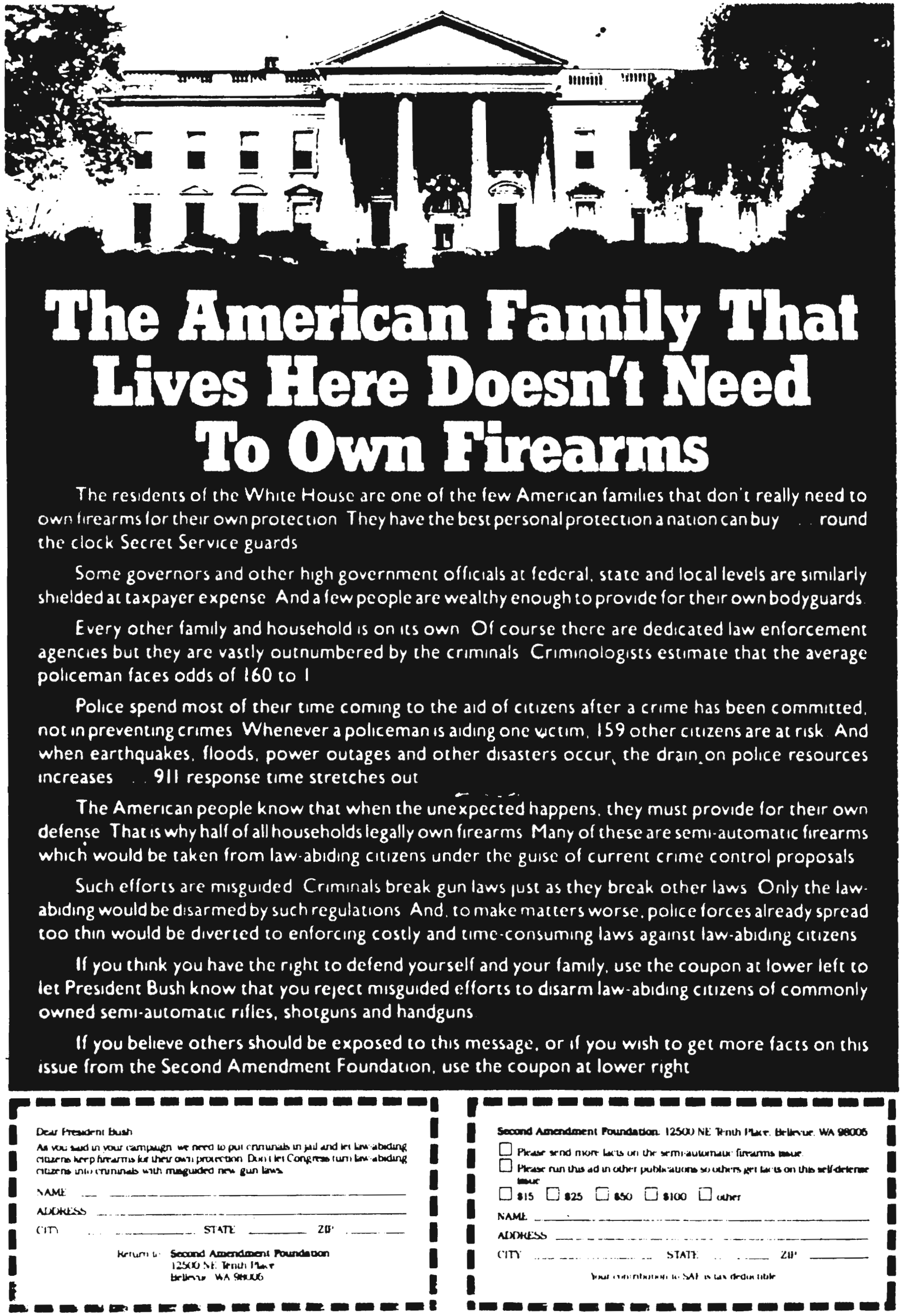


$2.00

ISSUE ONE HUNDRED AND ONE, VOLUME 15
DECEMBER FIRST NINETEEN NINETY

# TAP

*Published since 1971.*

TAP Magazine
P.O. Box 20264
Louisville, Ky 40250-0264

Welcome to issue 101 of T.A.P. Magazine. I know it has been a long time since the last issue. We have been through a few changes. Aristotle has resigned as editor and handed the magazine over to me. Since i was the publisher he felt i would best be able to pickup where he left off. I plan on making some major changes to the magazine over the next year. The first and most noticable is each issue will now cost money. Instead of just paying for postage like in the past. I will decide a cover price for each issue depending on the size and content. Most all issues will cost $1.00 for US citizens and $2.00 for overseas. Terms are CASH, postal money order, or regular money order with the payee left blank. We will not be able to take checks! They are just to much time and trouble. The reason for a price is because issues 99 & 100 took money from our pockets and depleted the supply of stamps we had. Also some of the stamps were lost because someone put elmers glue on the ones they sent in and it made about thirty dollars worth of stamps useless when some water got into the stamp supply. Someone left their window down and the dew did the rest.

Issues will be on a regular basis of one every 4 to 5 weeks. If i get some articles mailed in the issues will be out sooner. If i have to obtain information for each issue myself it will take longer. Just because you know something does not mean everyone else does. Share your knowledge and in return you might just get something back. To put it point blank i need everyone to write an article and MAIL it to me. If you can't write an article send a newspaper clipping, a book, something to contribute. If this happens the magazine will expand and be better then it ever has in 15 years of existence.

TAP also has a BBS where the staff and other readers can be reached. So if you want to exchange information a little faster then the USPS call 502/499-8933.

