

4) Take six inches of small multi-strand wire, after stripping about one half inch of the plastic from both ends of the wire

5) Carefully wrap one end of the wire around place #2 (note: on some radios of the same model, place #3 picks up better)

6) Carefully solder or super glue or just carefully twist the wire onto the best place (#2 or #3)

7) You can cut a small groove in the edge of the radio to let the wire extend outside of the radio when the case is closed

8) I cut a small hole in the back of my radio, so I could use the adjustable red coil to fine tune the shortwave stations

9) The red painted coil - see above - is used to fine tune the stations

10) Very carefully turn the coil to the left - counter clockwise - the coil is very easy to turn, do not force it, breaks easily, to fine tune shortwave stations

11) Take at least 5 feet of small multi strand wire, if not multi strand solid will, twist one end of this wire to the stripped end of the wire coming out of the radio. Be sure the end of this wire is stripped of insulation for about one or two inches.

12) After stripping the other end of this wire, touch or hook it to a metal frame - I use an aluminum window frame for this, still in the window.

13) If this was done properly you will receive quite a number of shortwave stations, mainly at night.

14) I regularly receive 8 to 10 english speaking stations, several french, german and spanish stations plus morse code - in the shortwave band.

15) With this modification you can listen to Full Disclosure Live.

16) Be sure the radio is tuned to the AM band of your radio not the FM. Switch it to AM.

17) You will not lose the FM or AM band, you will have to retune the radio to a local AM station after listening to shortwave, by adjusting the red coil.

Ed Note: This article was reprinted from a letter in Issue #30 of the excellent periodical Full Disclosure. Full Disclosure has top notch articles and information about surveillance, privacy, and constitutional issues. I recommend that you subscribe to it! Full Disclosure is $29.95 for 12 issues, payable to: First Amendment Press Inc., P.O. Box 67, Lowell, Michigan, 49331.

Ψ

How To Contact The Militia

Ed. Note: In light of some moves made by our elected representitives and their bureaucratic underlings that could be considered totalitarian, people across the country have been forming citizen's militias. The concept of a citizen militia is well grounded in our country's law; which considers every citizen above the age of 18 part of it, and makes a distinction betwen it, calling us the unorganized militia, and the organized militia which is the national guard and reserves. In addition, surpeme court cases involving firearms ownership have consistently based their decisions on the suitability of weapons for militia purposes. If one checks the laws, they will find that contrary to the recent ramblings of certain socialist media types, these militias are totally legal. Recently, we received this press release from one of these militia units...

UNCLASSIFIED
APPROVED FOR PUBLIC RELEASE

DATE: 18NOV94 FILE: PUB 94-001

TO: POTENTIAL & OPERATIONAL UNORGANIZED MILITIA UNITS

FROM: TRADOC, WEST/PUT NY UNORG MILITIA

TOPIC: INITIAL CONTACT SOI

BEGIN TEXT:

The following SOI has been adopted by WEST/PUT NY UNORG MILITIA and is intended for nationwide unclassified initial contact communications needs between different militia units. Standard OPSEC and COMSEC procedures apply.

Militia units should adopt their own secure SOIs for intra-unit communications, and for inter-unit communications after initial contact and credential verification. DO NOT USE THIS SOI FOR CLASSIFIED OR MISSION CRITICAL COMMUNICATIONS.

1 - Citizens Band:

Primary (initial contact) Channel: 14 AM mode

Secondary Channels: 5, 11, 30, 35 AM mode

The secondary channels are to be used in the order presented above in case of interference (14 to 5 to 11 to 30 to 35 to 14...). Tell your party to "Go up one.", and then proceed to the next secondary channel.

When communicating on this band, call "Break for Union Jack." to initiate communications with other Militia units on frequency.

2 - 2 Meter Amateur Radio Band: 146.535 Mhz., Simplex, No CTCSS/PL

An amateur radio license of at least Technician class is required to operate on this frequency. Initiate contact by calling CQ, and discreetly bringing up the subject. NOTE: This frequency is open to all radio amateurs holding the appropriate license classes. A portion of them do not share our beliefs.

3 - 49 Mhz. No License Band: Channel A,B,C,D,E in that order. If a frequency is in use in your area, go the next higher one.

Initiate communications with the phrase "Calling for a militia contact, this is <use pseudonym of choice>."

Ψ

Classifieds

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

CONSULTING SERVICES NOW AVAILABLE: The staff of **OCL/Magnitude: Cybertek** are now available for consulting on **information and electronic security, disaster preparedness, personal security/self-reliance, and specialized communications systems** for individuals and businesses. For more information write **OCL/Magnitude Consulting Services, P.O. Box 64, Brewster, NY 10509**

WANTED: Articles for Cybertek #10: We are seeking high-quality, practical, how-to articles on various aspects of technology, security, and self-reliance. Write us or call RuneStone BBS for topics of interest and compensation information, or to submit an article.

Classified Ad Fee: 5 cents/word. 20 word minimum.
Deadline for March/April '95 Issue: February 15, 1995.
Send ads to: Cybertek, P.O. Box 64, Brewster, NY 10509 ATTN: Classifieds

Ψ

Cybertek Newsletter Information

Senior Editor/Publisher
Thomas Icom
OCL/Magnitude
P.O. Box 64
Brewster, NY 10509
thomas.icom@iirg.com

Layout Editor
Änußis/IIRG
anubis@iirg.com

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

Subscription & Mailing Dept. Assistance
Brain Donor, The Harbinger of Death,
Necross Sinister, Ionizer/IIRG

Writers
Atreides, Nick Halflinger, Wildflower

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

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

Subscription Information
Individual: $15/year (6 issues)
Corporate: $80/year
Canadian: US $25/year
Overseas: US $30/year

Equivalent trades of similar periodicals, interesting electronic equipment, office supplies, envelopes, and 52 cent stamps accepted in lieu of monetary payment.

The information in this newsletter is presented for educational purposes only. No illegal use is implied or suggested.

"The most important thing a practitioner of any art can have is their own mind. The individuals who can resist following the crowd will always be ahead of their peers, and will always have the means to deal with persecution"

- Thomas Icom

Ψ

Issue #10 - March/April 1995

Cybertek

Technology, Security, Self-Reliance

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

Editorial:
Looking Back: The Past Five Years

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

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

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

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

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

The propaganda that has been directed against the

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

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

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

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

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

- Thomas Icom, Senior Editor

Ψ

Terrorism in a New World

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

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

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

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

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

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

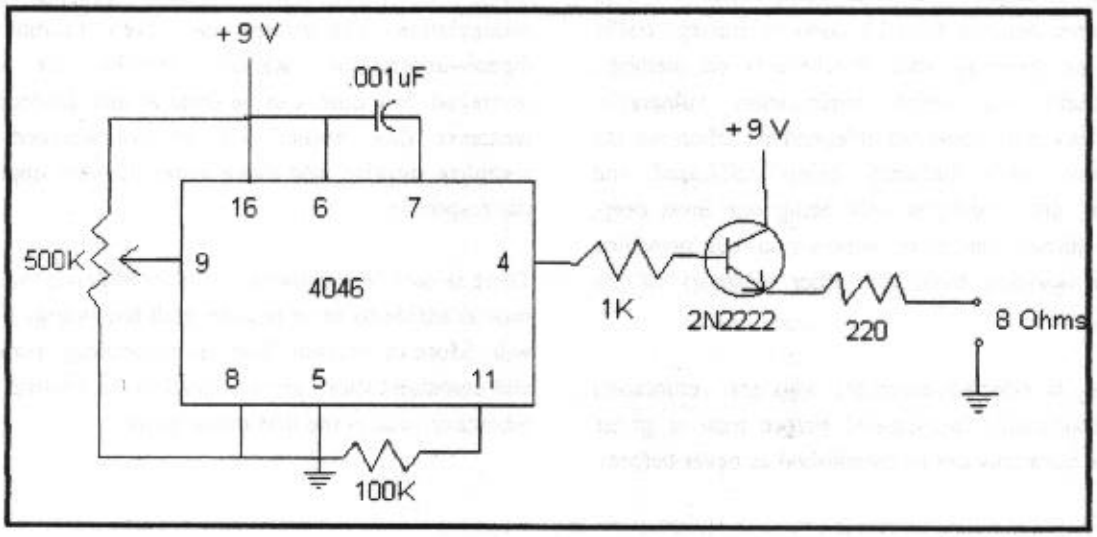
Communications technology has revolutionized the way the average man lives, works, thinks, and plays. The popularization of this technological infrastructure will provide a ready tool for the future terrorist--a global arena and a way to leverage limited resource. Soon to be gone (in most parts of the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

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

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

Audio Tone Generator Schematics

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



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

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

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

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

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

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

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

The Riddle of Steel

Long Knives, Swords, and Machetes

by **Jim Teff**

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

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

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

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

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

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

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

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

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

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

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

All of these are available from:

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

Ψ

Echinacea: An Indian Tea

by **Bleach**

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

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

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

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

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

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

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

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

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

References:

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

Ψ

A Guide to Computer Operational Security (OPSEC)

by **Bleach**

1.0 Introduction

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

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

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

2.0 Basic Security for the Computer User

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

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

2.1 Keeping a Low Profile Off The Computer

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

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

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

2.2 The PC's Basic Security

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

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

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

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

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

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

3.0 Online Introduction

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

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

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

4.0 Online Services

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

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

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

4.1 Prodigy

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

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

4.2 America Online

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

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

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

4.3 Online Service Conclusion

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

5.0 The INTERNET

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

5.1 The Legit User Seeking Operational Security

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

5.1.1 The Finger Command and Password Files

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

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

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

5.1.2 Commercial Internet Services

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

Many legit users will be happy with these types of

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

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

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

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

5.2 The Hacker Seeking OPSEC On The Internet

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

5.2.1 Targeting Systems

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

5.2.2 Spoofing

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

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

5.2.3 Cryptography

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

5.2.4 Outdials

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

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

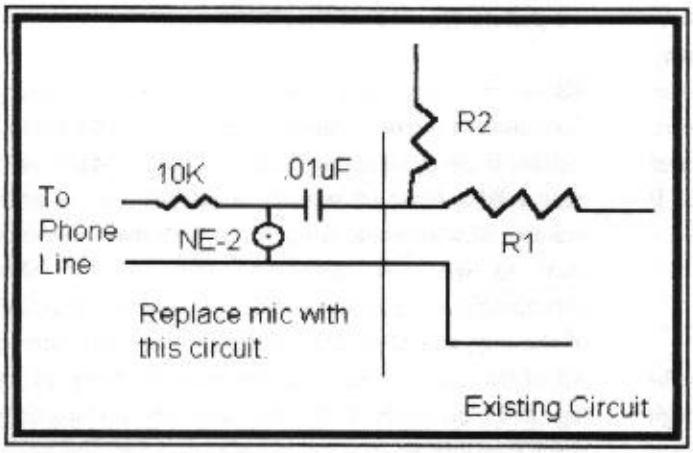
6.0 Bulletin Board Systems (BBS)

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

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

7.0 Language

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



Modifying the Radio Shack Wireless Microphone Kit for Telephone Surveillance.

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

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

8.0 Conclusion

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

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

The Ten Dollar Bug

by **Thomas Icom**

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

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

My Observations

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

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

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

Even Cheaper

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

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

Final Analysis

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

Ψ

Room Bug

by **S.V.M.**

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

Ψ

Survival Notes (#2)

by **Wildflower**

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

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

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

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

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

lit, then topped with an old circular saw blade.

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

Steam Power Resources

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

Some sources are:

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

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

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

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

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

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

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

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

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

Those wishing to correspond with me can send inquiries to:

WILDFLOWER
PO BOX 1745
New London, CT 06320

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

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

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

LIVE LONG & FREE!
Wildflower*95

Ψ

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

review by **Thomas Icom**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Good luck and good listening!
troach@netcom.com

Ψ

Cybertek Reviews
by **The Cybertek Staff**

The Ultimate Potato-Bazooka
Hair Spray Powered Vegetable Guns

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

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

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

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

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

available from M&M Engineering

1995 Police Call Radio Guide

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

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

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

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

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

Bootleg's DMV CD-ROMs

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

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

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

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

How to Live Well on Practically Nothing

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

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

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

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

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

The Art of Throwing Weapons

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

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

The Sling

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

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

Slash & Thrust, Flexible Weapons

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

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

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

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

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

Publishers' addresses:

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

Reviewers:
JT - Jim Teff
TI - Thomas Icom

Ψ

ᚲᛊᛒᛗᚱᛏᛖᚲ

Technology
Security
Self-Reliance

Cybertek

Issue #11 - May/June 1995

"THE CYBERPUNK TECHNICAL JOURNAL"

A people who mean to be their own governors must arm themselves with the power knowledge gives.
- James Madison

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

"It is error alone which needs the support of government. Truth can stand by itself."
- Thomas Jefferson

Expanding One's Focus to Keep the Edge

One of the main guiding principles for those who practice our assorted crafts is "keeping the edge". "Keeping the edge" is about staying on top by expanding your knowledge base. This not only includes staying current within your specialties, but also expanding into other fields. This is a natural part of your continuous growth process, and an essential survival trait. In these interesting times, you should have as broad a knowledge overview as possible in order for you to have the best chance for a long and prosperous life (which is the true essence of self-reliance and preparedness).

This expansion will often go into directions whose practical applicability isn't readily apparent. As part of the ongoing process of keeping the edge, you should ask yourself when in such a situation "How can I play with this?"

Jerod Pore, in his review of Cybertek #9 mentioned that our article on memetics was "a surprising departure from the nuts'n'bolts aspect of Cybertek." In a fashion I agree with him. Covering a "soft" technology such as memetics is a departure when one considers the vast majority of articles that have appeared in the past five years of our existence have deal with the "hard" technologies. Soft technologies however, are just as nuts'n'bolts as the hard ones.

Soft technologies such as memetic engineering and psychological operations are being put to practical use every day. You can see it by watching TV and even by reading Cybertek. The entertainment industry and mass media assault you twenty four hours a day with it in order to get you to buy XXXX brand of whatever, and to convince you that their totalitarian political and social views are the the only proper ones. Every time you walk into a store, sales people use it to get you to buy something. Once a year just before November, politicians depend on a successful application of it on their part to keep their jobs. On the other side, other alternative press publishers and I use it in an attempt to kick the brain cells of our readers into action so they will go out and think for themselves.

One only has to take a quick look at what's going on today to see that not only do soft technologies work, but they are being used against technology and self-reliance hobbyists constantly. Learning about the practical aspects of soft technologies can only help our side out.

- Thomas Icom, senior editor

On Playing The Game

by **Charlie Holmes**
2LT, MI, USA

Some day I may write a formal paper on propaganda, but for now I think this information best kept just among us in 00000000000000000000.

I will assume familiarity with "black," "white," and "gray" propaganda; what I claim is original with me is the explicit identification of what I call "Kandy-Apple Red Metal-Flake" propaganda: stuff that is so entertaining that recipients show it to others and/or reproduce it at their own expense!

Get it? Von Neumannism comes to propaganda!

Think of a few of the commonly-recognized uses of propaganda:

* "Preaching to the choir" -- invigorating and reinforcing the beliefs of those who already agree.

* Persuading those who are basically neutral or undecided.

* Convincing the opposition to change their minds.

* Confusing the opposition by disinformation, or "mind-fucking."

* Making the writer of the propaganda personally feel good.

This list does not claim necessarily to be exhaustive. What's key and crucial is this: Applied Von Neumannism (creating propaganda which REPRODUCES ITSELF) clearly enhances the performance of EACH OF THESE OBJECTIVES! The recipient who passes along (or, better, who MAKES COPIES of) a piece of propaganda has become a co-perpetrator in the propagandizing process! For free!

And it gets better: If your trusted friend or co-worker hands you a piece of propaganda (which he may not even KNOW to be intended as such) with the admonition, "Jesus, Joe, you gotta read this--it's the craziest thing I've ever seen!" you are going to give it a MUCH more sympathetic reception than if you receive identical material from a random stranger, say, from the "Fair Play for Haiti Committee." So as the propaganda gets passed along from one recipient to the next, the benefits are not merely quantitative (more copies in circulation--at other people's expense) but QUALITATIVE (each copy more likely to influence the recipient)!

My hook has been humor; if the stuff is funny enough, people will circulate it EVEN IF IT OFFENDS SOME OF THEIR OWN PRINCIPLES! I call this the "Doonesbury phenomenon": I think Trudeau is brilliant, incisive and insightful, especially when he is pillorying my ideological enemies, but EVEN WHEN HE IS SKEWERING SOME OF THE IDEALS I MOST HIGHLY REVERE (which is frequently, since I consider Uncle Duke a sort of role model.) Specifically, some of his vicious, unfair, devastating assaults on the Second Amendment have been so deliciously, darkly, wicked that I've shown them to other gun collectors, who have groaned and winced their amusement.

Notice that the afterword to "A New Lo" specifically encourages and reinforces this tendency: It is mentioned that "various respectable, honorable and noble memes find themselves inextricably interwoven with disturbing, scandalous, and subversive ones," and the reader is assured that this is a good thing, so just lie back and enjoy it. Notice also that it is never specifically alleged just WHICH memes are honorable and WHICH are subversive, so that the reader can make his own decisions in this area. The idea is that the reader--feeling, rightly, that the good far outweighs the bad --might just as well reproduce the whole thing.

* * * *

Normally in chess or checkers the game pieces stay the same color throughout the game. A piece that's yours can be counted on to always remain yours. Not so

when playing against my own Extraterrestrial Geniushood.

Consider my continuing game of "good cop/bad cop" with 000000 Aircraft. First notice that I've hyped both roles to the max: The "good cop" offered to immediately stop my tantrum, shut my mouth, and work for 000000 for minimum wage plus perks. The "bad cop" threatened to 00000000000000000000 00000 with a shocking story of 00000000000000000000 and wrongful termination. (Perhaps the metaphor should more appropriately be "savior cop/terrorist cop.")

OK, they know they can always have me back by just apologizing, eating crow, and admitting that those two fuckin' lizards 00000000 and "Ms. Smith" set 000000 up to get STOMPED LIKE A NARC AT A BIKER RALLY! (My offer was, of course, made not out of any altruism, but, rather, to give them an incentive not to have me killed.) They might be inclined to think of that offer as their "ace-in-the-hole," a "worst-case scenario bug-out plan," if you will. One of THEIR game assets.

But now think about WHAT HAPPENS TO THAT GAME PIECE AS IT AGES! For a couple of years, everything goes sort of OK: A disgruntled ex-employee is having a little fun at the expense of the assholes who libeled him as being "average" on his performance review and therefore got him laid off. OK, fine.

EVENTUALLY, however, the following is going to dawn: This guy they fucked over is EXTREMELY clever at finding ways to make them bleed (metaphorically, of course, as he will be punctilious about not violating any federal, state or local law). What if, after OSTENTATIOUSLY SIGNING ON WITH ANOTHER EMPLOYER, or EMIGRATING TO HOLLAND, he uses his right to speak at a shareholder's meeting about how 000000 not only butt-fucked him, but refused to make it right and hire him back even for minimum wage? What if he quite seriously RENTS THE MELKWEG FOR A PRESS CONFERENCE and solicits job offers from any and all Western democracies? And says that it's "all 000000's fault."

And what if he of course has no intention of really doing any of these things, but only hints at their possibility in order to MAKE 000000 REAL JUMPY?

So things are not always what they seem. And sometimes what appear to be YOUR assets can be TURNED IN PLACE when you ain't payin' attention.

Anybody paying attention?

* * * *

The O. Henry story "Gift of the Magi" points out a unique situation in Game Theory which I call the "altruist's dilemma"; I'll make the title clearer a bit later.

Recapping, for those who've never come across it, this particular Christmas story involves a couple who are very, very much in love, but also very, very poor. Her great pride is her flowing locks of hair; his is a valuable antique heirloom watch.

Lest I be erroneously accused of Philistinism by the rather emotionless dissection of their behavior from a game-theoretic standpoint, let me acknowledge beforehand that the important nub of the story concerns of course not the material objects given and received as Christmas presents, but, rather, the obvious revelation of the depth of their love--which happens to be demonstrated by those presents. OK. Fine. Having identified that significant component, we are now free to intellectually isolate ourselves from it, and consider ONLY the real-world, material consequences of their actions.

Those who are familiar with the story are already ahead of me here. To buy him a handsome fob for his treasured watch, she sells her hair to a wigmaker. He sells the watch to buy a set of lovely combs for her hair. This convinces both of the depth of each other's love, and, quite properly, they recognize that this is the best Christmas present of all. Again, fine. Powerful message that the "real meaning of Christmas" is not

about presents.

But return now just to game-theoretic material consequences. What has happened is the WORST POSSIBLE FUCK-UP ACHIEVABLE! If EITHER of them had done ANYTHING DIFFERENT AT ALL, the situation would have been UNAMBIGUOUSLY BETTER FOR BOTH OF THEM! Ponder that for a moment.

If she had given him nothing but a fuckin' card, and he had still sold the watch to buy her present, then she would have retained her hair, and both would have at least had the pleasure of seeing her hair adorned with the combs. Similarly, if he had stiffed her but she had sold her hair, then both could take some pleasure in admiring his watch and new fob. Finally, if both of them had just exchanged cards, each would have at least retained rather than renounced a treasured possession.

Notice further that the game system is perfectly symmetrical. Neither party can be "blamed" any more than the other for fucking up both their lives. Each party gave up something of known high value to him/herself, from a desire to give a thing of conjectured high value to his/her partner. Both got symmetrically screwed, and, again, if EITHER party had rejected altruism, such a choice would have BEEN BETTER FOR BOTH! This should not be terribly surprising, when you think about it, since many people have enough trouble trying to figure out what will make themselves happy, much less someone else.

Bear this in mind at election time, when the altruists are out in force, Sometimes we libertarians and conservatives decry various "welfare" schemes as simple vote-buying with taxpayers' money. Sometimes, of course, there's truth to this, but the spooky thing is that even if the altruists spending your taxes are every bit as sincere as the altruists in "Gift of the Magi," their legacy can be every bit as materially destructive!

