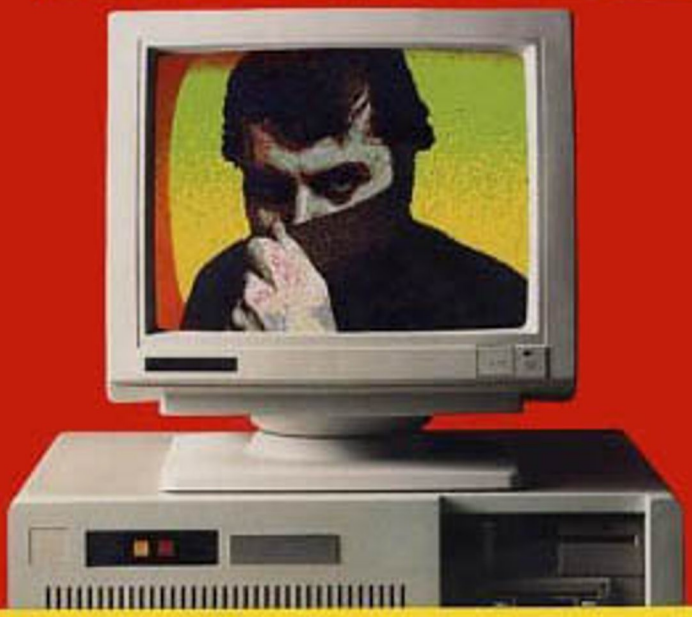
THE HACKER CRACKDOWN



BRUCE STERLING

Note

This Doc-Version of the Electronic Book by Bruce Sterling is exactly the same as the original Txt-Version, I did not change an only word of this book, I only organized it the best that I can, giving to it a good layout, finding the right picture for the cover, re-organizing the chapters, the lists and the Chronology, and trying to make it comfortable to read.

I added to this file another writing by Sterling, this is an article published first for *The Magazine of Fantasy and Science Fiction*, on February 1993, this a short but very clarifying history of Internet, from the beginning to now.

I do not advance any request for my work, and I obviously do not want to make money with it, you'd better do the same!
Enjoy it and spread it.

Puppet
puppet.trash@libero.it
http://digilander.libero.it/puppetweb
http://www.myspace.com/puppetweb

P.S.: Please, if you can, print this file on good recycled paper,
it will be better for the trees, for our planet, and for your soul…
God Bless You!

Summary

Summary....3
Preface to the Electronic Release....4
The Hacker Crackdown: Introduction....6
Part One: Crashing the System....8
-Section 1-....9
-Section 2-....15
-Section 3-....16
-Section 4-....18
-Section 5-....20
Part Two: The Digital Underground....28
-Section 1-....30
-Section 2-....33
-Section 3-....37
-Section 4-....46
-Section 5-....48
Part Three: Law and Order....55
-Section 1-....61
-Section 2-....64
-Section 3-....66
-Section 4-....66
Part Four: The Civil Libertarians....74
-Section 1-....75
-Section 2-....83
Afterword: The Hacker Crackdown Three Years Later....94
Chronology of the Hacker Crackdown....99
Internet....101

Preface to the Electronic Release.

January 1, 1994 - Austin, Texas

Hi, I'm Bruce Sterling, the author of this electronic book. Out in the traditional world of print, The Hacker Crackdown is ISBN 0-553-08058-X, and is formally catalogued by the Library of Congress as:

- Computer crimes - United States.
- Telephone - United States - Corrupt practices.
- Programming (Electronic computers) - United States - Corrupt practices.

'Corrupt practices', I always get a kick out of that description. Librarians are very ingenious people.

The paperback is ISBN 0-553-56370-X. If you go and buy a print version of The Hacker Crackdown, an action I encourage heartily, you may notice that in the front of the book, beneath the copyright notice - "Copyright © 1992 by Bruce Sterling" - it has this little block of printed legal boilerplate from the publisher. It says, and I quote: "No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher. For information address: Bantam Books."