## How to modify a Uniden Bearcat 760xlt for 800 Mhz.

By Anonymous/M.E.

Note: This was taken off the Arpanet.

Netlanders:

Concerning the Uniden Bearcat 760xlt, the mod for the 950xlt does work to restore lost freq. Disconnect pin 20 of the microprocessor from the circuit board and connect it to pin 19. I bent the pin slightly and cut it with the scissors of a swiss army knife then soldered an 1/8 lead cut from a cap across the pins near the top of the chip. I've yet to find any problem with this mod. But as always do so at your own risk. 73 (Packet Radio Address Deleted)

## A Hard Hack - By: The CyClone

Nowadays the truth is hard to come by. Politicians are lying, neighbors and friends do it too and even the government and the President do their share of lying. It is very difficult to determine what the truth is in our deceptive society. Be a Hacker, do what you want, who really cares anyhow? Read on my hacker friend. The truth lies near.

Exactly what is an elite person and how do they get to be that way? I know It is not always a good idea to present a rhetoric question in an essay but I figured It would be a quick and unmistakable thesis to decipher, so let us proceed with what we have.

I've known three people personally before and after they became elite and boy is there a difference. The first elite hacker I ever knew was The Whizard. He dropped out of FSU his first year --actually he got kicked out, but that is another story. In 1986 till mid 1987 The Whizard was a decent person. He would trade and talk to average hackers, which was helpful to people like me. The Whizard in mid 1987 put up a Commodore 64 BBS and started calling it elite. The Deth Dungeon (sp?) was the BBS's name which shortly became known country wide to other elites. After The Whizard became elite he started bragging and of course did elite things like carding and hacking. In this process I saw a generous friend become a money/power hungry bastard. Only after he got busted for carding (selling credit card numbers that is) did he come down from his "totem pole."

Case #2 is a person by the name of Badd Boy. We traded a few wares and went to a copy party before elite fever broke (literally) out. He was a "simpleton" until he started phreaking to make a name for himself. He was in a group called The Survivors definitely a top five group in 1988. Badd Boy felt the power and succumbed to the greed. Bragging set in and well, there was a peek. Luckily Badd Boy did not totally succumb to the greed like other hackers --he did care a little. In May 1988 two days before the great southern copy party (which was canceled) Badd Boy got busted for some major phreaking. It was a big bust ($50,000 worth of calls made) and hurt Badd Boy pretty bad although he is doing "ok" nowadays.

Case #3 was another typical lamer gone elite. A "boy" (around 15 as most starting hackers are) by the name of Flyboy used to call local boards and post lots of messages --"Trade with anyone." I traded with him for awhile until he did not return some of my disks. He was a typical "nice" person until he discovered phreaking. He phreaked, became elite and shunned away from "lamers." Flyboy seemed all powerful, sometimes bragged and took to the high roads. He put up a BBS called Fabulous Disaster, an Exodus board (he somehow got into the group). He would'nt consider talking to a lamer unless they had something he needed --he was to good for that. I'm not sure what ever happened to Flyboy but I'm pretty sure his board is now obsolete.

In these three case I am not whining because I couldn't get anything off these people (although It may seem this way to a person who calls himself elite), I am simply presenting my point of view. It is sort of like schizophrenia, I mean these people were quite nice and generous when they had little, but when encompassed with wealth and power things changed.

People are people and they all seem to be the same. Look around you now, and then look around when you are a million or two dollars richer. Did anything change? Wonder why?

M.E. Note: If any member of the Outlaw Telecommandos sees this mag or if anyone knows how to reach these people, please contact TAP Magazine.

## BREAK THE SYSTEM
## WIN-$25,000

## The TymCard
## 25,000 CHALLENGE

IQ, Inc., is about to release an anti-fraud "smart card" called TymCard, to be used by long distance telephone companies to help eliminate calling card fraud. We belive our product to be unbeatable. To detect any possible flaws in our system. IQ,Inc.,is offering a prize of $25,000 to the first person who can demonstrate that he or she has been able to access the system, at any time, by being able to generate a valid code at will. Accessing the system DOES NOT mean "breaking" one or more existing TymCards as that only allows temporary and insignificant access to the system.

EXAMPLE: If you knew the numbers of one or more TELECO calling cards, you would be able to make long distance calls that would be charged to that card- until you were discovered- and that number was deacivated. If,however, you had a "Blue box", you would be able to make calls at any time. You were able to "break the system" without need for any calling numbers. The only permanent solution, as far as TELECO was concerned, was to change the system which, in effect, "deactivated" the Blue box.

A condition of this challenge is that you supply to IQ,Inc., the details on how you were able to "crack the system" and assist IQ.Inc., to correct the flaw.

Each respondant to this challenge will be invited to a meeting with members of our staff. At this meeting you will be given much more technical information about TymCard as well as a decription of the service.

Please note that there is absolutely and positivly no charge to you to accept this challenge. If you desire to "borrow" an active TymCard that will allow you to test the system at any time, we ask for 50.00 cash deposit. This deposit will be returned to you, in full, upon the TymCard being returned to IQ.,Inc, as agreed.

If you are interested, please call (818) 592-0423
for more information as to the time and location of the next meeting.

NOTE: If you are not located in the Los Angeles area please call the number to arrang for complete information to be sent to you by mail.

Typed by TECHNO-COWBOY

Oct 1990

## BEARCAT 200XLT CELLULAR FREQUENCY RESTORATION
By Anonymous/M.E.

### NOTES

It is unlawful to monitor cellular telephone conversations. It is possible to monitor signals from the deleted ranges even without conversion. Simply add 21.7 MHZ to the deleted frequency and enter the higher (image) frequency. Reception is virtually identical in strength to that which would be heard on the deleted frequency.