I am not so paranoid as to suggest that the "welfare state" was really specifically designed to "dumb down" the human race as a whole, across every racial, religious, and ethnic group--but this is what it has done. Maybe every fuckin' politician since Lyndon Johnson truly and sincerely believed the propaganda: that everyone would live in a "better world" if the government forcibly takes money from those who can earn it to give to those who cannot. Maybe you bought it as well: your tax dollars legitimately taken from you at government gunpoint as your duty to "help the needy." Well, the Magi fucked you all over!

The "non-self-supporting" underclass has ballooned in size--not surprising when you consider they have been bribed to reproduce--yet their lives remain more or less wretched. LBJ's subsidized babies have themselves become breeders, and those who got really early starts may now have a third-generation granddaughter -- doubtless awaiting the day when a missed period means she is no longer just a "13-year-old girl" but now a "mother": entitled to a place of her own and a monthly check that grows larger with each of her kids. Are we clear on this? More people leading wretched lives, costing more gunpoint-collected taxes to support in wretchedness. EVERYBODY FUCKIN' LOSES!

Note how the very word "entitlement" has come to replace, say, "charity" to describe the welfare system. Used to be, giving to the needy was practicing a virtue. No more, apparently. If they're "entitled" to it, they must have some kind of a right to it. So now we talk of "punishing" the poor by not giving them handouts of forcibly-seized tax money. Fraudulent use of language, clearly, as best illustrated by asking you whether you improperly "punish" a street panhandler when you give him less money than he would have preferred, or (gasp!) maybe no money at all.

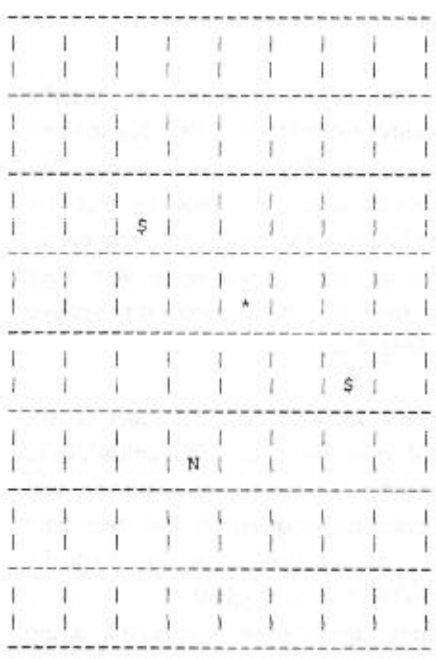
We've gotten a little off the game-theoretic aspects here, but let's return to one key observation: The "altruist's dilemma" is at least ONE FUCK-UP SCENARIO that could NEVER ARISE between self-interested players. ONLY those who attempt to place others' happiness over their own are susceptible to it. One more reason why altruism is fundamentally untenable as a "moral compass."

* * * *

We have already encountered the "win-win" concept before. That is, it is frequently in ONE'S OWN SELF-INTEREST to work out a solution where in some sense "everybody wins," if only because this option is THE BEST DEAL FOR ME THAT I CAN REASONABLY EXPECT TO CUT.

In other circumstances, however, one might attempt another strategy that could also be called "win-win [for me!]"; this refers to a different set of circumstances, namely, WHATEVER MY OPPONENT DOES, I STILL WIN! Powerful concept, n'est-ce pas? We'll call this the "Heads-I-win-tails-you-lose" principle to distinguish it from the already described "win-win."

A good example comes from chess:



The "N" is my knight, and the $-signs are essentially any two of YOUR high-value pieces (e.g., R,Q,K). I'm coming from a reasonable way off, and gonna JUMP FOR THE ASTERISK "*" which, by hypothesis, is NOT attacked by you. At this time, you are SCREWED: You can only save ONE, and I take the other.

There may (or may not) be other subtleties operating. The "$" squares may be attacked. Even so, you've lost a piece worth MORE THAN THE KNIGHT you take. Or, if I've done my homework, the "*" square will be attacked by another of MY pieces, and I also terminate the guy who takes out the knight.

Non-chess-players should consider that they are "X" in the below tic-tac-toe game, and that it is their move:

```
 X | O |
-----------
   | X |
-----------
   |   | O
```

Turns out that EITHER of the available left-hand boxes is a guaranteed win, as you will have TWO sets of "two-X's-in-a-row" and of course your opponent can only block ONE of them in his next move, leaving you a sure win on YOUR next move.

Do you see the relevance to "The Greatest Hoax Ever Told?"

Assume for the sake of argument that "7th Seal," "Letter to Janet Reno" and "Epistle to the Hebrews" are REALLY GOOD STUFF. (If you don't concur here, then perform the "thought experiment" of considering that someone HAD WRITTEN REALLY GOOD STUFF in an attempt to perpetrate the "resurrected Koresh" hoax.)

Somebody gets a letter with a whole bunch of printed paper and/or a floppy disk. (The disk is a good touch intrinsically, because it is a "thing of value" rather than just a "piece of propaganda paper.") Also, it is not only cheaper to mail than the same volume of printed paper, but it is easier and cheaper to COPY as well, whether to another floppy, a hard disk, or a BBS upload.

The cover letter is fuckin' astonishing, and doesn't ask for their money, their vote, or for them to do anything at all except maybe pray. (One of the few changes in the cover letter was to make "ask for your help" into "ask for your advice." Christ forbid they throw it away

after the first paragraph thinking that Dave is tryin' to hit 'em up for money.) The letter is addressed to them personally where possible. Dramatic postage stamps (holograms, moon landing) are often used.

Result: The recipient MUST assume that either (1) Koresh is indeed alive, or (2) Somebody awful damn smart, who ain't particularly worried about money, is trying to perpetrate the HOAX that he is. EITHER WAY, the recipient very likely will freak. Actually, the worst part may be that some of the writings seem SO FUCKIN' SPACY that another dichotomy beckons: Either (1) Koresh was MUCH weirder than we have heard so far, and is still alive, or (2) the hoaxer trying to fake his resurrection is WAY WEIRDER THAN KORESH HIMSELF! Almost hard to say which is the most mind-fucking, n'est-ce pas?

Ψ

Fun With Near Field Receivers

by **Thomas Icom**

A near field receiver is a piece of communications equipment whose purpose is to intercept radio communications in it's immediate vicinity. This "immediate vicinity" can be as far away as two miles depending on the strength of the transmitted signal and the antenna used on the near field receiver.

When connected to an antenna and turned on, a near field receiver starts sweeping its frequency coverage. When it hears a signal of adequate strength, it locks on and demodulates the audio. When it loses the signal it continues its sweep until it finds something else to listen to.

Most near field receivers are also capable of providing rudimentary trouble shooting data such as signal strength and deviation.

Near field receivers are commonly used in field service and counter- surveillance operations. A hand-held near field receiver with the proper features can replace some of the functions of the more expensive and bulky service monitor. When doing a sweep with a near field receiver, the receiver will lock onto the signal of any RF-based surveillance device within its frequency coverage at a greater range than the traditional field strength meter.

The Opto' R10

This article will focus on my experiences with the Optoelectronics R10 "Interceptor" near field receiver. The R10 is a high quality, reasonably priced, battery operated unit with a coverage of 30 Mhz. to 2 Ghz. Specifications and product reviews have appeared in other publications for those interested in such information and opinions.

The first thing that one should realize with the R10 is that it's operation is different than that of a conventional VHF/UHF "scanner" receiver. That's because its role in RF work is different.

With a scanner one either programs in specific frequencies into channel memories and then has the unit go through them, stopping when it encounters one with activity on it, or they program a high and low end of a frequency range and search that range for frequencies which have activity on them. A scanner is also a lot more sensitive than the R10, which enables it to receive radio signals from long distances.

The R10 is much less sensitive than a scanner. That's because it's intended to receive radio communications in the near field. Depending on the power, elevation, and antenna of the transmitter in question; this near field range can extend up to a couple miles, but is usually limited to about 2500 feet for a standard 25 watt mobile radio running a unity gain antenna. Instead of having memory channels or a search function, the R10 just sweeps its entire frequency range looking for a transmitter that is of adequate enough signal strength to be considered near field.

With the above in mind, the first thing one should remember about the R10 is that it's not a scanner, nor will it replace a scanner. The R10 is a powerful

specialized SIGINT tool, but if you want the capabilities a scanner provides you shouldn't be purchasing an R10.

The R10 works best in areas that don't have a high RF background level. In high RF background areas one can expect the overall effective range of the R10 to be reduced, and for it to be more likely to lock onto things like broadcast and paging transmitters.

It also works best in a stationary, as opposed to a mobile installation. In a mobile installation or when listening to mobile units, one will experience signal loss on fringe signals due to the "picket fencing" effect. Depending on whether or not other signals of adequate strength are in the area, one will either wind up getting a totally different signal acquisition or quickly reacquire the original signal.

The R10's unique capabilities and mode of operation take some getting used to. I suggest you spend a few weeks getting used to its peculiarities before actually going out and doing something serious with it.

Antennas

A lot of individuals seem to think that if they attach a "big" enough antenna to an R10, it will work better. They then get all upset when they turn it on and it constantly locks on a nearby FM or TV station. The R10 was generally not intended for use with a gain antenna. When one uses a broad-banded gain antenna with the R10 not only will the range will be increased, but also the possibility of picking up potentially undesirable signals like continuously transmitting broadcast stations or busy paging transmitters.

The best antenna I've found for general use is the telescoping whip. It's length can be adjusted to provide signal attenuation when tracking down surveillance devices and attenuating an undesirable signal, or to provide a resonant length when focusing on a specific frequency range. This antenna type is the one which is sold with the R10.

One can also use a yagi antenna with an R10 to great effect. Yagis are directional and tuned to a specific frequency band. These two characteristics help increase the effective range in the target band, and eliminate undesirable signals which originate outside the frequency band and direction of interest.

In addition to using the right antenna, the judicious use of filters, particularly bandpass and notch filters, can increase effective range and eliminate undesirable signals. One filter I would recommend getting right away is an "FM trap". This will eliminate the unit locking up on FM broadcast stations. After that, I would recommend bandpass filters for specific frequency ranges of interest.

Applications

In regard to SIGINT operations, the R10 has proven its utility on many different occasions.

It's utility in conducting counter surveillance sweeps for RF-based devices has already been mentioned. Assuming the device in question operates using non-encrypted FM modulation, the R10 will lock onto the device's signal upon walking into the affected room. By walking around the room and gradually attenuating the received signal strength by reducing the length of the telescoping antenna and adjusting the R10's squelch control, one will be able to pinpoint the location of the device . When one gets "on top" of the surveillance device, one will notice a full scale signal strength reading despite the fact that one has set maximum received signal attenuation (i.e.. the squelch control cut all the way back and the telescoping antenna fully collapsed), and a feedback squeal will result from the coupling of the device's microphone with the R10's speaker. The feedback will indicate that one is in the immediate area of the surveillance device. It will also alert the third listening party to the fact that their toy was discovered (keep this in mind).

The feedback squeal will only result if the surveillance device's mode of transmission is unencrypted FM voice. One however will still be able to note the device's

location by attenuating the received signal's strength and watching the signal strength meter for a full scale reading when one has maximum received signal attenuation. Once one has determined the approximate location by using that method, one should then be able to find the device by conducting a good thorough search and having some knowledge of what surveillance devices look like.

The R10 is excellent for cellular surveillance, especially when attached to a cellular band antenna and/or a cellular bandpass filter. Good signal locks have occurred on mobiles up to a half mile away when using a 5/8 wave cellular antenna in a mobile surveillance installation, and up to two or more miles away on cellsites when used with an 800 Mhz. yagi antenna. When surveilling cellular mobile units, the R10 is able to quickly reacquire a mobile when a frequency change occurs due to a hand-off to another cellsite.

For quick acquisition tactical signal intercepts, the R10 is excellent. A quick acquisition situation is when you notice or suspect nearby RF communication activity (i.e.. someone who's talking on a handheld radio nearby, being caught in a traffic jam, etc.) and you want to know what the parties are saying. A frequency search may not be possible due to time or manpower considerations. (Ever try to do a frequency search with a scanner while driving down the highway at 55+ MPH?)

I just recently used my R10 to good effect while caught in a traffic jam that resulted from a five car accident a half mile down the highway I was traveling on. Within minutes, the R10 had successfully intercepted several transmissions from people who were talking about the accident.

The R10 can act as a sensor system to alert you to RF activity in your immediate area. One can implement this application by turning down the sensitivity so that background signals (i.e.. FM and TV broadcast stations, paging transmitters, and other annoyances) are eliminated, and then having a friend with a handheld radio walk around one's immediate area while transmitting in order to get an idea of effective range. Once the range is determined, the R10 is left on and listened to. One could also add a sound activated alarm to the audio output to give a louder alert indication than the received audio alone would provide. When one hears audio one will know that someone is using radio communications within that predetermined range. By listening to the transmissions in question one should be able to determine the general identity and intentions of the radio user(s), and thus be able to generate an appropriate reaction to their presence.

Ψ

Survival Notes (#3)

by **Wildflower**

Car Emergency Kits

Trouble can occur anywhere on the road. Your radiator starts to leak, a tire gets punctured, your ignition just died, or something else; leaving you stranded, perhaps on a dirt road deep in some forest or along a freeway near home. If you are prepared with a good emergency kit you could fix the problem, or call for help and be able to wait in comfort till help comes; if not you could just go bananas in sheer panic!.

The following should be in anybody's emergency kit; stashed along with a good spare tire and jack: first aid kit, 3-7 days of food and water, roll of t-paper in a plastic bag; a large candle & matches, a warm wool blanket, a waterproof poncho, a good flashlight, a set of flares, a good tool kit with wrenches and socket set, folding shovel, folding saw, come-along winch with tow straps, jumper cables. It would be excellent to install a CB radio and a backup electric fuel pump. A set of good maps and a good compass come in handy too!

Yes it is a hefty kit so far. It is also good to include a can of radiator sealant, a can of tire inflater/sealant, emergency fan belt kit, spare bulbs & fuses, roll of wire, roll of duct tape, and a stick of quick setting epoxy mix.

Toss in a set of spare ignition parts and a cheap analog VOM meter, and you should be able to fix it until you reach home or civilization (which if you do, send me directions, please!)
OR suffer without when you are stuck miles from anywhere, hungry, tired, and freezing into a corpse!

Ammo Boxes

True, the GOVERNMENT is now reducing surplus ammo boxes into scrap metal. One has to devise other methods. Look up in the yellow pages of your phone book and locate wither an auto paint or custom paint dealer. Chances are one can buy new gallon cans with lids. Fill the can with ammo & desiccant packet, place can on floor, and with foot press shut the lid. Then paint can two coats of any exterior paint; when dry mark contents with laundry marker on lid. Can of ammo now ready for your burial cache.
-OR- look into utilizing Rubbermaid brand food containers, or even mason canning jars for storing ammo too.

Frogs...

are disappearing as either levels of Acid Rain or Ultraviolet Radiation increase in their environment. If they go extinct, good to wonder whom is next to go!? Think about it!

But the real ugly truth is that there are numerous plants and animals facing extinction, but until it gets to be a "National Crisis" little ever be done. As man has lost the feel of earth & its ties to his spirit; soon such men will follow the Dodo too. If you wish to survive, renew your ties to your earth, and remember you are either part of the problem or that of the solution; as you share this world with so many living critters, you are one of those critters too.
-OR- ignore this, go back and suck your beer and stare at the telly, you poor stupid dinosaur!

Food Storage

Criticized in Living Free was that a 3 year "Use & Replace" canned food supply be too "stale. Even if such a food supply is not "fresh food", it is far better to have a canned food supply than no food at all in a crisis of any sort. And as the near future looms ahead, am considering extending it to a "five year use & replace canned food supply". If you're going to stock ammo, gold, and whiskey; you'd be better off building up your food supply too!
-OR- BON A'PITIET, chewing on your gold pieces!

LIVE LONG & FREE!
Wildflower*95

Ψ

Application of Memetics

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

"...unless we're all part of the same dream. Only I do hope it's my dream, and not the Red King's! I don't like belonging to another person's dream..."
--The character of Alice in Lewis Carroll's "Through the Looking Glass"

Face it, reality is a consentual hallucination. The only reason why you know something is the color 'red' is because somebody else told you so. And how did they know? Because someone told them. To make reality even more complex, you really don't have any true perception of reality, you only perceive your perceptions. If you haven't had to stop reading and think about this for at least five minutes (and how do you know how long a minute is?), then you just don't get the point. What is the point? That your knowledge, behavior, and all those other fuzzy concepts are learned from what other people tell you and from mimicking role models. No matter how original you think you may be, no matter how much life experience you have collected on your own, it all still rests on the foundations that you borrowed, willy nilly, from others. Now for a little secret--the part of your brain that does this, without much help from you I might add, and even when you don't want it to happen, is still at it, is still borrowing whole hog from the world around you. How

else would you stay current in language, dress, social customs, and all that jazz? Here's another secret (notice how you perk up when you think you are going to be let in on a secret?); there are people out there who understand how it works a little better than you do (does that make you nervous?), and actually do something about it. Don't you think it's time you caught up with the rest of us (isn't it reassuring to be part of a group?) and found out how to do it too?

Welcome to the wonderful world of memetic engineering, the applied science of making friends think what you want them to think, and influencing enemies. Some might apply such a set of techniques to the commercial use of selling things, while others will see deeper and think of how to influence public opinion. This document is intended for that deeper thinker (and you do like to think of yourself as one of those, don't you?), and outlines the basic mechanisms for treating other peoples' minds as if they were your playground, and their own private Idaho.

Rule 1: Fix your target and the communication channel that reaches them.
Knowing whom you want targeted is not as easy as it sounds. Given that you have clearly framed what your objective is, you have to decide on an approach--do you want many 'believers' quickly but only for a short term, or do you need a fewer number but for a longer term? What action or reaction is desired from these people? Can it realistically be met in the short or medium term? Or does it require a long term 'paradigm shift' to accomplish? Why will they do this? Can you make them think that they have a good motive? Once you have all this figured out, you can sketch up a rough character profile and research exactly how such individuals get their 'input.' After all, if you control a person's surroundings or input, you essentially control the person.

Rule 2: Pretest possible reactions.
This is the fine tuning stage. Locate a potential target and take a test run to see what really happens when you start pushing their buttons. Take the feedback to heart and do any reengineering of the target, message, and channel you need to. Pretest again. Keep this up until you have it right.

Rule 3: Be flexible, and run the operation in place.
It helps to be 'in country' when doing this sort of thing. If you fit, even partially, the profile for the target, and you are immersed in the same 'signal saturation' they are, you have a better probability of creating an effective meme. You also have the chance to make changes or course corrections on the fly if you have to. Call this 'sticking with what you know.'

Rule 4: Know your context.
Know as much as possible about the general culture and subculture you targeting. You have to have everything down--vocabulary, syntax, timing, triggers, etc. to do this right. Be a cultural anthropologist. Look at those around you as if you were from Mars, not them. Question your assumptions.

Rule 5: Carefully pick the tone your message will take.
You can pitch your message in a variety of ways: positive, prophylactic, and negative. Positive memes are ego building messages for the recipient. Prophylactic memes simply prevent spread or infection by others. Negative memes are the easiest to craft and have accepted, since they exploit mistakes and faults that are either really there or at least perceived as being there. For example, take Israeli efforts to influence public opinion in the U.S.; they have not so much successfully implemented such an effort, as much as they are one of the few voices out there. They have managed to promote a continual media bombardment of the Arabs as the 'bad guy' in print and film, potent places for such a message. The prophylactic side-effects are potent as well--talk of Israeli propaganda at all can get you labeled as being anti-Semitic, and talk of Israeli media influence gets you branded as paranoid; either way, you don't get listened to. The Israelis have also managed to build a considerable myth around themselves as 'underdog' (when they have the most advanced force in the region), as having an unbeatable military (when they are only well trained and far from infallible), and as having a potent intelligence capability (when MOSSAD

has made some of the biggest blunders in the business). It all boils down to acting like the Wizard of Oz--acting powerful, mysterious, all-knowing, beyond judgment or reproach, when all you really are is a small, ordinary man hiding behind a threadbare curtain.

Rule 6: Decide on the duration and degree of repetition of your message.
Pavlov had some things wrong, but he also had some things right, such as "Re-enforce often!" It also helps to have a good amount of variation with the reinforcement, so that the message doesn't get ignored (if you hear the same thing too many times in just the same way, you learn to tune it out).

Rule 7: Use existing channels to move your message.
Don't get fancy, and don't try to move a meme across a newly established channel. Be careful with the new medium of the Internet (or Usenet)--people there are paranoid, scared, and skeptical in general, but that can be turned to your advantage if you understand that. Also, the Net acts as a 'community memory'--check out the beast known as the FAQ (Frequently Asked Questions) which are kept current and accurate by an informal collective that knows the topic (two good examples are the cryptography FAQ and the exercise FAQs). Careful with your facts, and be subtle with your spin.

Rule 8: Carefully construct your content.
A meme must be based on a solid intellectual, emotional, and economic model of the target population. It should aim at personalities, not issues. The 'mimicry' mechanism in people is susceptible because we are used to adopting patterns from other people. Issues just hit the intellectual gestalt and get processed, thus they have lower contagion; the only way issues can make it is if they imply a changed self image of the target subject, or are linked to an image of a person that the target can imagine themselves as.

Rule 9: Do not create new issues, but exploit existing ones.
It is easier to hijack an already 'in progress' meme and apply some spin control, reinterpretation, shift in perception, and a colorful dash of revisionism..

Rule 10: Aggregate your approach.
Build toward your true purpose over time; start memes out as being totally reliable to establish trust in the source. This 'collateral confirmation' gives credibility, and allows you to progress the future memes to approximate the target mindset. Be certain that the paradigm created by the meme fits into the existing climate, mindset, and general opinion, otherwise it has a low potential to spread and infect.

Rule 11: Don't make it seem like an attempt to influence them.
The hard sell turns people off; back off and let them come to you. You catch more people through letting them into the group reluctantly than you do by having 'press gangs' roving the countryside. People dislike the power trip of having to do things.

Rule 12: Keep it simple and emotional.
Frame the message to take advantage of releasers and gestalts; evoke emotions, since emotions are less susceptible to analysis, particularly in Western cultures.

Rule 13: Don't interfere (and benefit if possible) with Maslow's Hierarchy of Needs.
These are the basics: physical fulfillment, food, warmth, sleep, safety. They are also not so basic: positive self-image, esteem in the eyes of their peers, love, belonging, respect.