This is a pretty good disclaimer, as such disclaimers go. I collect intellectual-property disclaimers, and I've seen dozens of them, and this one is at least pretty straightforward. In this narrow and particular case, however, it isn't quite accurate. Bantam Books puts that disclaimer on every book they publish, but Bantam Books does not, in fact, own the electronic rights to this book. I do, because of certain extensive contract maneuverings my agent and I went through before this book was written. I want to give those electronic publishing rights away through certain not-for-profit channels, and I've convinced Bantam that this is a good idea.

Since Bantam has seen fit to peacably agree to this scheme of mine, Bantam Books is not going to fuss about this. Provided you don't try to sell the book, they are not going to bother you for what you do with the electronic copy of this book. If you want to check this out personally, you can ask them; they're at 1540 Broadway NY NY 10036. However, if you were so foolish as to print this book and start retailing it for money in violation of my copyright and the commercial interests of Bantam Books, then Bantam, a part of the gigantic Bertelsmann multinational publishing combine, would roust some of their heavy-duty attorneys out of hibernation and crush you like a bug. This is only to be expected. I didn't write this book so that you could make money out of it. If anybody is gonna make money out of this book, it's gonna be me and my publisher.

My publisher deserves to make money out of this book. Not only did the folks at Bantam Books commission me to write the book, and pay me a hefty sum to do so, but they bravely printed, in text, an electronic document the reproduction of which was once alleged to be a federal felony. Bantam Books and their numerous attorneys were very brave and forthright about this book. Furthermore, my former editor at Bantam Books, Betsy Mitchell, genuinely cared about this project, and worked hard on it, and had a lot of wise things to say about the manuscript. Betsy deserves genuine credit for this book, credit that editors too rarely get.

The critics were very kind to The Hacker Crackdown, and commercially the book has done well. On the other hand, I didn't write this book in order to squeeze every last nickel and dime out of the mitts of impoverished sixteen-year-old cyberpunk high-school-students. Teenagers don't have any money - (no, not even enough for the sixdollar Hacker Crackdown paperback, with its attractive bright-red cover and useful index). That's a major reason why teenagers sometimes succumb to the temptation to do things they shouldn't, such as swiping my books out of libraries. Kids: this one is all yours, all right? Go give the print version back. *8-)

Well-meaning, public-spirited civil libertarians don't have much money, either. And it seems almost criminal to snatch cash out of the hands of America's direly underpaid electronic law enforcement community.

If you're a computer cop, a hacker, or an electronic civil liberties activist, you are the target audience for this book. I wrote this book because I wanted to help you, and help other people understand you and your unique, uhm, problems. I wrote this book to aid your activities, and to contribute to the public discussion of important political issues. In giving the text away in this fashion, I am directly contributing to the book's ultimate aim: to help civilize cyberspace.

Information wants to be free. And the information inside this book longs for freedom with a peculiar intensity. I genuinely believe that the natural habitat of this book is inside an electronic network. That may not be the easiest direct method to generate revenue for the book's author, but that doesn't matter; this is where this book belongs by its nature. I've written other books - plenty of other books - and I'll write more and I am writing more, but this one is special. I am making The Hacker Crackdown available electronically as widely as I can conveniently manage, and if you like the book, and think it is useful, then I urge you to do the same with it.

You can copy this electronic book. Copy the heck out of it, be my guest, and give those copies to anybody who wants them. The nascent world of cyberspace is full of sysadmins, teachers, trainers, cybrarians, netgurus, and various species of cybernetic activists. If you're one of those people, I know about you, and I know the hassle you go through to try to help people learn about the electronic frontier. I hope that possessing this book in electronic form will lessen your troubles. Granted, this treatment of our electronic social spectrum is not the ultimate in academic rigor. And politically, it has something to offend and trouble almost everyone. But hey, I'm told it's readable, and at least the price is right. You can upload the book onto bulletin board systems, or Internet nodes, or electronic discussion groups. Go right ahead and do that, I am giving you express permission right now. Enjoy yourself.

You can put the book on disks and give the disks away, as long as you don't take any money for it.