The frequencies deleted at the factory may be restored, but the procedure should not be attempted by anyone unfamiliar with electronic circuitry. No one anywhere, anytime, in anyway, etc... assumes any responsibility for damage caused by this procedure.

**THIS MODIFICATION WILL VOID YOUR WARRANTY!**

### TOOLS

Small Philips Screwdriver
Small Wire Cutters

### DISASSEMBLY

1. Slide off the battery pack and remove your antenna.
2. Remove the two screws from the back of the scanner, the two screws which hold the battery retaining spring at the base, and the battery retaining spring itself.
3. Carefully pry the bottom of the rear cover from the radio and remove the cover.
4. Locate the two small screws at the base of the circuit board and remove them. Gently pull the front panel from the mainframe at the base and separate them.

### MODIFICATION

5. On the face of the circuit board that faces the front of the scanner when installed, locate the microprocessor IC labeled "UNIDEN UC-1147". Locate the 10K ohm resistor (brown, black, orange), which is positioned approximately along the longitudinal centerline of the board, and next to the microprocessor. The resistor is of the leadless type and should be positioned directly next to the microprocessor and above the "DEN" on the IC label.
6. Using the small wire cutters, cut the resistor body in two without disturbing anything next to it. If the left solder pad comes loose, it may be peeled from the board. Brush or blow away any debris. This completes the restoration.

### REASSEMBLY

Continued Next Page

7. Insert the top of the front panel into the slot under the volume/squelch control panel and, noting carefully the alignment of the dual-inline connector at the bottom of the board, press the front panel firmly into place. Be sure that the holes at the bottom of the circuit board line up with the holes in the plastic standoffs below them. Insert the two screws and gently tighten them.

8. Replace the back cover by inserting the top of the cover into the slot under the volume/squelch control panel; press the cover into place, insert and tighten the screws.

9. Reposition the battery retaining spring (slotted side toward notched hole), insert the two remaining screws and gently but securely tighten them.

10. Slide the battery pack into place; switch the scanner on to make sure the display comes on. If not, the battery is discharged or the dual-inline connector was misaligned during assembly (see step 7).

## CHECK OUT

11. Assuming the display comes on, press: MANUAL, 845.0, E; within two seconds the frequency 845.000 should appear on the display.

## AKNOWLEDGEMENTS

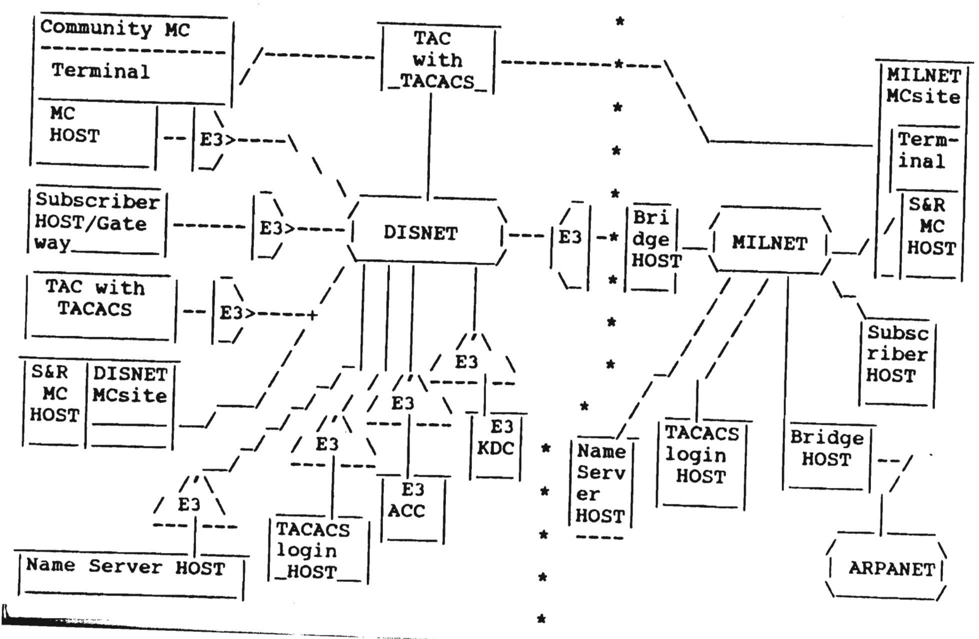
MONITORING TIMES
140 Dog Branch Road
Brasstown, North Carolina 28902

The Monitoring Times sells better instructions on how to do this, if you wish to obtain them, send a check for $2.00 and a stamped self-addressed envelope to the above address.

## DDN - The Defense Data Network

```
      \|/
By Star -*- Fire [a member of Mysterion Grp]
      /|\
```

Diagram of DDN:



## DDN - The Defense Data Network

The Department of Defense started the major networking scene in the US in the late '70s and early 80s. Their first baby was ARPANET (Advanced Research Projects Agency NETwork). It was just a development system to see how feasible a national computer network would be and to help facillitate information transfer between defense researchers (and some university projects). The world of InterNET has grown up around that existing foundation to become one of the most (THE most?) used network in the world as researchers in other nations found they also needed access to counterparts around the nation to exchange knowledge and ideas. Well to end this simple history I will get back to the DDN and its workings (what little I do really know of them) and it structure.