Rule 14: Evoke a group identification.
Pushing the buttons of your target's innate superiority, the shared suffering they have with the group, how they are the 'chosen' people goes a long way to reducing the maintenance necessary to keep members 'enrolled.'

Propaganda and Memetics

How do these two concepts differ? Propaganda creates a mindset that will accept or be neutral towards actions undertaken by the generating source. Memetics creates an active mindset that encourages participation (action,

reaction, proselytizing) and perpetuation of the intent of the generating source. It depends on whether you want people to be sedate or pro-active.

Conclusions

There are a number of people selling things, and I don't just mean those info-mercials. Some people are selling religions, others are selling pop psychotherapy, politicians sell themselves, sometimes literally. Some concepts could benefit from the tactics, similar to memetic tactics, that are used in those obnoxious info-mercials; maybe it is the removal from the abstract to the concrete that makes it so much more effective. No longer will you hear "It is better for the environment," "a united Ireland," or "democracy is good for you", but there will be a well-crafted meme showing you a person, someone you can identify with, someone you wouldn't mind being, enjoying the benefits of what before seemed like empty slogans. It certainly beats using the techniques to make people want 'buns of steel.

Ψ

Encrypting Numbers

Find an easy to remember ten word phrase, of which all the words begin with a different letter. For example:

The quick silver fox jumps over my lazy dog's back.

Now assign a digit to the first letter of each word:

T=1 Q=2 S=3 F=4 J=5 O=6 M=7 L=8 D=9 B=0

Should you have problems finding a similar phrase, you can take any sentence, and use the first ten unique letters, or even the first ten unique first letters of the words in the sentence. Using this paragraph as an example with the first technique, you'd use **SHOULDYAPR**. With the second technique, you'd use **SYHPFACTUL**.

You have a phone (or any other type of) number that you desire to protect; such as **203-832-8441**. Just substitute the letters for the numbers: **QBSLSQLFFT**.

One problem with this cipher is that most phone numbers in the United States and Canada are still in the old format where the middle digit of the area code is a 0 or 1 and the first two digits of an exchange can't be a 1 or 0. If someone clues into the fact that you are using this code, they could use that information to help compromise it. There is no rule however, that says you can't write down a phone number as 8328441203, 8441832203, 8441203832, or 1448238302. As more exchanges and area codes are added to the phone network which don't fit the old plan, this will become less of a problem.

This code is easy to keep around in one's head, and doesn't require a computer to implement.

Ψ

The Riddle of Steel

by **Jim Teff**

Product Reviews

Let me state for the record that I am not an employee of Smoky Mountain Knife Works, just a very satisfied customer. The quality of their merchandise surpasses the prices charged. Their prices are often better than those I paid for mail order blades 30 years ago *(Most grand masters are of advanced age - Ed.)*. Service is excellent. I phone in my order and usually receive it within a week. The one blade I returned with a manufacturing defect was cheerfully replaced. All in all, a great outfit to deal with.

Fighting Steel

Samurai - Manufacturer Unknown - Philippines
SH2 - 25" blade - $39.99
74522 - 22" blade - 29.99
74517 - 17" blade - $24.99
DRAGON - Set of 3 with stand - $99.99

The Katana style sword is the finest fighting blade ever designed. They can be wielded one or two-handed with equal ease. The curve of the blade makes slicing or draw-cutting smooth and natural. They are light and fast but sturdy enough for power cutting.

These Katanas and Wakisashi ("companion"/short sword) are excellently made and economically priced. The 22" model is perfect for across the back carry a-la Ninja. (The 25" blade is a little too long to allow drawing when worn in this fashion.) The scabbard is flatter than its Japanese cousin and the "shoulder strap" is more of a belt hanger. I removed the strap from the scabbard of my 22" Wakisashi, but left the D-rings to attach a Ninja-style saya made from a 72" shoelace, thong, or paracord.

The shiny brass tsuba and pommel can be covered with a sock or wrapped with a bandanna or cloth for stealth (or can be blackened with gun bluing but this will detract from its beauty). The brass will dull with age if not polished. The red wrapping on the handle and scabbard cannot be seen at night. If camo is a concern, you can wrap black, brown, green, or camo cloth around the scabbard and handle. Well balanced, stainless steel, sharp.

Dragon Slayer- Manufacturer Unknown - Philippines
745027 - $59.99
Blade 27" - Overall 33 3/4", 35" in wooden scabbard

If your taste leans more toward a hand-and-a-half, double-edged broadsword; this is the blade for you. Twenty seven inches of stainless steel with a full length fuller. Well balanced and sharp, this is the lowest priced practical broadsword I've handled. Conan himself would be proud of this steel.

Throwing Hatchet
6837744 - $5.99

Camp tool, hand-to-hand combat weapon, or throwing missile; the tomahawk has many facets. American Indians, Mountain Men, Explorers, Soldiers, and Pioneers swore by them. Battle axes and throwing axes have been used by warriors of all nations and all cultures throughout history.

These are 11 1/4" overall with a 6 3/4" head. They throw excellently and take and hold a good edge for camp chores or combat. The handle will break with a bad throw, but can be easily replaced with a new one cut from a sapling. The head has a round eye making handle replacement simple. I have five of these 'hawks - three with sapling handles, and they still throw like a charm! I am never without one in the field. No warrior's kit is complete without a 'hawk!

Large Night Watchman - United Cutlery- Taiwan
UC812 - $12.99

A nice heavy weighted aluminum nightstick, 19 7/8" long which unscrews a-la sword cane to reveal a 13 5/8" stainless steel stiletto blade. This is a handy little weapon although the blade is a bit light to parry with and I am not certain how well it would hold up thrusting through body armor or a heavy coat. Still and all, not a bad choice for your weapons battery.

Gil Hibben Thrower III - 10" overall
Dual Function Hunting/Throwing Knife
UC456 - $17.99

Yeah I know, kinda pricey. But it's the FINEST blade I've ever thrown! And, $17.99 isn't a lot for a good WORKING knife that can also be thrown. A very basic knife - no cross guard, no handle slabs - just one solid piece of heavy, rugged, stainless steel. Strong enough for a working or fighting knife. Good thin profile, easily concealed, nice heavy leather sheath.

All of these are available from:

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

Ψ

Issue #12 - July/August 1995

Cybertek

The Cyberpunk Technical Journal

Technology, Security, Self-Reliance

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

"A people who mean to be their own governors must arm themselves with the power knowledge gives."

- James Madison

The Cheesebox

by Thomas Icom

Background

The cheesebox turns two phone numbers into a loop line. What this enabled one to do was communicate with another party without having to disclose either party's phone number. The first party would call into line one, the second party would call into line two, and the cheesebox would connect the two lines together, enabling the two parties to communicate.

Other variations of the cheesebox, often called "CF (call forwarding) Boxes", or "Diverter Boxes" enabled one to call line one and receive line two's dialtone. These boxes are still available commercially; mated with an autodialer for use in a person's place of business to reroute calls to an answering service after hours.

Implementation

This version of the cheesebox is based around the Parallax BASIC Stamp. This microcontroller was chosen due to its small size, extreme versatility, and inexpensive price. The use of a micro-controller also enables one to use a minimal amount of support hardware, as control functions are handled via software.

There are two versions of software for this device. The first listing is designed to go off-hook as soon as a ring is detected on the primary (incoming) line. The second listing waits 30 seconds (The time can actually be any length up to 18 hours. That's one of the nice things about using a microcontroller.) after hearing an initial ring; at which time it will then pick up on the first ring of the next incoming call.

After detecting a ring, the device picks up the primary and secondary (outgoing) line. If the secondary line is not in use, one will receive the secondary line's dial-tone. If the secondary line is ringing at the time of seizure, the device will "answer" it. To the caller on the secondary line, this would sound like a regular phone call (alleviating some suspicion if instead the caller was just told to dial the number and wait in silence; thus indicating potential cheesebox usage). If the secondary line was in use, the caller into the primary line would be thrown into the conversation occurring on the secondary line. While this might prove to be interesting for PSYOP purposes, the use of this device in its current configuration for surveillance would be a poor choice, as the audio path would be two-way, and cheesebox picking up the secondary line would be as detectable as if someone picked up a regular extension (ie. a "click" would most likely be heard, and the line voltage would drop).

Once the Stamp picks up the phone, line voltage is used to latch open the two 12V line relays. The Stamp then goes back to waiting for a ring detect again. When the caller on the primary line hangs up, the line voltage will drop to zero and the relays will unlatch. The cheesebox is ready for another call.

When the Stamp is in its normal state, it draws 2 milliamps of current. When it picks up the phone, this goes up to 22 mA for about three-quarters a second. Under those circumstances, a 9V 600 mAh battery will last somewhere around ten to twelve days. This is extended by using the Stamp's sleep feature so that the Stamp only checks for a ring roughly three times a second;

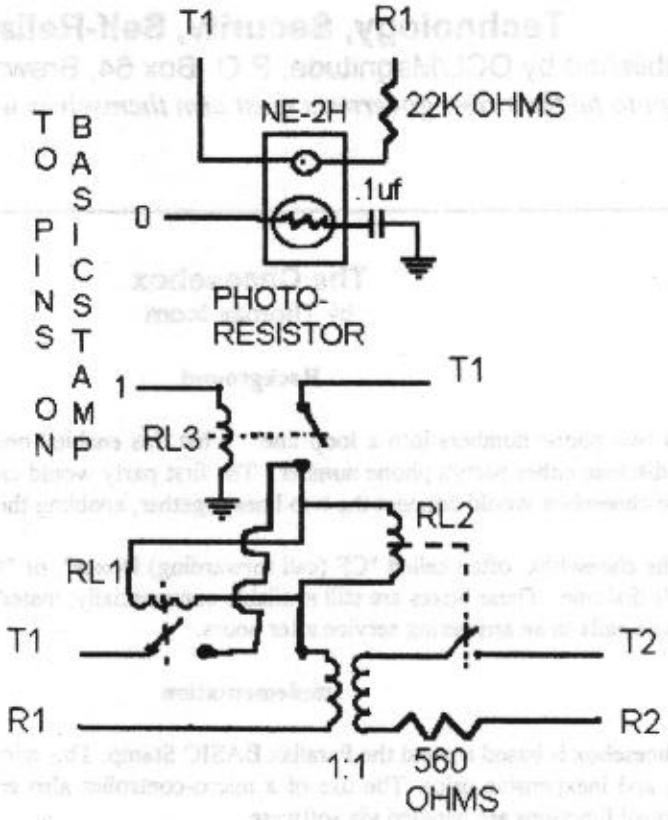
as opposed to a thousand times a second. When in sleep mode the current draw is only 20 uA (0.020 mA). This should extend the battery life to somewhere between twenty to thirty days, depending on use.

Hardware Construction

The first thing you should do is read the manual that came with your BASIC Stamp programming package. It's full of useful information you will need to know in order to successfully complete this project.

Hardware construction is pretty straightforward, due to a minimum number of components involved. The following will be required:

1 BASIC Stamp I Module with carrier board (available from Parallax)
1 BASIC Stamp Programming Package (Parallax)
1 Ring Detector Module, which consists of:
  1 NE-2H Neon Lamp (Radio Shack #272-1102)
  1 22K Ohm Resistor (Radio Shack 271-1128)
  1 Photocell (exact type not important. I used one from Radio Shack's #276-1657 package.)
  1 .1 uf Capacitor (Radio Shack #272-135)
1 5V SPST Reed Relay (Radio Shack #275-232)
2 12V SPST Reed relays (Radio Shack #275-233)
1 1:1 600 Ohm Isolation Transformer (Radio Shack #273-1374)
1 560 Ohm Resistor (Radio Shack #271-1116)
Hookup Wire
Electrical Tape
Electronic Tools (Soldering Iron, Solder, etc.)
4 Alligator Clips
1 Decent capacity 9V battery, preferably rechargable (such as the 600 mAh Radio Shack #23-229)



T1, R1 - Primary Line
T2, R2 - Secondary Line
RL1, RL2 - 12V Relay
RL3 - 5V Relay

The BASIC Stamp and Programming package can be ordered from:

Parallax
3805 Atherton Rd. #102
Rocklin, CA 95765
916-624-8333
FAX: 916-624-8003
BBS: 916-624-7101
FTP: ftp.parallaxinc.com
WWW: http://www.parallaxinc.com

This should all fit on the prototyping area of the Stamp's carrier board, although some care should be taken as to placement. The one step that should be paid attention to is the ring detector. This consists of the neon bulb (with it's dropping resistor) and photocell.

Take a length of electrical tape and wrap the photocell and neon bulb together, taking care that the leads of each component don't touch. You want to make this as light-proof as possible, a second layer/piece might be necessary. When this

is completed, attach the dropping resistor to one of the neon bulb's leads and attach the neon bulb/resistor combination to the phone line. Attach an ohm meter to the leads of the photocell. You should get some high reading. Now ring your phone and watch the ohm meter. The reading should go down significantly. If it does, then your device works. If not, check the construction and try again. The exact readings are unimportant, you just have to get a high reading when it's idle and a low reading when it detects a ring.

Once you have the ring detector working, you can attach it to the Stamp according to the schematic and calibrate it. Load up your programming software, attach and power up the Stamp, enter the editor and press Alt-P. When asked for the pin, input "0" (That's the pin you connected it to.) Hook up the ring detector to the phone line, and while the calibration routine is running; ring your phone. Write down the scale value that appears, you will need to put it in the source code at the appropriate place. (You should understand once you become familiar with the Stamp and see the source code.)

After the hardware construction phase is completed, load up your programming software, and put one of the following pieces of source code in the stamp.

Software

Pick Up on First Ring Version
CHEESE1.BAS:

```
start:  goto wait
pickup: high 1
        pause 1000
        low 1
        goto start
wait:   pot 0,xxx,b0    'xxx=The # received during calibration
        if b0>0 then pickup
        nap 4
        goto wait
```

Ring Once and Then Call Again Version
CHEESE2.BAS

```
start:  goto wait
pickup: high 1
        pause 1000
        low 1
        goto start
wait:   pot 0,xxx,b0    'xxx=The # received during calibratio
        if b0>0 then window
        nap 4
        goto wait
window: sleep 30
secheck: pot 0,xxx,b0   'See earlier pot command.
        if b0>0 then pickup
        nap 4
        goto secheck
```

Operation

Operation is pretty straightforward. A nine volt battery is attached and the box is hooked up to two phone lines. The primary wires will be attached to the incoming line, and the secondary wires to the outgoing. When a call is made into the primary line, the caller will be switched into the secondary. When the caller hangs up, the cheesebox resets itself and waits for another call.

Ω

The Essence of Warfare

by **Atreides**
The Nemesis Group

Heraclitus noted that a man cannot walk in the same river twice, for it was not the same river, and he was not the same man. Less eloquently, things change. It stands to reason that conflict, at once the driving force for change, the method of change, and the fall-out from change, would itself change in nature over time. As things change, and we are able to observe more of it, certain patterns begin to arise; distance, in space and time, certainly lends perspective.

Once Man thought the Earth was the center of the Universe; then Galileo worked out a theory of motion, and paid the price; Newton comes along, and given some room for contemplation, generalizes a number of principles; Einstein catches some flaws and postulates an even more generalized set of theories. We all stand on the shoulders of Giants.

No surprise, then, that some basic concepts behind the Art or Science of War are becoming more evident as we once again transform our ways of thinking on the subject.

Approaches to conflict in the world fall into a four-quadrant grid, passive-active on one axis, defense-offense on the other. Passive defense stems from the assumption that a situation is 'friendly,' while active defense assumes 'hostile.' American activities tend to fall into this first category, while those of the Cold War Soviet Union fell into the later. Passive defense is lethal--no wonder that America has found itself playing catch-up on every conflict it has ever engaged in. The inherent danger of active defense is seen in the fall of the Warsaw Pact and sponsor; total collapse from exhaustion as they actively tilted every windmill.

The other grid half is the realm of the active and passive use of force. Active offense, primarily the unnecessary bifurcation into attrition and manoeuvre warfare, is an area of excellence for the United States. Passive offense is an area that eludes the military establishment, although, as I will explain, this isn't necessary with a deeper understanding of what conflict is about.

Life is the struggle for the free energy in a system; even the most basic organisms are primarily 'concerned' with metabolism and reproduction. As a political economy progresses and evolves, interesting things happen, as you would expect in any system where complexity can be measured by the combinatorial of interaction of the aggregate sub-systems. Political economies (PE), social structures if you will, can be defined by the depth of what can be called 'dependency infrastructure,' or the 'value add' chain.

The most basic political economy is that of the Agrarian society, The Age of Bread. Such social structures have a very short 'material' value chain (phases in a process where the receiver of the process experiences a net gain in value or performance because of the prior process), and a short 'informational' value chain. For example, the material value chain of hunter-gatherers is minimal, just the raw labour involved in the acts of hunting and gathering, and the informational value chain is food stuff identification and processing knowledge. Slightly more complex is a feudal society, where already the material-based labour component was being replaced with the informational--blacksmithing and tack to create plows, knowledge of planting seasons, milling grain for bread, animal husbandry. This period is still preoccupied in the struggle for the basics of life--food, shelter, warmth, procreation (Maslow's Hierarchy); resource, labour, and capital are King (usually quite literally, trapped in a zero-sum game, hierarchical political economy).

The next phase of development is the Industrial Age, The Age of Mass Production. This phase has long value chains in material resource (components to build components to build components...; tools to build tools to build tools...), and a steadily growing value chain in informationals. Additionally, considerable effort is dedicated to the social contract, another example of spontaneous order, which allows the complexities of a political economy to function. The human species, not content to let such systems be self-regulating, has wasted enormous resource in the attempt to govern (in a cybernetic sense) the process, not realizing that where there is free competition, there is no dependency, something most groups claim to desire.

The current phase of development is what has been termed the Information Age, the Age of Patents. Material value chains are beginning to die back, while the informational value chain is increasing; this reflects the situation that embodied thoughts can have value (and in fact are replacing the resource-labour-capital triad), while still being dependent upon the infrastructure. Western civilizations, the most advanced of this phase, are fumbling with the new informational value chain that progresses data into information into knowledge into wisdom; most effort actually goes into simple shuttling of raw data and a little

information from here to there. The social contract is more confused than ever; specialization has been forced by the complexities of getting to this phase, yet most of the critical basis for interaction is being undermined. It is still increasingly an age of positive-sum games, heterarchies, etc.

Interestingly, extrapolation of this trend leads to a further or complete decay in the material value chain, possibly because of advances in space exploration or nanotechnology. We'll have to wait to get there-then to see which it is.

Now to return to conflict. In the Agrarian Phase, direct control of the means of production through possession was necessary; from this phase we have centuries of examples of 'conventional' warfare, attrition style. As advances were made into the Industrial Age, devastation of the dependency infrastructure was no longer a viable option--what was broken couldn't work for the winner's benefit. This led to progress in manoeuvre warfare, where control became important, rather than devastation. Other than a decidedly significant side-trip because of atomic and then nuclear weapons, this remains the guiding principle of modern warfare. In fact, it demonstrates (satisfying the correspondence principle as well) a more fundamental nature of 'warfare' oriented around the dependency infrastructure (DI):

-- Conventional warfare seeks victory by overwhelming or through forcing a failure of the opposition's DI.
-- Manoeuvre warfare seeks victory by taking control of key elements of the opposition's DI, essentially imparting control.
-- Guerrilla warfare orients around opportunistic attacks on the opposition's DI, making the energy cost of conflict too great to maintain.
-- Political warfare is control of the members of a political economy through (establishment and) control of a DI, coupled with media manipulation, propaganda.
-- Terrorism is a case of actions taken against the social contract to attract media attention to a conflict when the media is (perceived to be) controlled by the opposition.

A dependency infrastructure is composed of widely varied elements of the social contract of the political economy--command-control bodies, social services, education, the workings of an economy, communication systems, spiritual leaders, anything that supports the value chain of the phase.

Warfare, then, is about the control of the dependency infrastructure; some forms of warfare need not require a single shot to be fired, instead seeking victory through establishing control of the dependency infrastructure. This cognitive tool explains many things:

-- Gandhi was successful in large part by his demonstration that the infrastructure of the raj was in the control of the Indian people, and they reasserted themselves in this fashion. Other strategies of Gandhi bear study, including his self-creation as a media symbol and deliberate infliction of harm upon that symbol as a method of war, whether through his being arrested, or fasting to the point of personal bodily harm.
-- The problem of Iraq for the West, post-Gulf War, is that their dependency infrastructure was left intact, and in the hands of Saddam Hussein. This does not question the validity of the conflict itself, which has been claimed to be in the 'national interest.' The rule of thumb to see if something is a national interest? Does it have an effect on your dependency infrastructure to a dangerous degree. Any singular control of significant OPEC resources can be viewed as a weapon in the making.
-- Social unrest occurs because of a failure of the dependency infrastructure for those suspended and dependent inside it; riots are a symptom of this disease, by people who suffer from a cultural disease we have no name for.-- The odd relationship the U.S. has with terror; access to the free media market has become important to support for a cause, while the blind eye the U.S. turns on certain issues makes them a target. Any group who feels a media bias on an issue, Palestinians versus Zionist occupation, Ireland versus United Kingdom rule for example, will be caught trying to have it both ways.
-- The problems the U.S. faced in Viet Nam, such as the inability to control a dependency infrastructure with air strikes, or the total corruption of the allied infrastructure, driving anyone adversely effected to the alternative infrastructure supplied by the Viet Cong and NVA.

It also suggests a new form of warfare where victory comes from the establishment of alternative dependency infrastructures in a political economy, in conjunction with propaganda efforts (which would be useful in the Former Soviet Union, Central and South America, or North Africa for example). Let me also add that it is going to be a serious failing in areas such as Gaza/West Bank where no infrastructural development is being undertaken, the greatest threat to peace in the region.

Following this chain of reasoning, even new areas of thought on conflict make sense, such as the special case of information warfare--at one end it can be used as a weapon of mass destruction (WMD) just as nuclear, chemical, and biological weapons which overwhelm the dependency infrastructure of an opponent, and at the other end it can be used in guerrilla, terror, or political warfare to selectively destroy or surreptitiously control the dependency infrastructure. Seen on these terms, it makes perfect sense in terms of doctrine; it also explains why it is an increasing and soon to be critical threat to the nations of the West.

Conflict this far down the line is not getting any easier. To understand what is occurring in Bosnia or Somalia, you have to put them in their context; to understand future conflicts, with guerrillas, terrorists, propaganda, hackers, cyberpunks, et al, we will have to search for the basic essence of conflict--because only by understanding those basic principles will we be able to prevent the world from falling apart around us, or at least not be caught out by it when it does.

Ω

Alternative News Gathering Techniques

by **Thomas Icom**

What never ceases to amaze and disgust me is with the extensive means we have in this country for the dissemination of information, I find that it is more difficult to get real news about matters regarding personal survival, than it is to find out the latest fad in Hollywierd. I don't know whether it's because the American people have sunken to the lowest common denominator, or if it's because New World Order advocates in the media are deliberately trying to keep the people ignorant to further their aims

James Madison once said "A people who mean to be their own governors must arm themselves with the power knowledge gives." With that adage in mind, it would make perfect sense for the totalitarians to keep their potential subjects in the dark, as it would make their ascension to power easier. Whatever the reason, the result of this situation is that people into personal security and self-reliance have to make a little extra effort to stay informed.

Ironically enough, one of the best places for certain types of news and intelligence is the idiot box (TV). If you have cable, you probably have access to a network called "CSPAN". CSPAN is a public affairs network that feeds the activity of the senate and house of representatives right into your home without any commentary attached. When the house and senate aren't in session, they cover press conferences and meetings of public organizations. Not only does CSPAN let you see what your "elected representatives" are up to; it lets you know who your friends and enemies are. The latter can also be said of monitoring network-TV news and "popular shows". If you can stomach it, watching network-TV will also give you a practical education on enemy psychological warfare techniques. Such an education is necessary in order to implement effective counter-measures.

One of the "better" networks for news is CNN. Since all they do is news, they will report on things that will be missed by the other networks. The drawback to CNN is that you need to have Cable TV in order to get it. For those in areas without cable,I would suggest checking the FM and AM broadcast bands for an all-news station. Some news radio stations do rebroadcast CNN's audio.

The shortwave bands still remain one of the best sources for alternative news information. Despite their increasingly socialistic leanings, you can still receive better quality news from overseas stations such as the BBC and Radio Duestche Welle than you can from CBS, NBC, and ABC. More American stations are also coming on the air; a radical departure from the days when the VOA (Voice of America, a government run station) was this country's only voice on shortwave. These American stations, particularly WWCR, provide an excellent amount of alternative news and current affairs commentary in their programming. Specific frequencies for a shortwave broadcaster change periodically. A current issue of Popular Communications or Monitoring Times magazine will provide you with specific frequencies and times of broadcast, but if you just want to tune through the bands and look around, the most common frequencies (in Khz.) used for shortwave broadcasts are:

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

The frequencies below 10000 Khz. are better for nighttime reception; while those above 10000 Khz. are better for reception during the day.

Small press publications, colloquially known as "underground newspapers" or "'zines" are more popular today than ever with the advent of desktop publishing systems and personal copiers. I personally believe that the advent of low-cost personal computer-based publishing systems was one of the greatest things ever to happen to the cause of freedom! The reason behind this belief is that now anyone with a little spare cash and a cause can become their own press. So, what was once the domain of big corporations is now the domain of anyone who wants it!

There are too many excellent alternative press periodicals out there to list. I'm going to list a few of my favorites, but for more **I strongly suggest you subscribe to Factsheet Five**. Factsheet Five is a 'zine whose entire purpose is reviewing other 'zines. If you're looking for it, you'll find it in Factsheet Five. Factsheet Five is generally available at your local Barnes & Noble bookstore, or you can get it via mail.

Still talking about computers, another excellent alternative news gathering and dissemination technique are computer bulletin board systems (BBSes). A BBS is a computer system that is set up by a private individual for the purpose of other people calling into it to leave public messages private messages (e-mail) to other users, and public-domain (free distribution) software. Some of these BBSes are networked; which means that you can make a local call to a nearby BBS, post a message, and have it distributed across the world in 24 hours. Every semi-populated area has a local BBS that is part of "Fidonet", the largest of the BBS networks. Most BBSes are free to use; with you just paying for the cost of the phone call; although some solicit donations to help offset the cost of running the system.

All of this is done with your computer and a device called a "modem"; which interfaces your computer system to the phone lines. Modems and BBSes are another great invention for cyber-libertarians and other dangerous types who are into freedom. If you want to say something, just jump on your local Fidonet node and within a day or two your opinion will reach the opposite coast and everywhere in-between.

It's easier to get in the BBS scene than it is to get into desktop publishing. All you need is a computer, a modem, and a terminal program to make the two work together. You don't even need a "state-of-the-art" system to do all of this, as the standards used for communications are universal between the various computer systems.

Again there are too many BBS systems out there to mention them all, but for now I'll mention the official Cybertek BBS; RuneStone BBS, (203)-832-8441. When asked for the "newuser password" enter the word: CYBERDECK.

Going beyond BBSes, we have the Internet. The Internet has come a long way since its inception. It eliminates the disadvantages of BBSing (large LD phone bills and a relatively small audience) while retaining all the advantages. There is already a ton of information out there available on the Internet, so I won't go into any major detail on it. Nevertheless check it out. It's a very powerful tool.

In regards to news in your local area, the best thing I've seen is a "scanner radio". With one of these tuned to your police and fire frequencies, you'll get a first-hand report of events in your local area. While some places are beginning to scramble their radio transmissions, overall the practice isn't common. It might also pay to attend your local town-board meetings, as this will also give you a first-hand look at how well, or poorly, your community leaders are doing.

The entire shortwave frequency spectrum (1 Mhz. - 30 Mhz.), as well as the AM and FM broadcast bands will probably 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 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.

Also of interest to survivalists is the Emergency Broadcast System. This is run by the mostly non-existent 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 Emergency Broadcast System other than the fact it exists. However, if you have a spare AM/FM radio, or TV it might prove at least interesting to listen too, just to see what little the government informs you off, 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 might also want to tune around the ham radio bands in the event of a nationwide 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 infogoes over these frequencies; both official and unofficial. Common frequencies are:

3500 - 4000 Khz. (80 Meter)	7000-7300 Khz. (40 Meter)	14000-14350 Khz. (20 Meter)
21000 - 21450 Khz. (15 Meter)	28000-29700 Khz. (10 Meter)	144-148 Mhz. (2 Meter)

The frequencies labeled in Khz. are shortwave frequencies, and offer worldwide coverage. The 80 and 40 Meter bands offer better coverage at night. The 20 Meter band offers decent coverage around the clock. The 15 and 10 Meter bands are best during the day. The 2 Meter band is a local coverage band which is useful for finding out news regarding your local area. Also potentially useful to listen too would be the CB band. Everyone has at least one CB which makes it a good community "jungle telegraph".

The above is just a small sampling of radio frequencies that might yield useful information. You will also want to read Thomas Roach's excellent book The Hobbyists Guide to COMINT Collection and Analysis which was reviewed in Issue #10.

Small Press Periodicals Worth Checking Out

2600 Magazine: The Hacker Quarterly
P.O. Box 752
Middle Island, NY 11953
516-751-2600
Good magazine covering computer and phone security. You'll also want to acquire the eleven years worth of back issues, as they make great reference material.
$18/year

Factsheet Five
P.O. Box 170099
San Francisco, CA 94117-0099
$20/year
Reviews other small press 'zines. Excellent source for those of you wanting to expand your sources of alternative press periodicals.

Gray Areas
P.O. Box 808
Broomhall, PA 19008-0808
$23/year
A highly recommended magazine that covers "the gray areas of Life" - 'nuff said! Netta Gilboa, the editor and poublisher, is one of the few people I've seen who has given the computer underground an objective and realtively unbaised look, and let them have their own unedited voice; despite all the shit that certain STUPID people in that community have given her. (Those who disagree should compare her coverage of the community with that of the establishment media.) That fact alone gets her my support.

U.S. Militia - "The Only Magazine For Community Defense"
Kurt Saxon's excellent periodical version of The Poor Man's James Bond.
$35/year

Shoestring Entrepreneur
Another excellent self-sufficency periodical by KurtSaxon. This one is geared towards learning a trade and using it to go intobusiness for yourself.
$15/year

Kurt's periodicals are available from:
Atlan Formularies
P.O. Box 95

Alpena, AR 72611
(501)-437-2999

Iron Feather Journal
c/o Stevyn
P.O. Box 1905
Boulder, CO 80306
$5 for current issue
This techno-anarcho 'zine is another favorite of mine. I think Jerod Pore put it eloquently and accurately in Factsheet Five #52 when he said that *"Iron Feather Journal is the Anarchist's Cookbook of the '90s, without all the bogus data that would get you killed."*

Ω

Telecom Remote Control
Part 1: Introduction
by Thomas Icom

The use of the telecommunications network for remote control purposes has a number of advantages. It's world-wide in scope; allowing you to reliably activate remote control devices from anywhere in the world that has phone service to anywhere in the world that has phone service. While you might have problems in an underdeveloped third-world country, you won't anywhere else.

A number of signalling methods are available for telecom R/C applications. The first and easiest is a simple ring detect. The phone rings and the device activates. This does have the disadvantage of lacking control; as any ringing after installation will activate the device. To help alleviate this problem, you can add a counting circuit so that the device isn't activated until a certain number of rings have occurred. Another way is to adjunct the ring detector with a timer switch, so a certain amount of time must elapse before the ring detector becomes active. A benefit to ring detection is that the caller isn't billed as the phone isn't answered.

You can also have an auto-answer module with a DTMF decoder. In this instance, the device will be activated upon receiving the proper sequence of DTMF tones.

Dual-Tone Multifrequency (DTMF) tones, or "touch-tones" are the most common signalling method for R/C applications. DTMF signalling was originally designed as a means for quicker dialing for telephone subscribers. It's versatility has lent itself to other signalling uses. The wide availability of DTMF equipment has made it a common signalling method for accessing voice mail, interactive phone systems (such as the ones banks use for customers to receive their account information), remote dial-ins for PBXes, WATS extenders, and answering machines, and R/C devices.

The wide availability of DTMF equipment is also a security disadvantage. Your R/C device is vulnerable to anybody with a touch-tone phone and a little time on their hands. You can counteract this somewhat by making security codes longer, but this will lower efficiency by increasing system usage time, and might present a memory obstacle to the systems' users; who then might violate a basic security measure to assist them in accessing the system. (i.e. Never write anything down.)

Discrete single or dual tone signalling can also be used. Since the tone signals would be proprietary, security would be increased. The actual frequencies could be changed at will for an even greater increase in security.

To this end, many DTMF encoders and decoders can be modified to transmit and receive signals which are of a different frequency than those used for DTMF signalling. This is done by changing the reference crystal hooked to the device's encoder or decoder IC. A common example of this is the replacement of the crystal in a particular model of DTMF dialer in order to generate coin tones for toll fraud purposes. In our case however, a DTMF dialer is modified to satisfy a legitimate security need for a telecommunications based remote control application.

The ultimate method in security and versatility would be a microcontroller and an auto-answer modem. You could require a password to access the system, and then additional passwords to activate various devices. The modem could require any number of rings to answer. Finally, the micro controller could be programed to only accept certain commands at certain times.

The use of caller ID (CID) in telecom R/C devices adds another dimension to security. Devices can be set to activate only if called by a certain number. It would be no major feat to wire up an and-gate to certain segments in a CID box's display, so a control line goes high when a certain number calls. The caller would also not be billed for the call, as the CID data is sent during the ringing cycle.

The construction of devices for telecom R/C is easy due to the wide availability of off the shelf equipment that is either readily modifiable, or adaptable to "kit bashing". You should be able to assemble a plethora of devices after visiting a few tag sales, flea markets, surplus stores, pawn shops, or their local Radio Shack. By going that route one will be able to keep costs down. Even in an extreme condition you can acquire the necessary materials from a department store, but why spend $30 for a new piece of equipment you're going to take apart when you can spend only $5-$10?

In Part 2, I will present some telecommunications remote control projects and applications

Ω

The Precipice Problem: A Guide to the Destabilization of Western Civilization

by **Atreides**
The Nemesis Group

No one but a sage can utilize espionage... --Sun-Tzu

1.0 Introduction and Background

It has rapidly become possible for a small group of knowledgeable and skilled individuals to create chaos, wreak havoc, destabilize, and potentially destroy what is currently referred to as 'Western Civilization.'

Once it was possible to accomplish such goals through the removal, by various means, of the ruler of the dominant country of the 'Empire.' Rendering unto Caesar what is due him becomes moot if Caesar has been eliminated. However, the swift rise of democratized countries as the dominant powers of the world has added a certain amount of cultural resiliency, making such a manoeuvre obsolete. In its stead has arisen a new, more virulent, form of attack--such empires are now built upon economic strength (Gross National Product [GNP] is the most critical factor to be taken into account, even regarding military strength; witness the resolution of the Cold War in favor of the U.S. and NATO forces over the Soviets and Warsaw pact forces strictly via extended economic, as opposed to military or pure ideological, conflict), and such strength can be swiftly negated, as it relies upon technology. Caesar could always be quickly replaced, an economy cannot be.

Negation of an economy, and hence a country dependent upon it, is accomplished through the skilled manipulation and usage of technology in conjunction with the exploitation of the flaws--inherent, accidental, or deliberate--of a technology-based society.

An economic maxim of obvious truth is that control of the means of production implies control of a society. While the maxim has remained the same, the factors comprising it have evolved--the means of production have changed from the factory worker to the 'knowledge' worker and electricity has transformed from a unit of work to a unit of information, but then again, so has everything else (money, etc.).

Termed the Information Age of Western Civilization, it has given new possibilities and benefits to the citizens of the West, although it has left them in a completely exposed position as far as long term viability is concerned. It has created new avenues for dominance and manipulation [which is why the Japanese are trying to dominate through technology], and ultimately, the power to destroy is the power to control; technology is a sword which cuts both ways, an Achilles' Heel of the West.

'Western Civilization,' as it has evolved and currently stands, is defined by its advanced technology. Such technology is a recent development, historically speaking, and thus the window of opportunity for such an economic attack has only just opened. The combination of such 'newness' with the almost immediate dependence upon the usage of technology has created the most significantly vulnerable area of attack in the history of the culture.

The maxim 'those who do not study history are doomed to repeat it' once again plays truly in this case. For example, essentially every culture has built bridges; in fact, bridge building, masonry, goes back into the depths of time. Yet every culture, when learning to build bridges has made numerous mistakes, usually costing numerous human lives. This is the price associated with learning; tracking these developments eventually leads to the science of engineering.

The history of engineering, which builds bridges, ships, or airplanes is that of one disaster after another, but always something that can be learned from. What develops is an engineering 'rigor': performing testing and extensive analysis, and not trusting that something can be reliably done until you have actually done it.

Yet when it comes to technology, it seems that reason flew out the window. Even though you can't test code the way you can test metal or concrete's material strength, even though there are one-of-a-kind systems that were never intended to be doing the job they are forced to do, the West has passed over complete control of the critical functions holding their society together to the unreliable machines. Why? Because it was convenient, and some things (such as the large volume of phone traffic or banking transactions) just weren't possible otherwise.

The individuals 'in the know' on these problems are perfectly well aware that they can't verify the function of their technology, can't be certain that it does what they say it does reliably, and have no way of being positive that it doesn't do more than it says it does; they can't even guarantee 'bugless' code, let alone 'hardened' systems. But if nobody says that the Emperor has no clothes, maybe no one will notice. Perhaps a good example is that of the 'rules of the road': everyone knows that driving can be dangerous, yet sane drivers in sane situations will obey the common courtesies of driving (staying in the proper lane, stopping at lights and signs) even in the absence of an enforcing officer. Why? Because the potential for danger to life and limb is greater once you 'break' the rules. Here we have a similar situation--if everybody behaves and treats the systems very nicely, then they will continue to function as intended; stray outside the decorum of good behavior, and you have a disaster on your hands.

But that still leaves a vulnerable situation, an accident waiting to happen, or an opportunity looking for someone to take advantage of it if they know what they are doing.

A further note--it is only getting worse (or easier, depending on your viewpoint). Every day, more is automated, more network connections are established, more people, places, and things become dependent upon technology. Because of this, a society that is already standing on a Precipice becomes even more unsteady, stands on less firm ground, waiting to slip. Or be pushed. Remember, this isn't a case of 'going downhill'--it's a case of dropping off a steep cliff.

The advancing policies of both industry and government are actually increasing the risk the West is in; for example:

The creation of various standards (whether de facto through market clout or through imposition) does incredible damage; the major limiting factor to disease in humans, crops, and livestock has been the heterogeneous nature of the population; reduction of the technology arena to a homogeneous environment (for instance, with a major dominant hardware platform and operating system such as is occurring) only paves the way for the wreckers;

Almost every group in the West with some interest in computers, communications, consumer products, or technology in general is pushing for the creation of a 'super datahighway' or greater connectivity; if the dreamers have their way, everybody will be connected by a tangled web of twisted pair, coaxial cable, optical fiber, microwave, radio, and even local infrared.

This bestows great access upon John Doe, but it also builds an irrevocable dependence in the economy, the way people do business, and the way the culture works; even though technology has become wide scale in the financial community only within the last decade, groups such as banks, credit suppliers, or stock brokers would be helpless without it. Now extend that to John Doe, and see how little cash money he carries, how dependent upon 'plastic' he is, and how much chaos his life will be if everything crashes.

In addition to the economic functions that advocates wish to be turned over to the new systems, there are numerous social ones--from medical care to electoral voting; the potential damage that will eventually be able to be done is beyond calculation.

No large scale organization (from 'Empire' to the human body) can exist without a fundamental bedrock of communication and infrastructure, yet we see that the expansion of the existing 'Empire' has foundations built upon sand, and worse still, we're

busily at work pulling up the old granite foundation and replacing it with sandstone, all in the interest of renovation. Madness, indeed.

2.0 Operational Overview

Critical potential targets of the problem are the infrastructure of the economy. Much like a circulatory system in a human body, which provides oxygen and nourishment to the various parts, the infrastructure of an economy acts similarly. Destruction or damage to it on a massive scale causes irrecoverable harm to the basic structure and integrity of the economy. Operational techniques to carry out the 'hostile' outlined program are briefly discussed in the 'Informational' subsection of the 'NCBI' section later in this document.

Let's assume an adversary and see what they could do:

2.1 Telephone Communications

Conventional communications, including voice conversations, fax, data, etc. are providing absolutely critical support for the West--without them, little could occur owing to the dependence upon the frantic 'societal pace' and sizable and diverse territory covered. This dependence includes all transactions--domestic, international, government-- yet even the most sophisticated of communication set-ups is an AT&T 3B2 UNIX minicomputer with a telephone backplane hypernetworked together as an electronic switching system. Such systems are trivially simply to disable, commonly causing cascading malfunctions on their own.

Other component parts of the communications grid are also easy targets, such as the microwave transceivers, or satellites themselves, which can be brought back down to the ground through reprogramming of their on-board but ground-controlled attitude jets (simple to do if one can grab the legitimate equipment and software used to do such). The emergency 911 and 911E systems could also be specifically targeted in advance to contribute to the impact of the impending chaos.

Disabling the telephone system also, as collateral damage, disables all ancillary services which depend on communications via the system: police, fire, emergency medical care, alarms of all kind but primarily of security systems, power control, water, sewage regulation, etc.

Take as a case study the mishap which occurred in New York on Martin Luther King Jr. Day only a few years ago. Cascading failures of the switching systems caused communications havoc for the 'long lines' of the Eastern Seaboard. It is still inconclusive whether outside interference contributed to the failure, but the cost was enormous, even on a Federal holiday.

2.2 Power

Power generation plants are manually controlled, thus making them fairly resistant to tampering and manipulation from informational warfare attacks. This is primarily due to their having been designed and constructed during a period in which fail-safes were taken more seriously, as well as the potential for civil unrest, coupled with the fact that most are pre-'information age'. However, the power distribution and regulation systems are electronically controlled, making them potential targets.

If a hostile party wished to indulge in physical operations to augment the informational warfare, American power generation targets are 'easy pickings' from that stand-point. Security designs are remedial, coupled with poor implementation. For example, one nuclear power plant TNG principals analyzed had no 'forcing factors' requiring a confrontation with security systems or forces to destroy the plant; security is geared to fit regulation requirements and keep protesters away, rather than prevent an actual attack. The security precautions also seemed, absurdly enough, to take for granted that an attack would be aimed at taking control of the plant, rather than simply destroying it (which could be accomplished from outside the security perimeter with three people and costing less than $10,000 [U.S. 1993 dollars]).

2.3 Financial

Making direct attacks on the financial community that the West depends upon is quite easy--the emphasis in this community, even when security was considered worthwhile (security does not contribute to the 'bottom line' of quarterly profit and loss statements, and is thusly considered a waste of capital), it has been focused on prevention of theft, not against malicious attack. Even then, theft is covered by insurance, and the amount stolen comes nowhere near the amount necessary to retrofit more security into the systems; it is considered acceptable loss.

Obvious initial targets are the large funds transfer networks, such as SWIFT; domestic banking, and the now common method of access, the Automatic Teller Machine (ATM), is easy to cripple. Also targeted could be the credit system, including credit cards and credit bureaus (TRW, CBI). The average individual in Western Civilization has grown dependent upon plastic and 'vapor' money of the Electronic Age; commonly they have less than $100 (U.S., 1993 dollars) in negotiable tender on their person, trusting in their ability to quickly and conveniently get what they need.

This is all, however, just icing upon the cake. It is possible, with a little help from the systems already in place, to destroy the world's currency, capital, and equity markets in a matter of minutes. As the speed of technology came into play in the financial world, the brokerages and financial organizations quickly took advantage of it; it is now a competitive requirement for massive computing power to be constantly watching all the markets of the world, performing analyses, making decisions, and executing orders entirely without the approval or intervention of a human being. Such systems, called 'program trading,' have trillions of dollars at work directly, not counting the leverage gained from their positions; insertion of the right type of orders into the right machines would be devastating and trigger worldwide panic and financial collapse (for instance, the Japanese brokerages selling all their U.S. dollar positions, bonds, and stocks, coupled with reactionary orders in the American trading systems). It is odd that with all the speculation of disaster regarding the removal of humans from the decision loop for military technology, no one recognized the worse impending danger on the economic side.