The DoD (Dept of Defense) has been maintaining its own separate networks ever since ARPANET became a success and was "gobbled up" by the growing InterNET structure. The DoD wanted to be able to secure its important work and research and to do so it needed to be isolated from the existing infrastructure. They decided that a somewhat free flow of information would be necessary between constituents and that some kind of framework similar to Internet would be beneficial but that access to their systems would have to be limited by means more secure than anything available on the public Internet system. They developed MILNET for this specific purpose (to carry unclassified data traffic between defense contractors and researchers).

Beyond MILNET there were also been establish three other military nets under the auspices of the Defense Secure NETwork (DSNET). The three were DSNET1 for Secret data, DSNET2 for Top Secret data, and DSNET3 for special Top Secret data (probably weapons systems and plans, and ELINT/SIGINT systems -- but that is only a guess). These three each had a separate communications hub including local and widearea nets. The 3 DSNETS have been combined (are being combined) in a unified DISNET (Defense Integrated Security NETwork).

The Defense Communication Agency (DCA) was put in charge of maintaining the backbones of the defense networks (except ARPANET which is primarily used by the R&D community and is maintained by DARPA and is not really associated with DDN) as part of the Defense Communication System (DCS). All DDN Nets are not part (officially) of InterNET because of the security risks involved.

The restructuring of DDN into DISNET is a continually evolving project (especially in the area of Defense Messaging System - which I know little about at this time and WOULD LIKE TO SEE MORE INFO about if anyone knows about it ), but I will explain its structure as presently laid out...

"(1) Security architecture should include a well-defined set of network security services offered to subscribers"
Services:
CONFIDENTIALITY:
1.Mandatory Confidentiality - protects classified data using DDN rule based security
2.Discretionary Confid. - identity based (Need-to-Know) security
3.Traffic Flow Confid. - protects against disclosure by observing characteristics of data flow
\
_____See the encrypthion and communities descriptions below for more on this.

DATA INTEGRITY - protects against (OR ATLEAST TRYS TO DETECT) unauthorized

Continued Next Page

changes of data

IDENTIFICATION, AUTHENTICATION, AND ACCESS CONTROL : *

1. Identification- standard name for each system entity (just like every net.
2. Authentication- ensures that a stated identity is correct (HOW???)
3. Access Control- limits system resources to a correctly identified system

"(2) Subscribers should not pay for or be hampered by unneedded security"
^_______ Interesting...who does pay for un-needed security then?!?

""(4) Subscribers should share responsibility for security where appropriate" <----<<<< COULD THIS BE A MAJOR DOWNFALL?? Hmm...
* - As for I,A, and AC(above) These services are subscriber responsibility except for major communities and subcommunities.

STRUCTURE OF THE DDN :

The primary elements are computers called switches which communicate via inter-switch trunks.(DCA owns the switches and leases most trunks)

Each subscriber connects to DDN as a HOST or a TERMINAL. DDN serves hosts at the OSI (Open Systems Interconnect) network level; the Host - Switch interface is the standard X.25 (CCITT). Many of the hosts are gateways to other nets (mainly LANs) and the number of gateways is increasing.

Special Hosts:

Montitor Centers (MC) : they manage the switches, trunks, and other special hosts.
Name Server hosts - they translate the addresses of the other hosts

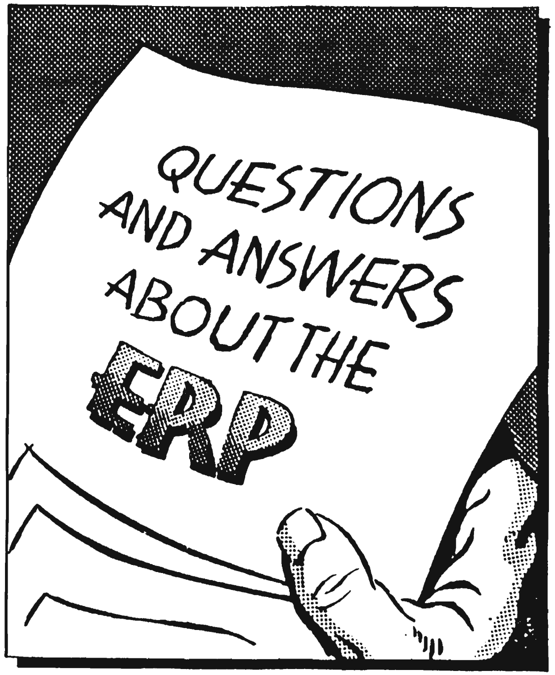
Terminal Access Controllers (TACs) - more limited DDN service. Instead of a direct Host-to-Switch connection you can connect to a TAC (via dial-up) and be addressed as a terminal by DDN through TAC. TAC uses TELNET protocol so terminal can communicate with a second DDN Host as if directly connected.

TAC Access Control Systems (TACACS) - prompt user to login at a TAC

Priority Access:
All DDN switches can handle data packets according to 4 level hierarchy system. precedence lavels are assigned to hosts and terminals by the Joint Chiefs of Staff. To my knowledge this hasn't been implemented yet.