2.4 Transportation/Logistics

Western Civilization has become so specialized that it is no longer has self-sustaining population centers; once basic logistics are disturbed, such centers of population are at great risk. Aviation is simple to paralyze; air traffic control systems are essential for any civilian flight. For sheer nuisance value, collateral systems such as the SABRE scheduling system could also be targeted. Shipping, trucking, and rail transport can all be crippled through their scheduling and coordination systems.

[The topic of transportation brings a small digression: an analysis of airport anti-terrorism security measures leads to interesting conclusions. It would be educational for the reader to consider the focus and results of terror attacks involving air travel pre- and post- introduction of airport metal detectors. Security measures seem to only have worsened the situation; how does such a discovery extrapolate to the introduction of thermal neutron analysis devices? TNG principals have analyzed the TNA device and conclude that the next generation of such terrorism will involve unary or binary chemical weapons, or non-nitrogen 'firestorm' type weapons, such as thermite (ignited by magnesium triggered by sodium metal set off by a water pressurization fuse). The more things change, the more they remain the same.]

2.5 SSA

The Social Security Administration is 'the hand that feeds'; it is also an easy target. This system, which provides payments for welfare, social security, and veterans, has no protection, no auditing, and no hope of restoration once removed.

2.6 IRS

The Internal Revenue Service quite recently made it possible to tamper with them. Introduction of 'electronic filing' of income tax has created the opportunity to flood their system with bad information (taking names at random from the telephone rolls, accessing the credit reporting system to gather essential information such as their taxpayer identification number and financial status, and then creating a 'bogus' tax return which would be filed).

The IRS system is one of the few 'hard' systems (meaning it has some of the better electronic protection), but it is targetable in two ways: an EMP generator, generating a damaging static charge of 50K volts to any conducting object, can be used to eliminate the system, or the system can be attacked in the same subtle fashion as the most 'secure' electronic systems in Western Civilization (see the section on 'isolated' systems in the Government section).

2.7 Communications

It could add considerably more terror and panic to incapacitate the conventional means of mass communication, cable and commercial or 'network' television. These system are completely dependent upon electronic switching, microwave, and satellite pathways for their deliveries, and security of such is poor, most attention having been focused at prevention of theft-of-signal.

2.8 Government & DoD/Intel

Oddly enough (for one would assume that this sector would be secure), a crippling amount of damage can be done to the government sector. The group responsible for protecting the West against just this sort of an attack, the National Security Agency, has been sorely remiss in their duty (just one small example: The brain trust in charge of technology security for the U.S. let their classified procurement records through most of the 80s be released in a database (Maryland Procurement Office);

worse yet, they didn't know it until they were told by an outsider. Knowing what they were buying provided a good degree of intelligence to the opposition; it also opens a future hole by exposing the type of technology to target to do them damage.).

Granted, making any technology secure is difficult; just as with a locked room, there are plenty of ways to pick a lock, force a door, steal a key, make the owner let you in, or just go through a window. Add to this that most of the people who are supposed to be protecting things are completely incapable of doing so--like virgins talking about sex, they are beyond their competence. There is, however, a sincere amount of deliberate negligence. Their rationale has been that protecting U.S. technology would be dangerous, as it would be exported or stolen, and then the U.S. would be in a position of being unable to break into their own systems, then in the hands of enemies. The implication, of course, is that NSA takes its job of being able to penetrate target systems as more important than protecting the West from a similar danger. Sheer folly.

NSA systems, such as the old PLATFORM network and their in-house system Dockmaster are difficult, but not unassailable targets. The scientists at NSA are counting on their 'isolated' systems to be impervious to this sort of tampering; it is unfortunate (for them) that there is no such thing as an isolated system. Even if the system is behind a giant 'blast door,' with supposedly no contact to the outside world, with the software written in DoD approved ADA, the system is still 'touchable.' The system has an operating system, other applications, the ADA programming tools and compilers, and a host of other mechanisms exist for getting something 'in' to the system, and that's all it takes. Even if the Defense Department were to institute prophylactic measures to attempt to keep such things from happening, Precipice style attacks can target through contractors and other suppliers, making all systems available for informational warfare attacks.

Precipice poses as serious a threat to the military strength of the NATO forces. It was the acknowledged technical superiority which enabled a quick and painless (for the West) end to the Gulf Conflict. Such an 'edge' can be removed quite simply, evening up things considerably (actually, more than evening up--today's typical NATO soldier is mostly helpless without his technology to back him up). Even the tactical nuclear devices will become unusable, as the 'PAL' codes that activate them are not kept on-site in a 'hard' (printed, for example) format that is readily usable; without such a code, which are individually unique per device, things like atomic mortar rounds equate with throwing rocks.

NATO tools of policy, such as Japan, the U.S. mechanism of choice for Asia, are also at risk. Japan is currently updating and relocating its antiquated equivalent of the 'Pentagon.' Analysis of the proposed new installation leaves Japan in a more vulnerable position that it is currently (which is pitiful; CIA has volubly and accurately complained that Japan 'leaks like a sieve' and has rightly refused to share crucial intelligence for just that reason).

Groups in the intelligence community will be hit even harder. As intel moved from HumInt to SigInt, it became more and more susceptible to 'spoofing' (tampering with the signal) or outright destruction of the means of gathering and analyzing the endless amounts of data generated by such systems. For instance, the CIA uses NeXT workstations, notoriously easy targets, for image analysis; the billions of dollars of satellite surveillance gear circling the globe becomes worthless if the systems aren't there to make sense of it (not to mention the risk to systems such as the ARGUS ring). Precipice style informational warfare attacks make an easy target of all C4I (Command, Control, Communications, Computers, Intelligence).

Law enforcement organizations are a mixed bag of security problems. Police, the Secret Service, and the Justice Department could all suffer greatly from major attacks; introduction of systems such as the Federal Crime Information Center, with fingerprint tracking, etc., if they pass the test of the ACLU, won't pass any security test. These groups have already been subject to a considerable amount of scrutiny by the 'underground' and are already thoroughly penetrated; for example, the Drug Enforcement Administration has been penetrated through their primary contractor, leaking names of informants (now deceased) and details of their system. The only group that has a mixed blessing is the Federal Bureau of Investigation, which still relies on pre-microchip technology and techniques for most of their work, lending them some immunity.

2.9 Business

Attacking the business community of the West is trivial compared with other targets. A simple tactic of hitting with maximum stealth and aiming for maximum damage with 'military grade' worm, virus, and penetration attacks will overwhelm any resistance they can offer. Some small protection against electronic attack has been implemented in the business community, yet it has a set of fatal flaws; such protection systems look for 'known' signatures of attack mechanisms, but the new and novel pass right through. Primary targets will be the mainframes, microcomputers, and networks that businesses in the West rely upon for everything from simple word processing, to decision support or factory automation.

2.10 Exploitable holes

Precipice style attacks can take advantage of the fallout from Western power politics and backstabbing. NATO paranoia prior, during, and subsequent to the Gulf Conflict has made Western leaders nervous about providing advanced weapons systems that may be turned against NATO forces by their current users, or, as was the worry with Saddam Hussein approaching Saudi Arabia, by someone acquiring them.

Because of this, the U.S. wanted the ability to deactivate or destroy, via a coded signal, any weapons system that is of American manufacture via 'software.' Such systems are also deliberately vulnerable to electronic penetration attacks (as per NSA doctrine). In an odd twist of irony, Japan has also likely implemented into their technology of military use the ability to destroy or deactivate the system at the hardware level; this is part of a veiled but very real and operational "Japan That Can Say 'No'" strategy that has shown up on occasion throughout our analyses. Knowledge of this weakness has caused the NSA to initiate its own chip manufacturing efforts for critical systems; this effort was out-of-date and outclassed from its inception.

3.0 Non-conventional warfare

We are witness to a new 'theatre' of operations opening up, where the antagonists can be anywhere, at any time, with immense leverage of their resources all out of proportion to the damage they can cause. The training grounds, a 'virtual' place, are not something that can be tracked by satellites, but more live within them; the entry cost to get in the game is so small as to be negligible, something that can be paid for as a by-product of 'riding the grid.' The profile of those capable of informational attacks is a combination of 'Carlos' and 'Robin Hood.' Today is the tomorrow you worried about yesterday.

3.1 NCBI

The crowning glory of non-conventional warfare are attacks carried out using nuclear devices, chemicals, biological weapons, and, as proposed herein, informational attacks. All of these mechanisms are known for their large, rather indiscriminate capabilities of destruction; informational attacks are additionally 'tactical' and can be quite surgical.

3.2 Informationals

As has been outlined previously, this is the primary method for a small group to leverage themselves into a considerable force; what one doesn't have the numbers to make short work of, one needs to stretch out over time. Technology provides the necessary ability to introduce systems over time and in such numbers as to create quite a stir at the previously appointed time, yet this can be done by a few or lone antagonist, and from anywhere they can hook into the 'grid'.

All that is required is the use of sophisticated electronic penetration techniques, computer worms and viruses, and the exploitation of existing 'targets of opportunity.' Such knowledge does not, as yet, grow on trees; there are perhaps a few handfuls of individuals with the necessary skills and desire to carry out a program such as Precipice.

The viruses and worms needed to execute the project are not terribly complex; indeed, this is a benefit, as such 'weapons' have only been discovered in the past through malfunction or when they had activated, post damage, usually in isolated circumstances--yet a full scale attack such as Precipice would target widely, and leave no room for response. Each specific target could be covered by redundant attacks, with one attack being a stealthy, bare-bones style intrusion (ideally a custom built attack aimed at each specific system, rather than a 'shotgun' approach), with the other being new, previously unheard of technology such as:

Morphing viruses, which constantly change their programming code and configuration to avoid a stable pattern that can be looked for;

Binary attacks/data viruses, which reside, Trojan Horse fashion in legitimate systems as only a few necessary bytes, only activating upon linkage with the remainder of the system which was disguised as unexecutable (and hence, a blind spot for 'hunter-killer' prophylactic systems) data files, or a section 'hidden' in 'unusable' sections of the system; such systems also pass through 'firewall' style protection;

Polymorphic worms, which are slightly cumbersome, but can reconfigure themselves to cross machine type boundaries, thus avoiding a 'yeast growth law' limitation to the spread;

'Factory' worms, that take advantage of networks hanging off of networks, by breaking into the 'parent' system, taking advantage of the newly available trusting resources and accesses, then propagating and seeding throughout the 'child' network(s), mutating, and then launching back through the gateway into the larger network;

Cryptographic worms, which infiltrate into the storage mechanism of the system, and encipher with a public-key system all the stored data, and decipher the retrieved data for a period of time, until one day the retrieval half of the pair 'commits suicide' and performs a low level format on itself, thus making all data in the system non-retrievable; note that this attack is deliberately reversible by the reintroduction of the decryption half of the worm;

Envoys, or expert penetration systems, that use knowledge-based system technology to learn from the penetration team and carry out further penetrations on its own.

The main group intended to 'combat' such infiltration, the National Security Agency, has been covering their inability to correct the problem for many years now. NSA relies upon 'secure' system metaphors such as the MULTICS model, yet these were invalidated years ago by the advance of such penetration technology (which can, in fact, use the protection mechanisms to their own advantage). Quite simply, there is little hope to prevent such intrusions.

4.0 Rationale--Who and Why

How would one benefit by such actions as the Precipice style attacks? Who would it profit? As with most things, there are varying colors and shades. Taking the two extremes and examining them is highly educational:

4.1 Full Scale Attack

Once the triggering event has occurred, John Doe and Jane Roe are in sorry shape. For instance, immediately there is no phone, police access, fire control access, medical care for emergencies, alarms, power, sanitation, money, credit cards, financial markets, economy, social programs, television, government or intelligence community. There will be limited transportation (none on a large scale, no logistics, personal transport is mostly temporary as fuel runs out, leaving muscle power), and supplies (food, water, fuel). Likely there will be military with conventional weaponry, their stockpiles, and radio communications available to them.

What happens next is pure supposition, but some things are clear--there will be immediate chaos. Control will be established after a certain period of time; society has a certain inertia holding it together. In the interim, the amount of damage that will be done will total into the trillions; this does not take into account the long term economic effects which will be uncorrectable.

The West will be suffering near-fatal internal strife, and will be quite unable to cope with anyone else's problems at the time. Even afterwards, if control is successfully reestablished, the countries of the West will be, at best, Second World parties, and unable to exert any real influence beyond their own borders for a time.

In what context is it desirable to destroy Western Civilization, primarily those countries that comprise what is known as NATO (North Atlantic Treaty Organization)? When the executing parties have something to gain--possibly their independence from NATO dominance, influence, and manipulation.

Historically, a 'breaking away' of this sort has only been possible when the dominating country was heavily involved elsewhere, financially strapped, or incapacitated. Even the American Revolution (1776 A.D.) was only possible in the context of Great Britain being quite occupied elsewhere. It is also humorous to note the symbolic 'first act' of that rebellion was economic, the dumping of commodities at the 'Boston Tea Party.'

The rules of rebellion are different than they were for the American conflict; the best model for running a modern effort towards self determination was the World War I effort of T.E. Lawrence and his compatriots. Such lessons come mostly in the form of "don't"s:

Don't attack militarily (it only forces the game to be played by the opponents rules, rather than your own [Iraq's miscalculation in the Gulf Conflict]);

Don't attack your opponent's strength directly but hit around the target (destroying logistics, for instance; increasing terror, or helplessness; not falling into a predictable pattern; obvious targets are commonly the best guarded, pitting your forces against your opponent's strength, a serious mistake);

Don't lose or give up your mobility, your foe isn't going anywhere (and if they do, it means you've won, incurring a whole new set of problems);

Don't let your opponent fight a single- or double-fronted war, always force them to maintain a hyperextended (thus overextended) front;

Don't fight a pitched battle, even by mistake, always maintain 'hit and run' tactics that give your forces the advantage;

Don't strike indiscriminately, or strike just to strike, be surgical in the precision with which operations are carried out;

Don't pick simple targets; seek leverage, go for 'more bang for your buck' style targets that cause extreme damage for little effort.

Western Civilization is wide open to attacks governed by these rules--it certainly isn't going anywhere (no one is packing up New York or Tokyo and moving them), mobility and time are on the side of the attacker. In fact, the best method of making such an attack by such 'rules' is by hitting the infrastructure and economy of the NATO countries and their dependents.

A few parties have the greatest desire to see this done; for instance, the Middle East has been the battle field since WWI, and post-WWII, because of the importance of oil and the West's need to control it. The Cold War raged through the region, with the U.S. using Israel (and later Egypt) as a tool of policy and control, ignoring even the most blatant human rights violations perpetrated by the Israelis and other allies against the Palestinians and other targets. But, similar to the way the Spanish Empire ran afoul of the harmless people they drove into the seas, known as the Buccans (for the fires over which they roasted the pigs the Spanish had seeded the islands with) and later as pirates, the Arabs refused to take the situation lightly and have been fighting ever since. Another interested and injured party would be in Ireland; long the target of British oppression, up to and including the earliest programs of organized, State-sanctioned genocide, certain among the Irish have desired self determination for centuries. A 'bytes, not bombs' strategy could be quite appealing to guerrilla and terrorist organizations world-wide; this comes from an increased awareness of the 'feedback' loop that terrorism makes possible. While it has been desirable (from their point of view) for such groups to attempt to force a government response to restrict civil and (in some cases) human rights to foster a feeling of oppression in the general populous, it usually only increases the militarization of anti-terror forces while not appreciably inconveniencing 'the masses' and can cost popular support. A shift in focus to terror activities that are not overtly violent would take away much of the justification of government forces for heavy militarization, would cause more damage to the system than their current methods, are safer for the terrorist, and the only option of response by government forces would be 'regulation' of technology and the jeopardized industries (which is a non-viable option).

The wish to have 'Uncle Sam' and his allies out of their lives have driven many a people to wage an up-until-now fruitless war. Something like Precipice would give them a new option that would break them free. Luckily for the West, the emphasis on the part of such parties has remained 'conventional' militarily, with some focus for their intelligence (including the education of their people in the West) on nuclear power.

The Western intelligence community has been in a difficult position regarding the Middle East (Arabic and Islamic) terrorists. One of the 'rules of the game' is that mutual deterrence works, or at least it used to. The U.S. has long had the ability to track the perpetrators of terrorists acts, knows the training base locations, etc. What has held back reprisals? Other than the obvious "don't blow your source" issue, there has also been a sort of "gentleman's agreement"--the U.S. wouldn't hit them, and the U.S. itself was immune from attacks on 'home territory.' The new players aren't following the rules. What makes something like Precipice attractive to players in the Middle East is two-fold:

It strikes at the very heart of the 'Great Satan';

They don't pay nearly as high a price as the West; other than the very top of the society, there is little intrusion of the benefits of the West, and even then, the pro-West aristocracy is hit, not the ruling elite of Islam, for example. A return to the simplicity of the 14th Century is attractive to these people.

4.2 Limited Conflict

Rather than all out 'nuclear war,' a small 'tactical' war is more likely, and more insidious. The two initial segments motivated to play this sort of game are dissident factions in the West and economically motivated concerns.

There are numerous internal elements of dissension in the West who would see this sort of an option as useful for its real or 'threat' value; the power to destroy something is the power to control it, and there are 'oh so many' ways to cause trouble.

Informational warfare attacks could be racially motivated (the neo-Nazi movement is quite motivated in the technical arena), terrorist launched, started by eco-terrorists, part of a blackmail attempt, or just a casual action by hostile parties.

Money is also a great motivator; a new degree of low-level conflict could mean an economic war of sabotage by 'allies' against each other (witness the programs initiated in Israel and Germany to build a competence in Precipice style attacks), or American usage against hostile 'economic' targets (not outside the realm of possibility; view it as the next step after sanctions--"If you won't stop selling X to Y, then we'll make certain you can't make X."). The Japanese are also gaining an understanding of the techniques and strategies as a side effect of their broad-based competitive intelligence programs. Additionally, industrial spying is breeding a subculture geared for this sort of work; the electronic criminals (hackers, crackers, and cyberpunks) discovered that 'stealing' money led to their being caught (the old game of 'follow the money'--you have to pick it somehow, somewhere, some day), while stealing information was much more lucrative and virtually untraceable.

The 'Information Age' is more like the 'Wild West' than anything else--there are no 'rules' to break, so it is a 'land' of opportunity. Targets in the West are too susceptible, not just to destruction, but to disruption, spoofing, and passive spying; all systems that technology touches in the West can be considered compromised.

5.0 Conclusions

How to conclude? The problems are there and aren't abating; I can draw conclusions, but there are few solutions. The buzz about information warfare will begin to occur as more and more people become technology savvy; just as with the initial reports of computer viruses and worms, I expect people to slap their forehead and say "I can do that!" By any account, I'm certain they can, and will.

[This article was originally written two years ago. Oddly enough, at the time nobody knew what I was talking about; since then, the topic has been mentioned in The Economist, The Wall Street Journal, and a wide variety of very poor books. I feel even more strongly today than I did then--it is just a matter of time. What I didn't expect was that the capabilities necessary to wage this sortof war would crop up in more than myself and a small group of people I'm familiar with; so much for being egotistical. As the old Chinese proverb goes, *'May you live in interesting times.'*]

Ω

Jim Teff's Magic Elixir

This is a great energy drink, thirst quencher, and general tonic.

For one glass, take approximately. 8 oz. of water and add one tablespoon of apple cider vinegar and one tablespoon honey (adjust to taste). For a 32 Oz. bottle, use 1/3 cup apple cider vinegar, 1/3 cup honey, and fill container with water.

Poor Man's Bota Canteen

This is priced right and holds more liquid than bike bottle. Take one 32 Oz. dishwashing liquid squirt bottle, rinse throughly with hot water several times, then fill with vinegar and let sit for few days to kill soap taste. A carrying strap can be made by taking a piece of paracord, leather thong, shoelace, or similar item tying it around the neck, and making a carrying strap loop with the free end.

Ω

Letters

We'd like to hear from you. Your suggestions, comments, commentary, opinions, feedback, and what-not is always welcome. Send it to:

Cybertek
P.O. Box 64
Brewster, NY 10509
ATTN: Feedback

Dear Thomas:

For years I dreamed of one day walking off, leaving society and living in the forest hiking from towns to camps of disenfranchised Hippies farming and squatting in the forest.

Most of my assets were purchased with the concept of use under a self-reliant campstyle life - with very little interpersonal interactions outside of the romance of inter-commune travel.

This was after the System's failure of course, and this dream was long before satellites and infrared scopes.

I must learn to use the technology of my parasitic foe - ever hungry law makers, because as we saw in Chechnya, the battle no longer belongs to the brave or strong, one must be cunning as well.

Thanks. - J.P.

Welcome to the Blue Oak Republic
founded 25 March 1994 by
Millennium Twain
Post Office Box E
Menlo Park, CA
94026, USA

The Blue Oak Republic is not a territory, nor a government, nor an organization:

It is the recognition of the limitless freedom of individual character and achievement, by an individual.

It is the identification of _infinite_ individual natural and expressed rights of private thought, communication, experience, activity, exploration, creativity, productivity, contract, ownership and enterprise.

It is full acceptance of the private responsibility for ethical integrity -- towards self, family, company, community, and nature.

To make the Blue Oak Republic a reality, just affirm the following Constitution or First Principles:

No harm or coercion will ever be directed by me against any other person or persons, against the property of others, or against nature.

I will always defend against wrongful violence to myself or others or the environment, utilizing all the power within me.

I will never construe the healthy individuality of perosnal character, or the creative activities of community, or the natural growth of industry and economy (in harmony with nature) as violent in any way.

Signed _____

[Please copy, post and distribute]

Ω

Classifieds

Hacking / Phreaking / Cracking / Electronics Information / Viruses / Anarchy / Internet information now available by computer disks, books, manuals or membership. Send $1 for catalog to: **SotMESC, Box 573, Long Beach, MS 39560**

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

CONSULTING SERVICES AVAILABLE: Information and Electronic Security, Disaster Preparedness, Personal Security/Self-Reliance, and Specialized Communications Systems for individuals and businesses. **Reasonable rates** as

Cybertek

THE CYBERPUNK TECHNICAL JOURNAL

Issue 13 - Fall/Winter 1995

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

A "how-to" guide for technology, security, and self-reliance.

IMPK

Hardwar, Softwar, Wetwar: Operational Objectives of Information Warfare

by **Atreides/The Nemesis Group**

Society, a political economy, is about a mechanism I will refer to as the 'value chain.' A value chain is an aggregate infrastructure of processes, best explained by example.

One instance of a value chain comes from Mankind's early days--metal. Based on what ores are readily available in an area, Man has built a variety of implements, starting with rough-hewn rock or wood, moving via the process of discovery and learning to more complex substances--iron, bronze, steel. Years and centuries pass, and the materials, knowledge, and processes that started turning out plowshares now turn out automobiles, airplanes, bridges, skyscrapers. Each step in the process, each advance made, adds just a little more value to the output of the previous step, building vastly more complex systems from the interactions of numerous smaller ones.

Politics is about the ownership and control of the value chain. Western democracies, founded on such contracts as the Declaration of Independence and the Constitution, are based on principles that every individual owns themselves and the fruits of their labour, that they are each entitled to an equal opportunity to be responsible for themselves. Western governments are the tools, the value chain the citizens created to gain an economy of scale--to do those things collectively that are best done so. Among such things is the provision of a common defense, in short, war.

War is a challenge to or from the value chain. Just as the discovery of steel heralded a new wave of conquests against those less developed, war is the competition of value chains. Whether fought with Toledo steel swords, or composite-armour tanks, conventional and unconventional warfare are about attacks on various stages of the material value chain, by methods best suited to the attack on each link. This is 'hardwar'--an obsessive emphasis on the real control of real things, in methods, means, and end objectives.

This approach loses sight of the fact that the material value chain is not the only value chain, and I would venture to say, not the most important one. Value chains stretch back to the beginnings of civilization, by definition in fact. Behaviour is purposeful, directed, and a driving force is needed, a motivation. Maslow worked out a hierarchy of needs that do much to explain the beginnings and evolution of political economies.

Maslow's Hierarchy of Need looks like this:
-- Physiological needs--survival, food, drink, health;
-- Safety needs, physical and emotional needs--clothing, shelter, protection;
-- Affection needs--family, belonging;
-- Esteem needs--self-respect, achievement, appreciation;
-- Self-fulfillment--realization and utilization of one's potential.

Man's Agrarian phase of development, and that shadowy period before, were focused on an almost purely material value chain, because just staying alive, reproduction and metabolism, took all of an individual's time and energy. Even here, however, the roots of another value chain are visible, something I will refer to as the informational value chain, a misnomer as I will point out shortly, but a necessary one for convenience of expression and understanding.

The process of survival was driving the beginnings of discovery, creating language so that such discoveries could be passed on, and education so that they could be made aggregate. Man was learning many things--how to build shelters, when to plant crops, how to mine ores and smelt metals, what plants are edible, the making of weapons, and the strategies and tactics of using them. Necessity is a Mother.

A mixed material-informational value chain existed in the Industrial period, as man had learned how to take his simple tools to make more complex tools, using them to add more and more 'value,' levels of complexity. This complexity forced specialization, and herein lay the foundations of the modern dedicated informational value chain. Obviously, this bifurcation of material and informational value chains is unnatural--in many ways, from our distant perspective, the advances made along the material value chain are purely the result of advances from the informational value chain.

While the process of the material value chain is dependent on the materials it relates to, the informational value chain has a much more (and at the same time, less) clear mechanism, which looks like this:

Data --> Information --> Knowledge --> Wisdom,

where the arrows represent 'transforms or evolves into.' These stages merit some explanation.

Data becomes information through a process of filtering, an exclusion process. In mathematics, this is set theory, where the concepts of 'belonging' and representation open a can of worms. Think of it as finding the needle in the haystack by removing anything that isn't a needle; more generally, the item or items are filtered from the larger body of data. Gregory Bateson called information 'any difference that makes a difference,' and he was quite correct. There are number of 'Smith' or 'Johnson' entries in the (U.S.A.) phonebook, but they aren't all necessarily the one you want to talk to.

The next stage of the informational value chain is information being transformed into knowledge; we have no 'real' understanding of how this occurs in our brains, but it has roots in our abilities to perform analysis, generalization, abstraction, extrapolation, and utilization. These are all functions of the decision-making process.

The final stage is the evolution from knowledge to wisdom, a deeper comprehension of the concepts, systems, relationships, interactions, and integration.

Oddly enough, explanation of the chain points out the problem with calling it an'informational value chain,' just as this is not really the 'Information Age'--society at this stage is actually oriented around data, shuttling it from one point to another, bumping against the constraints of throughput, bandwidth, and interactivity. There is no large scale function, no part of the political economy providing value-add in the process. The reason for this explosive emphasis on data is obviously the computer, and all the things a computer makes possible; the reason for there being no true value-add is that while computers are very good at moving data around, and can even be used in a limited way to filter data, the rest of the value chain is totally unaddressed by the advances in technology (forays into artificial intelligence notwithstanding).

Returning to the application of this thinking to the topic of warfare, conventional warfare is concerned primarily with the material value chain. Attrition-style warfare seeks direct control of the material basics--labour, capital, and resource--while manoeuvre-style warfare focuses on control of the 'key points,' dependencies in the material value chain. Unconventional warfare seeks to overload the material value chain by various methods, whether a nuclear weapon vaporizes large pieces of it, or guerrilla warfare undermines the chain by an 'ontological judo,' using the dis-economies of scale in the value chain against the value chain itself.

For simplicities sake, but following the same line of reasoning, I define information warfare, or 'softwar' as I think of it to avoid the misnomer, as conflict based upon and/or directed at the informational value chain.

Given the preoccupation of advanced political economies with the movement of data from point-to-point, it is no surprise that most thinking about softwar revolves around 'denial of service' (DOS) attacks shutting computers and networks down. There are a number of problems with this--it is very much an artifact of hardwar thinking bleeding over into softwar, it is unsubtle, inelegant, it betrays a lack of understanding of the 'first principles' of warfare, it looks more like a 'scorched earth' policy than any high strategy, and most of all, it misses the forest by looking only at the trees.

In hardwar, the most catastrophic attack that can be made is directed at the very bottom of the value chain; this is why there is a perfectly rational fear of nuclear, biological, and chemical weapons. Softwar is completely reversed--the farther into the value chain any attacks are made, the more leveraged they are, the less 'force' required, just as with the differences between attrition- and manoeuvre-style warfare. Clearly, a more detailed explanation of the relationship between an informational value chain and softwar is called for.

The existence of a deep informational value chain is, in many ways, the defining characteristic of an advanced civilization. This very existence is the first element available in softwar--just as steel won out over iron, having satellites beats not having them, and electronic communication beats a horse-borne messenger (figuratively).

The next stepping-stone to softwar is intelligence, in the espionage sense of the term; intel is largely a function of the collection of massive amounts of data, and then filtering that deluge. As far back as the dawn of Man, intel was a function of softwar, which comes as no surprise to anyone, least of all people such as Sun Tzu. Knowing its place in the value chain helps to explain many of the dilemmas of the intelligence community:

-- The escalating need and dependence on electronic collection of data countered with the information overload disaster;
-- The inability to keep pace with the increasing load of dynamic data;
-- The problem of electronic intelligence (ELINT) missing subtleties of motive, intent, and other nuance that human intelligence (HUMINT) used to provide;
-- The inherent flaw of the intelligence process remaining unbiased--the transformation of data into information automatically calls in to play a paradigm, interpretation, judgment, prioritization; this bias is amplified and exaggerated in the process of augmentation.

Softwar attacks on the civilian value chain infrastructure actually look more like hardwar attacks. Denial of service (DOS) attacks can range across the value chain, effecting the contributory infrastructure and social contract the way terrorism does. There are common elements, obvious from the assessment that the current phase of social development is only that of a data-based society--attacks will be on the electronic transport layer we think of as communications, and the control mechanisms we generally rely on as the 'societal glue.' An important note is that DOS attacks on civilian entities can't go farther up the value chain because there is no chain there to target. Military DOS attacks are focused on many of the same elements of command and control; this leads to the conclusion that civilian attacks are likely only to be collateral consequences from military objectives. The fear that such attacks will occur is well justified--after all, the techniques used by guerrillas and terrorists worldwide already map into this new domain. Whether they work is another things altogether--much of the low end of the military informational value chain is already hardened, a by-product of the nuclear

age. Satellites have always been assumed to be 'expendable,' and military command-and-control has been a target in millennia of warfare--capture of a commander in a hierarchical structure is more effective than trying to grind down troops, and while a heterarchy would better withstand attacks, no certain blow could be struck. This sort of softwar attack is survivable, correctable, and will cost a great deal in damages, but much like Pearl Harbor in World War II, it is likely to only infuriate the citizenry of the targeted political economy.

More subtle methods of DOS attacks may be effective, however. Historically, when analysis and decision-making power were seated in the same person, these were worthwhile targets; in modern times however, most politicians are totally orthogonal to the informational value chain, providing no value add themselves. The tools in place to provide such value add are, however, directly susceptible to such attack, and in many cases aren't even protected.

Assume for example that an Adversary planned a conflict and wanted to impair thedecision-making abilities of a powerful, advanced ally of their target. Are attacks on orbiting satellites that provide data on their region even possible, let alone cost effective? Unlikely. A little leverage brought to bear, however, can answer that problem. Imagine this chain of events:

-- A set of video cameras are placed so that they collect data, the license plates of vehicles going into the 'hostile' intelligence agency;
-- Data is continually collected and processed;
-- The license plates are checked for in a variety of databases to provide the name and any other data on the owner and likely driver;
-- The driver's credit and personal data is pulled, as well as any other information that can be checked from the ever-growing number of databases;
-- Based on the data derived, a structural map of the organization is developed, founded on such things as salary levels, education level, specialty, et al;
-- Certain functions are targeted, such as analysis sections or skill bases, such as knowledge of the Adversary's region or language;
-- Just prior to hostilities, such individuals are targeted for either subversion or elimination.

This sort of DOS attack is directly targeted at the deeper levels on the informational value chain--those with knowledge or wisdom about the region and Adversary. It has many benefits besides being cheap, direct, and leveraged; it leaves the political players 'in the game,' but without any way to makes sense of the overwhelming levels of data generated prior to or during a conflict. Because of the common mechanism of reliance by the military on politicians to set objectives, any coherent military response by the targeted country is also hamstrung. It takes no great sophistication to carry out exactly this sort of attack, but the impact, particularly the transformation of the political structure into one of 'value subtracted,' is considerable. Recovery from such an attack is a matter of luck in making all the right choices in the time period it takes to rebuild the lost functionality, an unknown period, but far longer than rebooting a computer and reinstalling software as after a DOS hardwar attack.

A true softwar attack is one of covert perversion, best thought of in terms of a military adage--war is deception. People make decisions based on their cognitive environment, their infosphere; control of the data comprising such an environment allows a certain amount of control over those in it. The drawback of course is that the better the information of the opponent about their infosphere, the closer the deception must be to the reality provided by the environment. Very much a situation of Garbage In, Garbage Out (GIGO), this sort of attack is about the use of lies and mis/disinformation to produce very real results. It can be very direct, and successful when so--surrendering when you only think you are surrounded but aren't, inflatable tanks and airplane skeletons to misdirect thinking regarding the time and place of an attack, or an impossible-to-implement missile defense system that leads a believing opponent to spend itself into collapse. Such attacks will become more prevalent and subtle when direct control of data channels is possible; the double-edged sword of the media can be grasped more directly than was CNN by the West during the Gulf War, and to much better effect, but care must be taken to avoid the sapping of will that occurred during the Viet Nam conflict.

Viet Nam, besides teaching a host of lessons in conventional warfare, guerrilla warfare, hardwar, and softwar, was also a masterful piece of the 'high end' of softwar--'wetwar,' the battle for will and mindshare.

Wetwar, derived from the concept of 'wetware,' the hardware/software of the human mind, is war conducted entirely through subtle, mainly non-violent means, to control the deepest end of the informational value chain--an insidious form of propaganda directed at will, support, and perception of data. Viet Nam is a case study of intentional and unintentional wetwar, with brainwashing, confessions by POWs, media bias in the data --> information link, GIs televised coming home in body bags, Hanoi Jane, winning yet losing the Tet offensive, bombing campaigns that drove neutral civilians to join the alternative and hostile infrastructure set up and controlled by the wily opponent, et al. This form of warfare is the pinnacle of skill, where your opponent defeats himself, and then writes you a bank draft and says he was sorry.

Information warfare, whatever its form--hardwar, softwar, or wetwar--is simple and complex, subtle and obvious, a product of an advanced civilization yet oddly echoed in ancient Sun Tzu, part of the past and a still-unrealized future. It can no more be dismissed than any other form of war; not to prepare for it is the act of a fool, yet it is difficult to prepare for. Focusing on one small area, such as DOS attacks, leads to errors just as the idea of attrition and air superiority did in Viet Nam--control of one part of an infrastructure or value chain is like trying to control a puppet with only one string. Understanding information warfare is very much a search for an understanding of conflict and progress, Aquinas' concept of a return to the first principles. You can go so far down the path, only to find yourself back at the very beginning.

"In battle there are not more than two methods of attack--the direct and indirect; yet these two in combination give rise to an endless series of maneuvers. The direct and indirect lead on to each other in turn. It is like moving in a circle--you never come to an end. Who can exhaust the possibilities of their combination?" -- Sun Tzu

Ω

Decoding Touch Tones

by **Thomas Icom**

Doing this is relatively simple for everyone except all those individuals on Usenet who keep asking about it. This ought to set everyone straight. Decoding DTMF (Dual Tone Multi Frequency: what everybody outside of Ma Bell calls Touch Tones, as "Touch Tone" is a trademark of Western Electric, one of Ma Bell's children.) is simply a matter of having access to a DTMF decoder. These can be purchased in various levels of sophistication, built, or "borrowed".

Starting with the simple first, I'll talk about "borrowing" a DTMF decoder. If you have a pager, you can borrow one of the pager company's. Record the Touch Tones you wish to decode, call your pager, and play the tape into the phone. When you get paged, the numbers on your pager will be the DTMF sequence. You can do the same with certain VMBs. When you call a VMB, enter in a bogus DTMF sequence and see if it'll tell you "NNNN is not a valid mailbox.". If it responds with the sequence you'd entered, you can use that to decode unknown DTMF sequences.

Those of you with a Soundblaster/AbLib card in their PC can try one of the programs that turns your sound card into a DTMF decoder. There are a few such programs floating around on BBSes and FTP sites. The RuneStone BBS (official Cybertek support BBS 203-832-8441, NUP: Cyberdeck) also has Soundblaster DTMF decoder software available for downloading. I experimented with a few pieces of software and wasn't impressed; as all of the one's I tested were prone to falsing and lacking somewhat in sensitivity. A PC also lacks portability for real-time decoding in the field. .Since they are available for free however, you might want to try what you can find and see if it works for what you need it for. One point which you should be aware of is that some of the programs available require a "real" Soundblaster. If you have a clone they won't work.

For those of you who can solder, DTMF decoder ICs are sold for less than $10. They can be interfaced to a PC and work well. Full DTMF decoder kits are also available for less than the finished product. There have been hundreds of DTMF decoder schematics published and released into electronic domain (some are on the 'Stone) over the years. If you're going the do-it-yourself route, avoid plans that are more than a few years old. New ICs are constantly being developed which cost less, and are more reliable.

Schematics which you should avoid at any cost are ones which implement the 567 Tone Decoder IC. While it was a nice chip in it's time; by today's standards it takes too long to get a good lock and is too prone to falsing. A DTMF decoder implementation using this chip is also 10 times the size of more modern designs, as a total of eight 567 chips are used to do the job that one chip can do today.

One that is readily available appears on page 169 of Paul Bergsman's excellent and highly recommended book **Controlling the World With Your PC**. I acquired my copy at my local Barnes & Noble, or you can get it from **HighText, P.O. Box 1489, Solana Beach, CA 92075**. Paul's book is the bible for real-world interfacing for the PC.

Another set of recently published DTMF decoder plans can be found in the September 1995 Issue of **Nuts & Volts** magazine. These plans use a California Micro Devices CM8880 IC and a BASIC Stamp. A kit based on this project is available for $22 (not including the BASIC Stamp and LCD Serial Backpack used for the display) from:

Scott Edwards Electronics
964 Cactus Lane
Sierra Vista, AZ 85635
520-459-4802
FAX 520-459-0623
72037,2612@compuserve.com

Finally, one can go and buy a completed DTMF decoder. The assembled units start at less than $60, and used equipment can be had for even less at Hamfests. Starting at the bargain basement we have:

Motron Electronics
310 Garfield St., Suite 4
P.O. Box 2748
Eugene, OR 97402
800-338-9058, 503-687-2118
motron.info@emerald.com

Their TDD-8X DTMF decoder is $59. It features an 8 digit display, 104 character memory, and serial port for connection to a PC. For DNR work in those backwoods areas that have yet to receive DTMF service, Motron has the TM-16A which will also decode rotary dialing for $179. With the RS-232 port option the price of that unit goes up to $249. For those of you who have remote control

applications in mind, for $99 Motron sells their AK-16 DTMF Controller Board. It features 16 relay driver outputs, up to 12 digit security code capability, ASCII serial output of incoming DTMF tones, and DTMF user-programmability.

For those looking for a nice looking "Rolls Royce" type unit in order to impress their next TSCM client, you have two choices:

Optoelectronics
5821 NE 14th Avenue
Ft. Lauderdale, FL 33334
800,327-5912, 305-771-2050

Universal Radio
6830 Americana Pkwy.
Reynoldsburg, OH 43068
800,431-3939, 614-866-4267

Universal sells (for $399.95 + $6 s/h) their M-400 decoder. This unit decodes DTMF; as well as POCSAG, GOLAY (pager modes), CTCSS (PL), DCS (DPL) (tone codes which are used to access radio repeaters and prevent interference), and whole bunch of other digital communications modes used on the shortwave and ham bands.

Optoelectronics also sells a similar unit, their DC440. This unit is only $259, and only decodes DTMF, CTCSS, and DCS. It has a 127 character memory and interface to a PC when mated with a CI-V to RS-232 converter. If you don't need all the extras the Universal unit has and want something that'll interface with a PC, go with the Opto' unit.

Ω

Backyard Pyrotechnics I

by **Pyronomy**

The following series of articles will give details on how pyrotechnic devices might be constructed. It is my intent that the descriptions given are for informational purposes only. WARNING: THE FOLLOWING MATERIAL DEALS WITH PYROTECHNIC DEVICES THAT CAN BE HAZARDOUS. SO PLEASE USE CAUTION:

I think that it would be prudent to explain the difference between pyrotechnics and explosives. Explosives are broken down into several categories. Low order explosives are things like gunpowder, flash powder, black powder, etc. They tend to burn rapidly or deflagrate. There power as explosives usually comes from the bursting of the container that they are in. High order explosives are things such as dynamite, plastic explosives, nitroglycerin, etc. They work under a different principle called detonation. Detonation in the most basic terms is the rapid, self-propagating decomposition of an explosive accompanied by a high pressure-temperature shockwave that moves at 1000-9000 meters per second. This is not generally considered in the chemistry world as burning. Primary or initiating explosives are the last class. Some of these are mercury fulminate, lead azide, etc. These can be sensitive to either shock or burning or both. They generally are more powerful than low explosives and produce a shock wave that is used to detonate high explosives. The only class that we will be dealing with in this series are the low order explosives.

Pyrotechnics are an art form that has a history thousands of years old. They are constructed for the purpose of providing exciting displays for groups of people large and small. They existed even before anyone conceived the idea of using black powder to hurt their enemies. Explosives on the other hand generally are used to do some type of work. Be it in war or in peace they generally have a tendency to destroy. If this is your purpose then this article isn't for you. Most pyrotechnic devices are explosive in some way and are therefore listed as explosives. Usually this is necessary for the devices to achieve the desired effect. I will cover devices that are intended to make pleasing displays be it on the ground or in the air. If you want to play with the big boys go join the army.

At this time I would like to say a little something about this outrage in Oklahoma. McVeigh, or whoever is guilty, I hope they give you to the families of the ones you murdered YOU PIECE OF DUNG. While I am on the subject what is this bullshit the press is doing to the Militias. I've never seen such a load in my life. Several slimes do something horrible and the press goes and stereotypes a whole class of people without any investigation to see what kind of people they really are. Well if you are reading this you obviously don't believe anything that those jerks say anyway. What was the purpose of this bombing anyway? Are we supposed to be impressed with this chicken shit attack? You didn't even have the balls to be there. What are you pissed about Waco? Hell I didn't like it either but I wouldn't kill someone because of it. Lets just pull the plug on you and be done with it because you obviously don't have a clue.

Anyway it's a shame that this happened because it has side effects that some people are not aware of. For one thing those people that find the main theme of this article interesting and might want to try working with fireworks will soon find it harder to get some of the things that they might need. The laws will probably get a lot tougher on anyone that might construct anything that someone else who is either nosy, stupid, or misinformed might think is a danger to society. They might even see the required reading material disappear. I don't know about you but it bothers me a hell of a lot.

I don't want anyone to have the false impression that I am all knowledgeable on this subject. For me it is a hobby that I happen to cherish with a very large passion. There will be some suggestions later on some reading material that will help.

WARNING: THESE DEVICES CAN BE DANGEROUS POSSIBLY FATAL SO BE CAREFUL. Safety is the key to successful and pleasing pyrotechnic displays. Therefore we are going to discuss safety now and throughout this series of articles.

Some of the DO's and DON'Ts

NO SMOKING: This means while handling chemicals or when constructing, firing, and transporting devices.

Be gentle when handling your devices as some can be sensitive to rough handling. You can't be too careful when involved with a hobby like this one.

The first thing you should do before constructing any devices is to check the laws wherever you are to find out if it is legal. There are several different classes of explosives that have been designated by the Dept. of Transportation. Pyrotechnic devices like the common firecracker, bottle rockets, those little pieces of junk that just burn on the ground with merely a whimper and party poppers are in Class C. The smaller sized paper tube launched aerial shells that go up a couple of hundred feet then burst are also Class C. Some states sub-divide this class into sparklers and ground devices that shoot sparks. Some are even so lame as to have everything banned. There is also Class B. This is where most of the big professional displays reside. These are probably familiar to everyone who has lived through one Fourth of July. They consist mainly of a round that is launched from a metal tube and burst high in the air. I'm not exactly sure what the boundary is between Class B and C. The largest aerial shells that I have seen on sale in fireworks stands was 2 1/4" in diameter and was marked Class C. Most of the aerial devices that we will be discussing will be higher than normal altitude Class C.