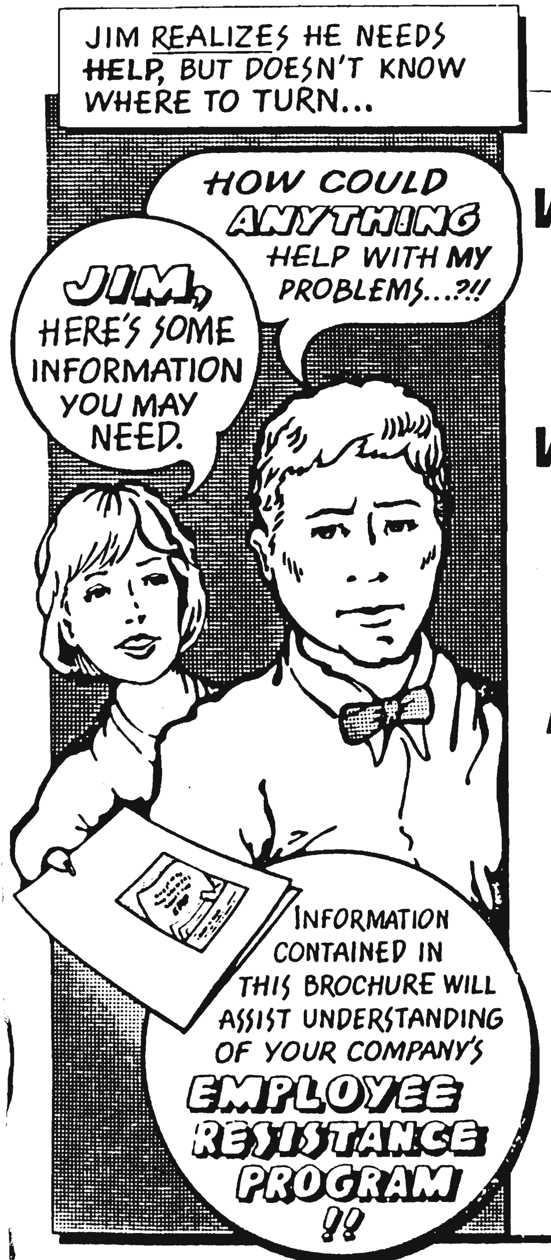
Host to Host Encryption:
DISNET uses a end-to-end encryption system (E3) called BLACKER. These are installed on each host-to-switch path of all hosts including TACs . These BLACKER front end devices (BFEs) encrypt all data packets but leave the X.25 header unencrypted for the backbone to use. The BLACKER system includes a Key Distribut-ion Center (KDC) and Access Control Center (ACC) hosts. BLACKER is a Class A1 System (under the Trusted Computer System Evaluation Criteria / "Orange Book"), and it will be able to prevent a community MC from communicating with other MCs in other communities; this will not happen for a while and the MC sites will still have a terminal through a TAC directly to a switch without going through BFE.

Bridges between Nets:
The plan calls for limited gateways between MILNET and DISNET to allow unclassified data traffic (in the form of store-and-forward electronic mail in both directions). Data entering DISNET from MILNET will be identified as



PROVIDED BY

THE DEMOCRATIC FREE PEOPLE'S ARTISTS AND WRITERS COLLECTIVE OF SATURDAY THE 14TH INC. ©1989 ALL GAME PRESERVED


JIM REALIZES HE NEEDS HELP, BUT DOESN'T KNOW WHERE TO TURN...
HOW COULD ANYTHING HELP WITH MY PROBLEMS...?!!
JIM, HERE'S SOME INFORMATION YOU MAY NEED.
INFORMATION CONTAINED IN THIS BROCHURE WILL ASSIST UNDERSTANDING OF YOUR COMPANY'S EMPLOYEE RESISTANCE PROGRAM !!

## What is an ERP?

The Employee Resistance Program is a support "network" of disgruntled employees like yourself. The ERP provides an outlet for the frustrations of everyday working life which, if allowed to build up, can break one's spirit or even trigger a psychotic episode.

## Why does my company have an ER P?

Because it doesn't know it has one. ERPs quietly spring up in the fertile soil of bad working conditions. Random drug testing, constant toadying, and Orwellian methods of surveillance contribute to a "shitty" work environment. An estimated 95% of all jobs include some or all of these elements. Your company almost certainly has an ERP.

## How does the ER P work?

It begins spontaneously, when one employee has had his or her fill of the everyday "bullshit" he or she must submit to just to stay alive. First come petty acts of sabotage and theft of company resources and time (for example, this brochure was created at the workplace, on company time), and from there it escalates. Workers are encouraged to add personal touches to the ERP. Creativity is key. Many workers, even without coordinating activities, can wreak major havoc, from which the company may never recover. Methods vary from one employee to the next, so no discernible pattern emerges to tip off corporate troubleshooters. This system is virtually foolproof.

## Is the ERP really confidential?

It must be; we've still got our jobs. Since the employee works alone, the only risk of discovery comes through carelessness. A worker successful in using the ERP may be tempted to brag to his or her fellows, who might be corporate stooges. Ego massaging such as this throws confidentiality out the window and the employee out the door. Be carefull As William Casey, the late CIA chief, said, "Two can keep a secret if one of them is dead."

## Why is a program like this needed?

The ERP is needed to help victimized employees pass back to the employer the high psychic costs of enduring daily the organized degradation that is work. Corporations that fail to recognize this suffer from terminal rot and are destroyed by the ERP, out of mercy. Thus, the ERP benefits employee and employer alike.

## What kinds of problems does the ER P assist individuals with?

There are a wide range of problems, all stemming from an employer's neurotic need for control over every aspect of an employee's life on the job or off it. This constant prying causes drug and alcohol abuse, family discord, depression, trauma, financial strain, and emotional disorders.

## What about family members?

Family members should apply the ERP to their own lives. They should offer advice, encouragement, and, most of all, an oasis of sanity to which the employee can escape at day's end.

## How do I enter the ER P program?

You enter by taking that first step, however small, towards fighting back. One evening, you and your friends are sitting on the porch, "shooting the shit." Having exhausted the usual topics of women, sports, and the Greenhouse Effect, you begin swapping stories about the job. As you drink, your pent-up rage at your job rises toward the surface. Someone relates a classic tale of "really fucking over" the boss. Now on your tenth beer, you hear most of it before passing out. Badly hung over the next morning, your head in the toilet, you remember little. But you realize that your job is an endless string of such mornings. And another link is forged.

## Am I responsible for payment for these services?

No way. This strictly a public service, provided by people like yourself, who want to see an obsolete corporate order squashed like a turd under a tennis shoe. In any case, what could we charge for? This is largely a do-it-yourself program, a sort of Popular Mechanix project you cook up in the basement of your mind. If you pay anyone, pay yourself; you've earned it.

## Who do I talk to when I have a problem?

Your friends, mostly (except those at your job, unless you're really sure). Anyone who has some integrity and an idea of how life really works. Do some reading. Try Raoul Vaneighem's "The Revolution of Everyday Life," Bob Black's "Abolish Work," the "Pranks" issue of ReSearch Magazine, or The Situationist International Anthology, ed. by Ben Knabb. Don't pass up "The Book of theSubgenius" ($12 ppd to World Subgenius Foundation, P.O Box 140306, Dallas, TX 75214). You are not alone. We're around here somewhere.

## What can I expect on my initial visit?

Visit? What are you talking about? Perhaps you are concerned that the ERP promotes violence. Not so. The ERP calls for the employee to put a little pressure on a tottering system, then jump out of the way as it collapses. And sell the pieces for scrap. We do get our share of nerds ("ERPies" we call them). It's unavoidable. Ignore them.

## When can I contactthe ERP network?

Theoretically, any time of the day or night is acceptable. Many in our program, by virtue of the jobs that drove them to us in the first place, keep odd hours. When it comes to planning some ERP tactics, a midnight meeting can be very conducive to the flow of creative ideas.

such by the bridge.
The DDN plans forbid a subscriber from connecting to both MILNET and DISNET and also forbids DoD system to connect both to a DDN segment and to a segment that does not conform to DDN security structure.

Other Stuff:
To insure that every subscriber system can exercise discretionary access control over its resources through DDN, and of DDN resources via the subscriber system, DDN requires that all subscribers be TCSEC Class C2 secure. By september '92 any non-complying system will need OSD and JCS waivers or DCA can remove them from the Net.

DDN plans to segregate subscribers according to whether or not they meet the TCSEC C2 requirement. Conforming systems comprise a Trusted Subcommunity within each security level. Within this subcommunity hosts can freely communicate. NonConforming systems with waivers will form Closed Communities within each level. Direct net communications between subcommunities will be prevented by switching logic in MILNET and by BLACKER in DISNET except over trusted bridges.

This information brought to you by Mysterion Group

## American Telephone & Telegraph **SECURITY DIVISION**

free pay telephone calling!
i will now share with you my experiences with pay telephones. you will discover that it is possible to get money from a pay phone with a minimum of effort.

theory: most pay phones use four wires for the transmission of data and codes to the central office. two of them are used for voice (usually red and green), one is a ground, and the last is used with the others for the transmission of codes.

it is with this last wire that you will be working with. on the pay phode that i usually did this to, it was colored purple, but most likely will be another color.

what you will do is simply find a pay phone which has exposed wires, such that one of them can be disconnected and connected at ease without fear of discovery.
you will discover that it is usually a good idea to have some electrical tape along with you and some tool for cutting this tape.
through trial and error, you will disconnect one wire at a time starting with the wires different than green and red. you do want a dial tone during this operation.

what you want to disconnect is the wire supplying the codes to the telephone company so that the pay phone will not get the 'busy' or 'hang-up' command.
leave this wire disconnected when you discover it.

what will happen: anytime that someone puts any amount of money into the pay phone, the deposit will not register with the phone company and it will be held in the 'temporary' chamber of the pay phone.
then, (a day later or so) you just code back to the phone, reconnect the wire, and click the hook a few times and the phone will dump it all out the shute.
(what is happening is that the 'hangup' code that the phone was not receiving due to the wire being disconnected suddenly gets the code and dumps its' 'temporary' storage spot.

you can make a nice amount of money this way, but remember that a repairman will stop by every few times it is reported broken and repair it, so check it at least once a day.

enjoy and have fun.. many phones i have done this to, and it works well with each.. if there is interest, i do have information on hardwiring to other phone lines...

# AJ Hacker Zappers

## You never know when hackers will strike.

Sometimes they just nibble away; other times they attack full force. Wishful thinking won't stop them, and most dial-up modems open your system to anyone dialing the right telephone number.

What you need is the AJ Hacker Zappers—security modems and encryption devices ready and able to protect your data files from intruders.

### No Data Security Problem is Too Tough

With powerful weapons like Callback, Answerback, and Encryption, AJ Hacker Zappers will tackle your toughest data communications security problems—from PC security to remote call-in diagnostics.

### AJ Hacker Zapper Security Modems

The AJ 2412-AD3H and AJ 2441-1. 2400 bps, "AT" compatible, Hacker Zapper modems with Callback, Answerback, and Passwords. With up to 200 Callback numbers plus optional MNP 4 or 5, the rack-mountable AJ 2441-1 is unbeatable for central site security.

### Encryption—Even Electronic Mail

If you need encryption, the AJ Data*Safe provides DES (Government approved) encryption for file transfers and PC files. Even electronic mail.Use the AJ Data*Safe to encrypt your electronic mail messages and your mail will be unintelligible to mailbox snoops.

### The Solution

AJ security modems alone or with the AJ Data*Safe. Affordable and sophisticated Hacker Zappers from Anderson Jacobson.

ANDERSON JACOBSON

CIRCLE 1 ON READER SERVICE CARD

In this issue we will try and answer some questions and the ones we can't we hope that our readers can. So enjoy.