OK back to safety. Do not fire any devices on public property as it is dangerous and probably not legal. The author assumes no liability for damage or injuries caused by the use of this information. Okay enough so here is the list of minimum safety equipment needed.

SAFETY EQUIPMENT NEEDED	**WHERE TO GET IT**
Face Shield	Hardware Store
Breathing Mask	"
Thick Latex Gloves	"
Welding Gloves	Welding Supply
Welding Arm Shields	"
Leather Shoes	

The equipment listed should be used anytime you are mixing your chemicals or when constructing devices. I know they are cumbersome but it is better to be safe than sorry. Especially the shoes.(Blackmatch will burn through house slippers. I know this from personal experience.)

Credits

It would be wrong for me to continue without giving credit to the individuals from whom I acquired the basic information that I am about to impart to you. The first is the fantastic series of books by Kurt Saxon entitled The Poor Mans James Bond. There are four books in the series covering every possible area of self reliance. All contain numerous how-to manuals from A to Z. You want to know, it's in there. Another one is Granddad's Wonderful Book of Chemistry. It contains everything that you would want to know about laboratories and chemical processes. Another series written by Mr. Saxon is The Survivor. This series is jam packed with how-to articles that are on every subject that you could possibly want. I would highly suggest all of these books as they are very valuable. The best ones as far as pyrotechnics are concerned are Granddad's, PMJB I and PMJB II. In PMJB I you will find Fireworks & Explosives Like Granddad Used To Make which is a group of articles including Scientific American 1903, Dick's Encyclopedia of Formulas & Processes 1872, The Techno-Chemical Receipt Book 1896, and Henley's Twentieth Century Formulas 1907. It also contains Pyrotechny by George Weingart (1947). It is considered by most to be the authority on pyrotechnics. The last one is American Pyrotechnist by VanderHorck. It contains articles by numerous authors about constructing mechanical devices used in the manufacture of pyrotechnic devices. In PMJB II you will find a reprint of Tenney Davis's book The Chemistry of Powder and Explosives published in 1943. It is modern and has done away with most of the older terms used for some of the chemicals used. However it is a very good idea to have Granddad's around as it does explain the older terms. I would like to express my gratitude to Kurt for the vast effort he has put into this series. It is well rounded and will provide a great many hours of pleasurable reading. THANKS KURT. would also like to suggest getting a chemical dictionary or maybe borrow one and check certain aspects of the chemicals that are used in pyrotechnics. You should especially check the sections on hazards, properties, and usage.

I would like also to thank Stormbringer in D.C. (BBURPP) for turning me on to PMJB and for the inspiration. Asrael (OOPS Sorry bout them tax records Dad) Asphyxia also for the inspiration. Hey AZ be careful with that Perchlorate. And last but not least Thomas Icom for the opportunity to pen this series.

Materials

The hardest part of it all is acquiring the materials unless you have an unlimited budget which I think most folks don't. So I am going to give you some hints on how to construct some of the things that will be needed.

Scales are a must if you want your compositions to be consistent. All of the compositions used are given by weight proportions. A cheap set of proportion scales are to be described. You will need the following:

Wood appox. 18"x 4"x 1/2"

Plastic/Vinyl strip 12" long and as thin as you can get it (I used a piece of 1" vinyl window blind)

Wire appox. 4" long and fairly stiff 10-14 ga. (I used brass brazing wire)

Bend the wire in a U shape 3/4" in from each end. Make two holes in the wood slightly smaller than the wire. The holes should be placed so that the wire is in the middle length-wise and perpendicular to the length and 1/4" deep. The wire should be inserted so it is no more than 1/2" off the board. Put a slot in the plastic so that it will balance on the wire. Add a small container shaped like a scoop at one end of the strip by using a 2" piece of plastic drinking straw and duct tape. On the opposite side of the strip using a small piece of tape attach a dime about half way between the wire and the end. This will allow you to weigh out fairly small equal amounts of the chemicals.

The scales are used in the following manner. Place something under the scoop to catch any chemicals that might not make it into the scoop. Place your chemical in the scoop until it is just heavy enough to tip the scoop down all the way. This is one proportion that weighs somewhere around half a dime. It doesn't really matter how much as all the formulas are given as parts by weight proportion. Any way you go about it is okay as long as you make sure that the weights are consistent.

Chemicals

CAUTION: ALL OF THE CHEMICALS BEING USED ARE EITHER POISONOUS OR DANGEROUS IN SOME WAY. PLEASE USE SAFETY PRECAUTIONS WHEN HANDLING THEM:

The formulas that are used will only be tested possibly modified versions of ones found in the various sources that have already been mentioned. No formulas will be given that have not been personally tested to ensure some measure of safety and consistency. There are several categories of chemicals that are used. Oxidizers and reducers are the most important as far as the actual burning of compositions. Binders tend to hold the compositions together physically and also have the tendency to moderate the burn rates. Some also have the tendency toward being combustible.

Oxidizers do just what their name implies by providing oxygen to sustain the burning. We will get into more detail on the actual terms at a later time when we start to get into the section on constructing stars and such as that. Some are listed here:

Potassium Nitrate is the oxidizer that is used in Black Powder. It is used in numerous compositions that contain a carbon based reducer. It should be obtained from the chemical supply house.

Potassium Perchlorate is a lot more powerful oxidizer than the nitrate as it contains more oxygen. Like the other chemical compounds made from chloric or perchloric acids it can be rather sensitive in certain circumstances. Such as when mixed with finely divided metals such as aluminum or copper. It also gives up chlorine which helps to deepen the color of your fire. It can be obtained from the supply house. Note that it also is more sensitive to shock when mixed with sulfur and may be set off when struck real hard with a hammer. It is a strong irritant.

If you have an excess of bravery one of the most powerful oxidizers is Potassium Chlorate. If you decide to use it get all the PMJB books and read them from cover to cover many times to make damn sure you know exactly what you are doing. It has a tendency to spontaneously explode when mixed dry with certain things such as sulfur and red phosphorus and should be wetted thoroughly including an antiacid before handling. Thanks for that note Kurt.

Another rather powerful but hazardous oxidizer is readily available as of this writing is Potassium Permanganate. It is generally a purple colored granular substance that grinds up into a reddish purple powder. Be aware that it is very caustic and will burn skin on contact. It is very sensitive when mixed with reducing agents and when mixed with powdered aluminum it is as powerful and maybe even a little stronger than the flash powder described further on in this article.

Barium Nitrate (used for green fire) is a good oxidizer and also helps color the flame green. It also comes from the supply house. Most Barium compounds are poisonous so caution is important. Make sure that you wear your mask and gloves when using this in a well ventilated area.

Strontium Nitrate (used for red fire) colors the flame red and also provides oxygen. If you have access to a 100-200 mesh screen it may be obtained from common road flares. But be aware that most contain binders such as kerosene which could possibly cause problems. It is best to buy it from the supply house. Most Strontium compounds also tend to be hazardous in some way or other. They are usually poisonous and should be treated with caution. They are shock sensitive when mixed with reducing agents.

Ammonium Perchlorate is also a powerful oxidizer that is available and is mainly used in rocket engines. I have not used it yet but have acquired some for testing purposes and will let you know what I find out.

Reducers on the other hand are in the simplest terms what gets burned. I know that some will find that too simple a description but its easy to understand. Some are listed below.

Charcoal can be found at the hardware store but contains a lot of trash in it so it is recommended that you spend the bucks and buy soft charcoal sticks at the art store. These can be ground up real easily and are my first choice.

Powdered Aluminum can be obtained through a chemical supply house or if you're into chemistry made at home, but I bought it. NOTE: Filed aluminum doesn't work well unless it is very fine. Do not use sandpaper to make it small as it will contain many particles from the paper and could taint the quality. Be aware that most finely powdered metals can be explosive when mixed with oxygen. Some also can be toxic in this form.

Zinc Dust is another metal that can be used in the arts. It may be obtained from the supply house in a couple of forms. In bits and pieces, in a powdered form, and in a powdered form called mossy. This means that it was powdered by pouring molten zinc into water. The form I have acquired is the regular powder.

Sulfur has the main job of evenly spreading fire to all parts of the composition in which it is incorporated. It also acts as a reducer by being combustible. It is best obtained from the supply house.

Binders can have multiple purposes when included in some compositions. They hold things together and sometimes act as reducers. These will be described individually.

Shellac is a good binder when wetted with ethyl alcohol. It also is combustible so tends to act as a reducer.

Stearine is a binder and a reducer at the same time. It is sold at the hobby store for use in candles. It is sometimes used in making blue fire.

Another binder is powdered water soluble things such as dextrin but I have as yet been unable to find a source. IF you find one please pass it along. I am in the process of trying a couple of ideas along this line and will let you know what I find.

You will also need a couple of wetting agents to suspend your binding agents so they will be evenly distributed within the compositions. Isopropyl alcohol (rubbing alcohol) is used in certain cases that will be mentioned later. Ethyl alcohol to be used when shellac is being used in a composition. Denatured Alcohol can also be used if it is the kind that has been denatured by methanol only. It should not contain any other denaturants. Water is used when dealing with some of the Nitrate and Perchlorate composition and will be noted at that time. Never mix any Chlorate compositions dry as they tend to go BOOM.

Cannon Fuse can be found at gun shops and gun shows. It may also be found at your better hobby shops that carry model rocketry supplies. Make sure to test the fuses burn rate.

Other chemicals are also needed for special purposes such as Ammonium Chloride which is used as a source of chlorine in the burning to help in deepening the color. It is also used in making a pretty good white smoke. Be aware that it has the tendency to draw moisture from the air.

Mercurous Chloride (Calomel) is also a good chlorine source but be advised that it produces poisonous fumes especially when burning and should be used only where there is extremely good ventilation. It is used primarily in the making of blue and green fire. It does not seem to take up moisture from the air like Ammonium Chloride and is preferred over it. Generally when chlorates or perchlorates are used for an oxidizer there is no need to add any extra chlorine source. This compound in any form is very poisonous.

Black Powder is available at most gun shops that cater to muzzle loading enthusiasts. It comes mainly segregated by grain size. 2F is the size that I have found to be the most useful. It can be carefully ground in small amounts with a porcelain mortar and pestle if the need arises.

I have touched only the tip of the iceberg here so please refer to PMJB for a complete list of what will be needed.

Black Match

Black match is a type of fuse used in certain ground and aerial devices. It is also very cheap and easy to make. You will need cotton twine and some finely ground Black Powder(BP). You will also need some kind of frame to stretch the fuse over to allow it to dry. Take 3 strands of the string and twist together then tie to one side of the frame. Twist the strands then tie tightly to the other side of the frame. Take a shallow container and put some BP in it. Add water 1 drop at a time mixing constantly with a wooden stick. Continue adding water until the BP is a thick paste. While wearing rubber gloves completely saturate the string with this paste. Wipe off any excess and allow to dry completely. This fuse burns at about 1" per second. It can be made to burn very fast by inserting it into a paper tube about 1/4" in diameter. This is called Quick Match and burns faster than you could possibly get away from so be careful when using it. The Black Match is also a lot cheaper than Cannon Fuse and is sufficient for use when testing compositions.

Flash Powder

Flash powder is a mixture of Potassium Perchlorate and the finest powdered Aluminum that can be acquired. 400 mesh works real well. You would be wise to wear a particle mask, face shield and rubber gloves for measuring your chemicals and also welding gloves when mixing them, just in case. Also it would be wise to do so when making devices. Measure 2 parts Perchlorate and 1 part Aluminum. Combine them on a piece of aluminum foil and gently mix together thoroughly with a plastic measuring spoon. Store in a plastic bottle. ** DO NOT STORE IN PLASTIC BAGS ** This composition is not real sensitive to static like Black Powder is but has been set off by static under test conditions so use caution when choosing your containers. This composition if placed in a test cup made from aluminum foil that is 1" in diameter and 3/4" deep to a depth of 1/4" and fired with enough cannon fuse to allow time for departure flashes, makes an audible poof and makes lots of white smoke. If loaded to a depth of about 5/8" you get one helluva boom, a big flash, and enough smoke to be seen from a long way off. The first time that I did this it scared the bejeezes out of me. I was not aware that any of the low order explosives would do this in that small an amount and under those conditions. Obviously I had failed to

take into account the speed in which this stuff burns. When tightly contained it can build up pressure fast. I urge extreme caution when using this composition.

First Device

Now lets start the construction of a small firecracker that is approximately M-80 grade maybe even a little better. Be advised that this device can remove a hand. It is best to place it on the ground standing straight up so that the end plugs won't bean someone on the head or something like that.

Take a thick walled paper tube (fax paper roll or home made) about 5/8" in diameter and 2" long. The walls of the tube should be a least 1/8" thick. Make a wadding with toilet paper (TP) by inserting one wadded up sheet in the tube and packing tightly against a hard surface with a cylinder that will just fit the tube. Eject it from the tube then make another. Insert one of these into the tube leaving 1/4" space between it and the end of the tube. Fill this space with a quick drying two part epoxy cement and let it cure completely. Take a sharp pointed round object and make a hole in the middle of the side of the tube that will fit the fuse very tightly. Insert at the minimum 6 seconds worth of fuse into the hole until it turns toward either end. If you made the hole correctly the fuse should be rather hard to remove. If not use some Elmer's glue around the base of the fuse to hold it in firmly. Once again let it dry completely. Now stand the tube on end and add flash powder until 1/3 of the containers interior is covered.(Another alternative is to fill it completely and pack lightly using the end plug. I am still experimenting to find the right amount so be careful when trying this.) Insert a piece of wadded up TP in the tube and lightly pack just enough to hold the powder together leaving room for the other wadding that you made. Now insert the wadding and epoxy as before once again allowing to dry completely. You now have a device that I hope you enjoy. I put one of these under a 55 gallon plastic trash can that was inverted on concrete and it went 10' into the air. This device throws a very hard wadding so watch out.

Sources

Poor Mans James Bond, Granddad's, & The Survivor available from:
Atlan Formularies
P.O.Box 95
Alpena, AR 72611
(501) 437-2999

Ω

Notes From Ground Zero

by **Wildflower**

Buying tools can be a real pain if the tool you paid for turns out to fail after a short while, usually at a critical time & place; opening oneself to frustration, possible injury, even death! Too many of today's tools are really mass-produced crap, especially those sold at "bargain prices".

Take for example VISEGRIP (tm) pliers, which have numerous imitations on the open market.Now the real Visegrip pliers will last for many years of heavy duty jobbing, while the five dollar copies last only a few hours, if lucky, before failing. Yet despite such failures have seen people just buy another copy tool, rather than the real thing, just to "save money". Sheesh!

Now, not all cheap tools are bad, such as some tools coming out of China which are of good quality at a low price, but buyer beware. This is a rare item nowadays! It's best to compare the quality of the more expensive tool against its cheaper version to be certain of its quality before wasting your good money.

As for power tools, if can afford to do so buy the "industrial" types, for they are built to last for a long, long time, and are easier to repair and maintain than their more inexpensive versions. HINT: Buy the replacement brush sets and replacement bearings within the same year of purchase or the power tool for easier servicing later.

LAST: Do remember to wear appropriate goggles, gloves, ear protection, etc.; as no one has perfected spare eyes, ear drums, and fingers for the first aid kit yet! Only a fool refuses, until they are a dead fool. Such protection is easy to use anytime and anywhere!

THE POCKET PORTABLE SHOP: Recently acquired the RECHARGABLE DREMEL CORDLESS ROTARY TOLL ("MINIMITE": MODEL 750) which uses a rechargable power pack (recharges in 3 hours). With a dual speed of 5000 RPM (Slow)/10,000 RMP (Fast); this tool can utilize most of the various minibits to carve, shape, drill, cut, etc. light wood to light metals. (COST: about $30 (spare pack $20) at most hobby shops)

The MINIMITE, with spare pack and recharger can fit an M-65 coat pocket; along with a small variety of minibits. Ideal for many "in the field" jobs as well as at home. Also makes a great "beginners" tool for many "first workshops".

For better "UMP!"; consider one of the more powerful DREMEL ROTARY TOOLS, which can be used in the field if powered by an inverter off your 12V battery pack or system. Also of note is the saw, flexible tool shaft, and even drill press adapters for your DREMEL TOOL.

The PARASOL BUTANE TOOL : (Sold at Radio Shack) can be recharged with fresh butane at home or in the field, comes with interchangable tips for: SOLDERING, HOT KNIFE, TORCH, or even a HOT BLOWER for softening plastics or peeling hard paints. Comes equipped with a cap containing a flint igniter. This portable tool is most useful at remote sites that have no power outlets for conventionally powered soldering irons, etc. *NOTE* This tool may clog up on cheap butane refillers, also tends to wear out fast, especially on "most used" tips.

VISEGRIP BRAND TOOLS: Avoid initations, for few ever last as long as the real thing! The real thing, from the mini 4WR Visegrip pliers to the other types including clamps and pipe wrenches; may damn well cost more than the imitation copy, but will never fail on the most critical job, like so many imitations have done so. *NOTE* The small 4 to 5 WR Visegrip pliers are not only excellent pocket tools, but can also serve as "adjustable thumbscrews", even for emergency dentristry; as in pulling teeth! For most field kits, buy two of each size.

As unusual weather keeps occuring, do be certain to establish a cache of canned foods now, as uncertain of national production which may drop this year as additional extremes/dangerous stroms/drought take their toll on the nation's food production areas. Even a can of beans is far better fare than a floppy disk any day! Also far cheaper to buy know, than if food becomes short. Prices will definitely rise quickly, amking that can of beans cost more than a brand new 486 chip, if not the entire board.

Also consider other prices to rise on medicine, clothing, ammo, ectra. Gold and silver may buy even less than what you can buy it with later on. So, why be caught "short"? Also such items can command even higher "barter trade value" later on, comprehendee?

During the last big way (WW II), savvy people buried extra fuel in one gallon cans under their rose bushes, even under their flower beds! Consider at least 10 gallons of auto fuel concealed underground nearby for "emergency travel needs" as a wise investment. Consider burial in two to five gallon plastic fuel containers, with fuel stabilizer added, under your rose bush! If you really got room, consider a plastic 55 gallon drum or two under that old rose bush, especially if you're going to stay.

Now past the fall of it all, one could tap gas station fuel tanks for fuel, especially if one has a manual operated diaphram water pump from a sailboat. These pumps can even pick up the last few inches of fuel left at the bottom of the fuel tank (do filter afterwards). Another option is those electric auto fuel pumps that mount directly into a fuel tank, but take care to seal all completely against accidental spark ignition of tank fumes.

Also, don't forget to check abandoned cars and trucks for fuel, as many still have a filterable gallon or two left in their tanks for salvage (even if gauge reads empty). The easiest way to recover such fuel is to crawl under and penetrate tank with a sharp awl & mallet, but be damn careful not to generate sparks while doing so. Far better to siphon with a hose connected to an electric or manual fuel pump. If auto is compatable to yours, take the time to strip useful parts; including usable tires, working lights, generator and battery. or at least notre location on map for later salvaging when possible.

Any automobile is a "treasure chest" of reusable materials for the home shop to utilize. No doubt as one's new local civilization starts to rise, even garbage dumps will be mined for useful metals, wood, plastics, etc.; rather than trying to find natural raw materials elsewhere. And be damn certain, most products exchanged, will be rebuilt or newly manufcatured to be "rerpairable, recyclable, reusable" instead of the more traditional "use it once & discard" mentality of now!

As for lifestyles, one will not be so easy to escape by using the automobile to distance oneself between work & home. People will have to realisticly deal with each other, or face real expulsion, for such beliefs as racist, sexist, even moral; from their community. In other words "GET ALONG OR GET OUT!", and for those who believe in murder, rape or even violence, live damn short times when caught in any community about.

BASICLY: One has to be prepared to be "the meanest S.O.B." so that one could "live long at peace"; while tolerating each other, and giving those who want peace the means to do so. Otherwise one will be exploited, raped, and killed by the most sadistical bunch of bastards about, for they can only tolerate you as dead, period!

Checklist For Survival

1) Stay in good shape and stay healthy.
2) Have lots of friends.
3) Have a good solid house or building to live in, possibly even for future generations to add to; with good solid construction of thick walls and roof; along with access to good well water from inside; be able to withstand local hordes of shitheads.
4) Good land, or nearby access to; for food production.
5) Good water well or good storage of water, along with good filters.
6) A very good, extra large capacity sewage storage tank or leech field, constructed away from contaminating possible safe water areas.
7) A shop equipped with good hand tools.
8) Kitchen with hand powered grinders, wood stove, icebox, manual can opener, etc.
9) Alternative means of power and fuel production in use, or in storage awaiting future needs.
10) A good multiband radio and CB radio.
11) If armed with firearms, reloader and supplies.
12) A good first aid to surgicalkit, with extra supplies.
13) A good reference library of books.
14) A good "mountrail" bicycle, spare tires and parts.
15) A good inflatable raft, small boat, or "daysailor" sail boat (with a small gas outboard with extra fuel & spare parts)

16) Extra seeds, fertilizer, also a good soil test kit.
17) Good kerosene lanterns& extra wicks & fuel.
18) Have already established a one to five year "use and replace" rotational supply of clothing, foods, medicines, etc. In case of a real emergency, this becomes your "reserves" until replacements can be found or grown, which could be a very long time 'til so!
19) Impossible to store everything,so store what cannot be easily made to combine later with what can. For example: transistors vs. a radio coil.
20) A good sense of humor, a good ability to make do with what one has and to do without one has not, a good solid belief in no matter what comes, you can deal with it one day at a time.

Live Long & Free!
Wildflower*95

Ω

The Riddle Of Steel

by Jim Teff

The Value Of Lo-Tek

In a survival/guerrilla warfare/self-sufficient situation ammo and parts will be in short supply and difficult to come by. Lo-tek tools and weapons like those used by pioneers, mountain men and primitive tribes are easily maintained, repaired or replaced. Most require no ammo or use ammo provided by nature (slings use stones, atlatls use sticks, etc.). They also have the advantage of silence and are great psychological weapons (Good God, he has a battleaxe!)