Dear TAP,

I got TAP #97 last week and GREATLY enjoyed reading it. Highly informative. I wouldn't consider myself a hacker, but your article "A beginners guide to hacking" makes it very alluring (however, my hardware consists of a commodore 64 with a VIC-20 modem and cassette tape software). Is there any hope? Should i change modems? The other articles were also informative; I've already succeeded with the "Redneck Penny."

Austin, TX

Dear Austin,

Issue 97 was our first attempt at the digest size issue and we liked it a lot better also. To answer your questions about a commodore. The modem that has the most hacking and phreaking software written for it is the c1670 modem. It is made by commodore. They range in price from 50-80 dollars. It depends on if you buy it locally or mail order. You would also want to get a 1541 disk drive, many programs won't work with a cassette tape. That should get you headed in the right direction. I also think you will find "Phoneman" a very good terminal program. It has many different tone emulators for colored boxes.

Dear TAP,

I was wondering if it's possible to make a universal garage door opener. Like the TV remotes that are universal and work on any TV. This would allow you to open someones garage without having a certain opener.

Dayton, OH

Dear Dayton,

I don't know the exact frequencies that garage door openers run on, but i would assume that once found you could make an adjustable one with a knob of some kind to increase or decrease the range. If any reader can help please send the range the frequencies run in, or help on how this could be done.

Dear TAP,

I would like to know if it's possible to copy or pirate nintendo games?
TAP Reply,

I have heard that nintendo games use a means of copy protection.  They have different eproms on about every 1,000 cartridges made.  Thus making each lot different from all the others.  If you had a way to copy the eproms and burn them

Continued next page

into a blank one i guess it would work. But if they have copy protection built in you would have to find a way to bypass it.

Dear TAP,

Why don't you all put out an online type magazine like Phrack or ATI does?

TAP Reply,

We have been thinking about doing this for a few months now. As soon as all the staff has a computer and a modem we might attempt something. It would have to be different from all the rest though.

Dear TAP,

Was that really a picture of you guys on the cover of issue 99?

TAP Reply,

Nope, we found that picture on a telephone poll, but thought what the hell, it would make a fancy cover.

Dear TAP,

How come 2600 never mentions you as being another hacker publication in their mag?

TAP Reply,

Ask Eric Corley i don't know...

Dear TAP,

How can you publish this stuff without the PHeds arresting you for doing it?

TAP Reply,

We gave them some donuts filled with brainwashing grape jelly and they don't know we exist.

Dear TAP,

How can you guys publish for free? I like the mag and enjoy reading it but wonder how you guys do it?

Arizona

Dear Arizona,

TAP used to be free when it was just a newsletter, but since we have gone to the digest/magazine size it costs to much to give away free.

Dear TAP,

Continued Next Page

I have written many articles how do i get them published in TAP magazine?

Milwaukee, WI

Dear Milwaukee,

We would like to get many article from our readers. We can't print them all, some might not fit our format or be up to par with what we would use, but feel free to send us anything you think we might like reading. Newspaper clippings can also be useful to let us know whats going on in your area.

Dear TAP,

With all the stuff about Operation Sundevil why didn't you have any info on it?

Dallas, TX

Dear Dallas,

We thought since it was in and on most everything else we would save you from the effort of reading it all over again. We cannot take a stand unless we know both sides of the story and with the federal cover ups and changing stories every week we just see it as another massive scare tactic. If for some reason you have been on an island or in a cave you can find info on Sundevil in CUD, 2600, Phrack, newspapers and just about every online service out there.

Contrary to popular belief, the American hackers have not lost the craving for knowledge that has made us hackers. Although most people seem to think that the europeans and japanese have surpassed the U.S. in the quest for knowledge and learning spirit. Hacking is alive and well in the good ol' U.S. of A. We might be a bit cautious because of the recent deterioration of our rights and the over zealous activities of the nazi-like S.S. (U.S. Secret Service) but that is just the American instinct for survival. If the U.S. hackers were as open about hacking as in the old days, the S.S. and every other law enforcement official looking for a promotion would surely target the "EVIL" hackers for another "lets take away their rights" session. It is only logical that we, the hackers, should take certain precautions to protect our privacy and freedom. While the lesser of our community has to retreat into the "It's just not like the 70's anymore" syndrome, the REAL hackers have been busy probing and pondering the aspects of all the newest technology.

The future is now! And we in the future have all the best toys. Of our favorite are the wireless telephones. Among the wireless phones, there are three major types. Cordless, Radio, and Cellular. In upcoming issues, I will be printing some of the better articles on wireless phones. Some are written by myself while others have been reprinted from text files. In any case the information will be presented in the best possible format for your maximum cerebral stimulation. This first set of articles will deal with the cellular phones and radio scanners which can be used to monitor phone transmissions. Please note that as always, All information in TAP Magazine is for informational purposes only!

# THE DNA BOX
## Hacking Cellular Phones
By

The Outlaw Telecommandos

### PART ONE

It turns out that there are several Japanese handheld transceivers (HT's) available in the US for use by ham radio hobbyists that have hidden features allowing them to operate in the 800MHz band used by cellular telephones. Using an FSK decoder chip and a personal computer running an assembly language program to record and decipher the ID beeps at the beginning of cellular calls, a "phone book" of cellular ID's can be compiled. A simple FSK oscillator controlled by the PC can then be used to dial out using the Handheld Transceiver and the captured ID codes.

A low tech analysis could be done by taping the beeps and playing them back at slow speed into an oscilloscope. An edited tape may even be adequate for retransmission; no deciphering required.

Several radio stores in Los Angeles sell the HT's and have given advice in the past about how to access the hidden out-of-band tuning features in the ROMS of the Japanese HT's(See other articles.) It's possible now to listen in to cellular phone conversations without building any special hardware. In fact if you have a good antenna, or live near a cellular repeater tower, you can pick up cellular calls using a UHF TV with a sliding tuner by tuning in "channels" between 72 and 83 on the UHF dial (See future issue of TAP.)

Beside the obvious benefits of unlimited, untraceable, national mobile voice communication, there are other uses for cellular hacking.
For instance: most people using cellular phones are pretty upscale.
It may be possible to scan for ID codes of the telephones of major corporations and their executives and get insider stock trading information. Simply by logging the called and calling parties you will be able to compile a database mapping out the executive level command & communication structure. If this is linked to a remote controlled tape deck you will know precisely what is going on and be able to note any unusual activity, such as calls between the executives of corporations that are in a takeover or leveraged buy out relationship. It is even likely that you will occasionally intercept calls between investors and their stock brokers, or calls discussing plans for new contracts.

This data is most safely used for insider trading of your own; there will be no way that the Securities and Exchange Commission can establish a link between you and the insiders. A more risky proposition would be to offer any intelligence gathered to competitors for a price as industrial espionage.

Then there are the anarchy & disruption angles for cybernetic guerrilla action at the corporate economic & financial level. Leaking info to the press can kill a deal or move stock prices prematurely. Intelligence gathered via cellular hacking can also be used to plan operations against corporate mainframes by providing names and keywords, or indicating vital information to be searched for. Listening to the phone calls of candidates and their campaign staff is also a field rich in possibilities.

A related technology waiting to be hacked is the nationwide net of pocket pagers. The possibilities for executive harassment using beeper technology are relatively unexplored.

There are also several on-line instant stock & commodity quotation systems that use SCA subcarriers to transmit investment data. By watching activity on these networks you will be able to look over the shoulder of investors as they plan their strategy - what kind of inquiries are they making and what the results are.

Here are a few of the online investment services (business offices, ca.1987)

| | | |
|---|---|---|
| DATAQUICK | 1-800-762-DATA (voice) | Southern CA Real Property Data |
| Lotus Signal/QuoTrek | 1-800-272-2855 (voice)<br>1-800-433-6955 (voice) | Stock Market Data |
| FutureSource | 1-800-621-2628 ext.34 (voice) | Futures Trading Data |

(Or check recent ads in Wall Street Journal etc.)

At any rate, I propose that we start pooling info about cellular phones toward the goal of building a 'rosetta stone' of cellular dialing protocols, frequencies, technical info and hardware/software hacks. (Send all info to TAP)

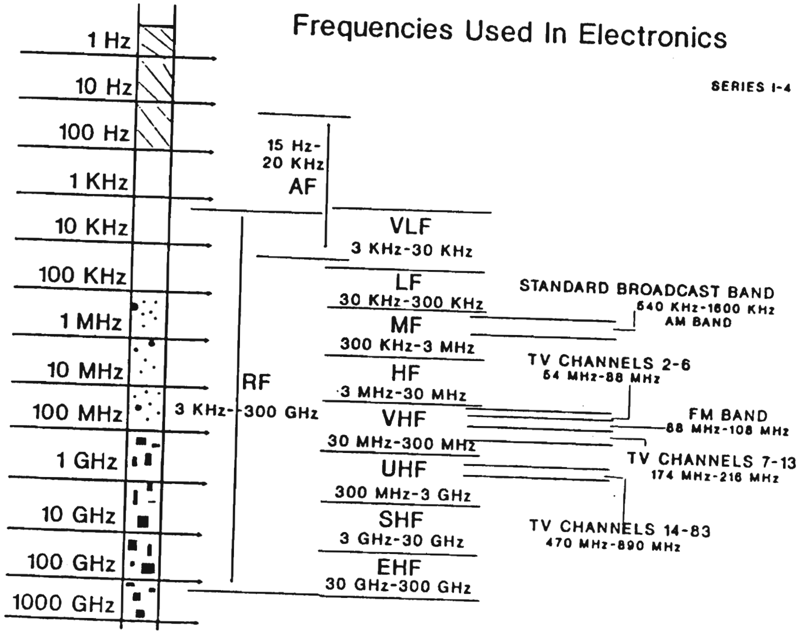
High on the hit list is a service/repair manual for a cellular phone, and journal or technical articles about the inner workings of the cellular phone system.

### DEFINITIONS for FREQUENCIES 1-4

| Prefix | Symbols | Value |
|---|---|---|
| kilo | K | 1,000 or ($10^3$) |
| mega | M | 1,000,000 or ($10^6$) |
| giga | G | 1,000,000,000 or ($10^9$) |

| | |
|---|---|
| AF | Audio Frequencies |
| EHF | Extremely-High Frequencies |
| HF | High Frequencies |
| LF | Low Frequencies |
| MF | Medium Frequencies |
| RF | Radio Frequencies |
| SHF | Super-High Frequencies |
| UHF | Ultra-High Frequencies |
| VLF | Very-Low Frequencies |
| VHF | Very-High Frequencies |

WE'D LIKE TO
REMIND YOU
THAT THE
UNCENSORED CONTENT
OF THIS
NEWSLETTER
IS MADE POSSIBLE
BY THE
CONSTITUTION OF THE
UNITED STATES.


Frequencies Used In Electronics

SERIES 1-4

TAP Magazine participates in a program whereby you may receive threats and visits from law enforcement agencies. If for some reason you would prefer not to be part of this program please send $49.99 and have your name removed from the hit list. Just joking, but it sounded good!