I am not saying you should abandon modern weapons, tools and technology; only to conserve it and not become totally dependent on it. Lo-tek is cost effective. Use it to supplement your system. The Vietcong, for example, made extensive use of blowguns, spears, crossbows, knives, and primitive boobytraps with devastating effect. Before you buy expensive gear that the "survival experts" tell you that you can't survive without, think about what you already have which will perform the given function. There are many pieces of equipment you can make for yourself, many things around the house which can be pressed into service or adapted to the cause. These are but a few things you should consider:

Trash bags and zip-lock bags protect supplies and equipment.
Empty dishwashing liquid bottles make excellent bota canteens.
Cut off legs from old jeans can be made into possibles bags.

Product Reviews

China Hunter - Model XL 144, Manufacturer - Tomahawk, Made in China, Price $2.49
Another fantastic bargain from Smoky Mountain Knife Works! This one is a quality stainless steel 6" blade hunting knife with a leather ring (a la Ka-Bar) and mock stag grips, brass guard and aluminum pommel which will take and hold a good edge and perform all the functions a utility blade should. At $2.49 each ($2.25 if you buy six or more) you should keep a few as spares.

Zulu Assegai Spear, Manufacturer - Cold Steel, Made in USA, Price - $24.99, sheath - $7.99
There are places near my suburban home where deer will walk right up to you while you are fishing. This spear would be just the ticket for hunting from a tree stand or blind. I recommend replacing the short shaft provided with on 5' - 7' for greater accuracy, weight and penetration. Do not throw at hard targets like trees if you do this. The blade may not stand up well to this sort of punishment. With short or long shaft this is an excellent close combat weapon capable of penetrating body armor.

Parsu Double Axe, manufacturer - Unknown, Made in Pakistan, Price - $14.99
Four styles of battleaxe are available from S.M.K.W.:

Mughal Axe - 39" overall - Price $18.99	Punjabi Balla Axe - 32" overall - Price $18.99
Parsu Double Axe - 30" overall - Price $14.99	Bhims Big Axe - 29" overall - Price $14.99

I purchased the Parsu expecting a decorator only and was pleased to find it could be used as a practical close combat weapon. The top spike is a little flimsy so I replaced it with a 38" bolt. The head is held on by three small brads which I removed, drilled out the holes and replaced with wood screws. If the shaft breaks it can be easily replaced with a broomstick or sapling. This exotic barbarian weapon is capable of downing an opponent with a single blow. All of the above are available from:

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

Equipment Checklist

Tools For Living Off The Land

The tools/weapons listed here are basic, multi-purpose hand tools. They are inexpensive, easily obtained and cost-effective to operate. With them you can live a primitive existence in style. Use these tools to make others, build shelter, gather food and cook.

Machete Tomahawk	Hunting/utility Knife	Axe	Folding buck saw	Folding pruning saw
Multi-tool (ie Leatherman)	Entrenching tool	Brace and bits	Hand drill	Sharpening stone

Hunting/Fishing Gear

Telescoping or takedown rod and reel	Tackle box with asst. lures, hooks, sinkers, bobbers, etc.
Fillet knife	Trot lines
Snares (optional - traps)	Slingshot and shot
Sling (make)	Fish gigs

Cooking Gear

Wok (you can cook almost anything with this)	Cast iron deep skillet with lid (doubles as dutch oven)
Coffee pot (also used to boil water for other purposes)	BBQ fork, spatula, spoon, tongs, ladle
Ginsu knife	Messkit
Canteens (improvise)	

Ω

Militia Training: Operation WitWeb

Preparing for last war

Most of the kinds of tactical training that militia units across the country have been doing have been focused on the tactical situations found in conventional or counterinsurgency warfare. And most of the alert systems that have been set up depend on telephone communications. While such exercises have some merit, they neglect the kinds of scenarios that we are more likely to face. This document describes in a general way a different kind of exercise designed to prepare militiamen for more likely scenarios, emphasizing reconnaissance, intelligence, and insurgency methods.

We call this kind of exercise WitWeb because it sets up a webwork of witnesses. Think of ourselves as a spider, spinning of web to catch some flies. In this case, the flies are corrupt or abusive officials or other criminals. Our objective is to gather and distribute evidence, protect witnesses, investigators, and other innocent persons, and bring the perpetrators to justice.

Elements of Operation WitWeb

(1) The operation should take place over a definite period of time, such as from Friday to Sunday evening.
(2) Participants would operate singly or in teams of not more than three persons.
(3) Each participant would initially receive an assignment to go to a specified location at a specified time.
(4) At each location he would either perform some action and go to another location, pick up further instructions from a dead drop, or rendezvous with another participant, exchange recognition signs, and exchange items or further instructions.
(5) Each participant would hit multiple locations during the course of the exercise, and would log the travel times, distances, and any other pertinent information about each leg of the journey.
(6) At the end, each participant would report to a task leader, who would receive his report and any items he was to deliver.
(7) One of the activities would be to reconnoiter a target site, find an observation point from which it could be surreptitiously observed, if any, and if found, describe the observation point to another participant, who would attempt to observe from that site for some period of time, while a third participant would observe his observation to determine how well he was concealing his observation.
(8) Another activity would be to videotape a target, with the date/time record feature on, then rapidly exchange the good tape for a blank and hand off the good tape to one or more couriers who would escape the scene rapidly and in different directions, deliver the tape to a location where it would be duplicated, then execute a simulated delivery of the duplicates to key persons, to hiding sites, or to media contacts.
(9) Among the observation targets would be the homes of activists, the homes of straight government agents who might be the targets of actions intended to discredit the militia, mobilization points of enemy forces, or other locations at which some event of interest seems likely to occur.

(10) Each participant would have a way to alert the others in the event of trouble at a site requiring either convergence or dispersal, indicating whether convergence should be equipped to observe or to take protective actions.
(11) One activity would be to simply spread an alert message to all the militiamen in the area as rapidly as possible without using electronic media. The methods could include voice relay, coded written messages, or hand or light signals.
(12) Another activity would be to code and/or decode messages as rapidly as possible, using both technical implements, such as computers, and non-technical, such as one-time written keys.
(13) The exercise might be supplemented by recruiting persons who regularly live and work in the target areas to be alert and prepared to observe, preferably with video cameras, in which case they would be provided with a way to alert the militia to come pick up the video tape as soon as possible after it was taken, and provide a blank tape as a replacement.
(14) The list of observation targets would be continually revised and expanded, and observations made on a random basis, so that no one, not even most of the militiamen, could be sure when any given observation might be made, but also so that no one could be sure that any given target would not be observed during any given period of time.
(15) Video cameras would be supplemented with still cameras using high-resolution film, to get detail that video can't.
(16) Observers would make lists of relevant things in the area, such as vehicles and their license plates, so that statistics could be compiled and parties of interest identified. Of particular interest would be unassigned license numbers.
(17) One activity would be to collect trash from important sites for analysis.
(18) One type of target would be storage sites and vehicles transporting illegal drugs or other dangerous contraband, with special emphasis on identifying official involvement, so that when reported to authorities the militia would not be reporting it to the same authorities involved in making the shipments.
(19) One type of activity might be the actual interception of drug shipments, combined with the destruction of most of the drugs so that they could not be diverted by officials back onto the street, but leaving enough for use as evidence in court.
(20) Another type of activity might be the observation, in relays, of the movement of election ballots, from initial production to final counting, to identify election fraud. This might involve the use of hidden cameras, including the transmission of video to a receiver who could preserve the evidence in case the on-site observer got caught with the camera.
(21) Lacking more dramatic targets, participants might practice observing lesser instances of malfeasance, such as noncompliance with legal or contractual standards for construction, environmental protection, medical procedures, or other activities which are liable to occur in the absence of witnesses.

Working with other resources

These exercises are likely to turn into serious operations involving real corruption and abuse. Therefore, it is important to line up other resources that may be important:

(1) Straight law enforcement agents. But contact should probably be with individuals rather than with departments, which may contain dirty agents.
(2) Straight reporters. Again, contact should be with individuals who have proven their willingness to take personal risks to expose the truth.
(3) Straight elected officials. In most cases, the official himself may be too busy, but one should be in contact with a key staff person.
(4) Media messaging systems. One should prepare in advance to disseminate important information to the media generally, especially key persons with talk radio and TV stations, newspapers, and mudraking magazines. This should include a computer set up to email or fax to multiple targets. Messages should always be directed to specific individuals, with a backup if the first one is out.

Things to keep in mind

(1) Participants in this exercise should remain as inconspicuous as possible.
(2) Participants should remain mobile so that they do not themselves become easy targets for attack or apprehension.
(3) There should be preparations for any participant who learns "too much" to go underground while preserving the evidence, with everything needed, such as money, ID, a cellular phone or ham radio, a vehicle with plates not linked to him, or disguises, to remain underground for an extended period of time, while preserving the ability to maintain necessary contact.

Militia Organizing: Advance Teams

Breadth of Organization

One of the most important missions of activated militia units is to organize units in other counties throughout the state, and even in other states. While it is important to involve as many people as possible in each county, down to the neighborhood level, it is also important to achieve geographic spread, so that no county of any state is without at least one unit. A certain number of active members of each unit should be designated to this mission, which involves the following suggested elements.

Elements of Advance Organization

[ ] Form 2-3 person teams. It is possible to work with more or less, but for various reasons, this seems to be an optimal number. One of them provides the vehicle.

[ ] Prepare target list of counties. Start with a list of all counties that do not yet have a known activated militia unit. Arrange the list in descending order of priority, based on factors such as population size, proximity to major highways, location in districts of important legislators, or proximity to important sites of other kinds. More populous counties will have more potential recruits living closer together, which will make it easier for them to meet and work together. Proximity to major highways is to try to get unbroken chains of units connecting major population centers, which may be important for communications and logistics. In Texas an important county would be McLennan, because it contains Waco and the site of the Davidian Massacre, where the populace needs to be activated to get a grand jury to bring indictments of the persons responsible for that atrocity.

[ ] Divide the target list among the advance teams. Some consideration should be given to familiarity of the team members with the counties and their inhabitants.

[ ] Get lists of patriots and persons inquiring about militia involvement. Such lists can be acquired from various sources, such as some of the more publicized militias of other states, subscription lists for various patriotic publications, and participants in various patriotic activities.

[ ] Mail literature to any prospects in the target counties. Such literature should contain two things: a message which arouses the reader to take action, and information on what actions he or she can take. The first might consist of tales of official corruption and abuse. The second of how to activate a local militia and contact those already activated. Ask them to respond in some certain number of days, such as seven.

[ ] Send more literature to those who respond. This may be enough to get them to activate a militia unit in their county.

[ ] Follow up on mailing targets, both those who don't respond and those who do, with phone calls. Qualify them for their level of interest, their concerns, their resources, and their intentions.

[ ] Schedule visits to each targeted county by its designated team. Let any prospects know you are coming, and try to arrange to meet with them. If there are no prospects, then go in cold and scout for some.

[ ] The team should visit likely places and persons who might refer them to prospective recruits. Gun shops, American Legion and VFW halls, civic organizations, sheriff and fire departments. Ask for the names and phone numbers of persons who have expressed concern about the threats to our rights under the Constitution.

[ ] Follow up on the leads. If the person seems interested in getting involved, leave him some literature and a phone number for the team. Compile a list of prospects, discuss the members of the list with each other to identify prospective leaders and potential conflicts. Suggest that those interested get together, and try to get them to commit to a place and time, then inform all the others.

[ ] Publicize the organizing meeting. Put a notice in the local newspaper, if there is time, and call in to any talk radio station that serves the area to announce the date, time, and place of the organizing meeting, and a contact phone number for details. This should be an easily remembered name in an easily remembered city, so that the person can call information if they don't take down the phone number.

[ ] Send literature packages to prospective attendees. To the extent possible, try to have them all come with a common foundation of understanding of the basic ideas, and with such things as proposed by-laws, so that they will not have to waste time at the meeting reading new materials.

[ ] Have the team present at the organizing meeting. Provide a speech which motivates and explains the key ideas. Have the attendees introduce themselves to each other, and perhaps explain their experiences and concerns. Hand out literature to any who did not previously receive such.

[ ] If the attendees are ready to do so, have them adopt the by-laws, elect a commander, and agree on the date, time, and place for the next meeting. Appoint persons to seek more permanent meeting places, handle publicity, reach out for more participants, and establish training and study groups on various topics. Make sure everyone who needs to contact one another gets each others' names and phone numbers.

[ ] Have the team present at the second meeting. If by-laws were not adopted and a commander and other officers elected at the first meeting, get them to do so at the second meeting. Also get them to form task groups on various subjects: military training, disaster control, legal issues, logistics, communications, public information, recruitment, site arrangements, and security.

[ ] Leave them alone for a couple of months. Let them work out their own problems for a while, without guidance from outsiders, other than newsletters, reports, and other communications from correspondence committees.

[ ] Do a follow up visit. See how they are doing. Try to help them overcome any problems that may have developed, but don't help too much. The best approach is to ask them questions and let them find their own answers.

[ ] Try to get them to organize their own advance teams. Have them coordinate with other active units to divide the target counties among them and do the same thing that was done with them.

[ ] Try to get all the counties to work toward synchronized events. Militia Day April 19. Independence Day July 4. Election day. Visits by elected officials. Special fiestas and holidays, parades, and political events.

[ ] Assemble multiple teams to organize the last remaining counties. Get teams from several neighboring counties to converge on those that remain to be activated, until every one has at least one active militia unit.

[ ] Engage law-enforcement supporters to recruit their colleagues in targeted counties. If you have the support of a sheriff or constable in one county, get him to visit, or at least call, his counterpart in the targeted county, and ask him to attend militia meetings and learn about the movement.

[ ] Likewise, engage media people, public officials, and civic leaders. Often such people are more influenced by their counterparts from other counties than by their own neighbors. Take advantage of these chains of influence.

[ ] Keep the free media flowing. Issue a steady stream of press releases, notices of meetings, statements on constitutional issues, and important events, including legislation and official acts that may impact on the militia movement. Get people interviewed on talk radio stations, and call in to them regularly with succinct messages on some point that needs to be more widely understood and discussed.

[ ] Organize letter-writing parties. Get everyone together and have them write letters to legislators, the governor, congressmen, the president, editors, or whoever needs attention. Use models of well-written letters that got responses or that got published. Make sure they don't all read alike. Offer recognition to the best ones. Make sure they are signed, stamped, and sealed before everyone leaves, and make sure they get mailed.

[ ] Organize state-wide alert system. Make sure there are at least three persons in each county who can serve as points of contact for alerts, to verify rumors, and to check on the condition of activists.

[ ] Extend this effort into other states. But be careful not to offend existing militia leaders in those states. Send literature, but avoid going in without conferring with any established state leaders, and without an invitation from the people in the target county.

[ ] Extend the alert system to other states. Make sure every active militiaman in any county of any state can find and contact someone in any given county of any other state.

[ ] Establish wireless communications links. Make sure there is an unbroken series of reliable repeaters for ham packet links between any two militia units in the country. Test it frequently.

For more information contact:
Constitution Society
6900 San Pedro #147-230, San Antonio, TX 78216
210-224-2868

Ω

Urban Survival, Part I

by **Douglas P. Bell**

To start with, let's get over the idea that all survivalists are going to get out of "the city" in time to set up a "survival retreat". Not all survivalists are going to have the money, time or inclination to leave the city life and move to the middle of nowhere. First off, leaving your job and having no money will doom you faster than anything you can think of! Also some of us just enjoy the city lifestyle and do not enjoy the bucolic life. So the problem remains, what are the urban survivalists to do?

Let's start with shelter. Most of us live in either single family homes or apartments and if you rent your house or apartment that limits what you can and can not do there. After all, it would do little good if you were to set up a fully equipped nuclear bomb shelter in the basement and got thrown out the following week!

However, this does not mean you are totally at the mercy of the landlord and the elements. First off, try talking to your landlord about survivalism, or just feel them out about their ideas of the future. This might include nuclear war, depression, gov't control over their life, etc. If done carefully, many people who would otherwise think of you as a fool or nut case will come around very nicely. If not, well you aren't out anything.

If you live in one of the impersonal high-rise apartment buildings, and they have nothing to do with you outside of getting your rent check, you might try and find out where the chimney and venting pipes are and if you are near enough you can tap into them for your heat and air without anyone knowing. If the heat supply was cut off for some reason, you could put in a small wood/oil burning stove, vent it right out the chimney, and no one would know it was you.

For a water supply, you could use 2 liter pop bottles or plastic gallon milk jugs. If you happen to live in an apartment building with a gravity fed water system, that is the water supply is on the roof, during bad times you could simply go up on the roof, shut the valves off, and tell everyone the water supply ran out. No matter what you do, it would not hurt to have a good supply of water stored just in case.

As to food, a years supply of freeze dried, air dried and canned goods can be stored in a closet; so space, if you really want it, should not be a big problem. Normally there is a lot of "dead" space to be found, under tables, beds, dressers, desks, etc., so that you should be able to store a goodly amount of stuff away where it will be out of sight, or at least out of the way.

For cooking that food a wood stove will work just fine; although camp stoves, such as the Coleman, are also small, reasonably light weight and easy to use. Remember however that burning anything will use up your Oxygen, so have an outside air supply coming in. This is especially true of charcoal stoves or grills. Used in an enclosed area it will simply put you to sleep, for good! Also beware of treated wood or plastics that will give off toxic fumes, so you don't poison yourself.

Now I know you've been waiting for this, so we will now talk about guns. What exactly you need is not easily done from long distance, although there are a few basic things that most people can agree on. In urban fighting, distances are not likely to be long, a few hundred yards at most, so you don't need a full power battle rifle capable of shooting 1000 yards and through several walls. Also depending on where you are, you may not be able to legally own handguns or "assault" style weapons.

All is not lost however. A short barreled lever action rifle, such as the Winchester 94 "Trapper" model, Marlin 336, 1894 or Rossie M92 is not likely to send the neighbors into fits of rage as would a H&K 91 or 94. The SKS in 7.62x39 is in about the same power range as the .30-30 and is extremely cheap right now (in the $100-$140 range, although this is always going up), as is the ammo, so you might consider it as well. The Marlin "Camp" guns in either 9mm Luger or .45 ACP would also make good "house" guns, although the range out of the short barrels or in the pistol calibers would be limited.

That's not all bad however, as a city in break down is likely to have roving bands of gangs or even National Guard units (remember after Hurricane Hugo when the Guard units joined in the looting?) that are better armed and/or more willing to use their weapons than you. So the less shooting you do, the less attention you will attract to yourself.

For close range firepower or "street sweeping" it is hard to beat a shotgun. A discount house here (and many gunshows) often have the Remington 870 Express model with a rifle slug barrel and a vent rib "Rem-Choke" (interchangeable screw in choke) barrel for under $300.00, which has to be one of the great bargains in the firearms field. The only down side of this gun is it is only available in 12 gauge, and many smaller or less experienced shooters might prefer 20 gauge, although regular 870s are available in just about any gauge you could want.

Other shotguns you might also want to look at are the Winchester 1200/1300 or Ranger models as well as the Mossberg 500, especially the Bullpup model that moves the action back just in front of the recoil pad and gives the gun an overall length of under 30" with an 18" barrel or just over 30" with a 20" barrel. Get the longer 20" barrel as the added few inches will dampen the recoil and especially the noise or blast when compared to an 18" barrel.

For left handed shooters or others who don't want the shells ejected from the side for some reason, the Ithaca 37 (or Model 87 as it is currently called) and Browning BPS ejects the shells out the bottom, so the shells land at your feet instead of flinging past the left handers' face. Remington also makes a left handed 870 if you would want one.

As to handguns, the police departments of many cities are turning in their revolvers for 9mm automatics. This has placed a goodly number of revolvers in either .38 Special or .357 Magnum on the market at very reasonable prices. Many of these guns will have holster wear, that is the bluing of the gun will be worn, but this will in no way affect how the gun shoots.

If possible, get the .357 Magnum over the same model in .38 Special (such as the S&W Model 10 in .38 Special and the same thing in .357 called the Model 13) and adjustable sights if offered. The .357 Magnum can shoot .38 Specials just fine, and this gives you the choice of two different cartridges (.38 Special and .357 Magnum) rather than just one (.38 Special), as well as being able to sight in for the different loads.

Ω

Thoughts From The Interzone...

I've been getting a lot of questions about our BBSes. We currently have four (with more being planned) BBS systems available for Cybertek support and feedback. The first one is on the internet at l0pht.com. To get in, just simply enter "BBS" at the user prompt, and follow the directions. Let the SYSOP, Brian Oblivion, know you're a Cybertek subscriber. The L0pht also holds a Cybertek FTP and WWW site at ftp.l0pht.com and http://www.l0pht.com/ respectively. We expect to have more sites up in the future. The rest are phone BBS, **The Runestone, 860-832-8441, new user password: Cyberdeck**; **Digital Underground, 203-281-1265**, and **The Toll Center, 718-445-5019**. These are private systems that the SYSOPs let us have some space on. For those of you without modems, we now also have a VMB up and running at **860-225-1625 (1OCL)** where you can leave voice and FAX feedback to writers and request info. Writers' box numbers will be listed in the masthead.

Cybertek has gone quarterly. I unfortunately had to do this as running it bimonthly was becoming a big drain on my time and finances. Subscribers will still get the number of issues they paid for (six). It's just that the subscription will run a year and a half, instead of a year. If things improve in those two areas, I'll take it back to a bimonthly schedule.

Those of you wanting to talk with other subscribers and technomancers can now jump on our IRC channel, #Cybertek. We hope this'll provide a place on IRC where anyone can go and have a meaningful technical discussion. Many thanks go to Fencer for his help with this.

Finally, if you are going to be moving, please notify us of your change of address if you still want to receive your subscription. We've gotten quite a few envelopes back from past mailings as a result of this. If you've moved, please take the time to send us off a quick postcard with your new address.

As always, if anyone ever has any questions, comments, suggestions, or whatever I can be reached either via the VMB system at **860-225-1625, Box 6426** (If I'm around and hear your message, I'll pick up.), through email via **ticom@connix.com** or (when I'm on it) on our IRC channel. -Tom