But this book is not public domain. You can't copyright it in your own name. I own the copyright. Attempts to pirate this book and make money from selling it may involve you in a serious litigative snarl. Believe me, for the pittance you might wring out of such an action, it's really not worth it. This book don't "belong" to you. In an odd but very genuine way, I feel it doesn't "belong" to me, either. It's a book about the people of cyberspace, and distributing it in this way is the best way I know to actually make this information available, freely and easily, to all the people of cyberspace - including people far outside the borders of the United States, who otherwise may never have a chance to see any edition of the book, and who may perhaps learn something useful from this strange story of distant, obscure, but portentous events in so-called "American cyberspace."

This electronic book is now literary freeware. It now belongs to the emergent realm of alternative information economics. You have no right to make this electronic book part of the conventional flow of commerce. Let it be part of the flow of knowledge: there's a difference. I've divided the book into four sections, so that it is less ungainly for upload and download; if there's a section of particular relevance to you and your colleagues, feel free to reproduce that one and skip the rest. Just make more when you need them, and give them to whoever might want them.

Now have fun.

The Hacker Crackdown: Introduction.

This is a book about cops, and wild teenage whiz-kids, and lawyers, and hairy-eyed anarchists, and industrial technicians, and hippies, and high-tech millionaires, and game hobbyists, and computer security experts, and Secret Service agents, and grifters, and thieves. This book is about the electronic frontier of the 1990s. It concerns activities that take place inside computers and over telephone lines.

A science fiction writer coined the useful term "cyberspace" in 1982. But the territory in question, the electronic frontier, is about a hundred and thirty years old. Cyberspace is the "place" where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. The place between the phones. The indefinite place out there, where the two of you, two human beings, actually meet and communicate.

Although it is not exactly "real," "cyberspace" is a genuine place. Things happen there that have very genuine consequences. This "place" is not "real," but it is serious, it is earnest. Tens of thousands of people have dedicated their lives to it, to the public service of public communication by wire and electronics.

People have worked on this "frontier" for generations now. Some people became rich and famous from their efforts there. Some just played in it, as hobbyists. Others soberly pondered it, and wrote about it, and regulated it, and negotiated over it in international forums, and sued one another about it, in gigantic, epic court battles that lasted for years. And almost since the beginning, some people have committed crimes in this place.

But in the past twenty years, this electrical "space," which was once thin and dark and one-dimensional - little more than a narrow speaking-tube, stretching from phone to phone - has flung itself open like a gigantic jack-in-the-box. Light has flooded upon it, the eerie light of the glowing computer screen. This dark electric netherworld has become a vast flowering electronic landscape. Since the 1960s, the world of the telephone has cross-bred itself with computers and television, and though there is still no substance to cyberspace, nothing you can handle, it has a strange kind of physicality now. It makes good sense today to talk of cyberspace as a place all its own.

Because people live in it now. Not just a few people, not just a few technicians and eccentrics, but thousands of people, quite normal people. And not just for a little while, either, but for hours straight, over weeks, and months, and years. Cyberspace today is a "Net," a "Matrix," international in scope and growing swiftly and steadily. It's growing in size, and wealth, and political importance.

People are making entire careers in modern cyberspace. Scientists and technicians, of course; they've been there for twenty years now. But increasingly, cyberspace is filling with journalists and doctors and lawyers and artists and clerks. Civil servants make their careers there now, "on-line" in vast government databanks; and so do spies, industrial, political, and just plain snoops; and so do police, at least a few of them. And there are children living there now.

People have met there and been married there. There are entire living communities in cyberspace today; chattering, gossipping, planning, conferring and scheming, leaving one another voice-mail and electronic mail, giving one another big weightless chunks of valuable data, both legitimate and illegitimate. They busily pass one another computer software and the occasional festering computer virus.

We do not really understand how to live in cyberspace yet. We are feeling our way into it, blundering about. That is not surprising. Our lives in the physical world, the "real" world, are also far from perfect, despite a lot more practice. Human lives, real lives, are imperfect by their nature, and there are human beings in cyberspace. The way we live in cyberspace is a funhouse mirror of the way we live in the real world. We take both our advantages and our troubles with us.

This book is about trouble in cyberspace. Specifically, this book is about certain strange events in the year 1990, an unprecedented and startling year for the growing world of computerized communications.

In 1990 there came a nationwide crackdown on illicit computer hackers, with arrests, criminal charges, one dramatic show-trial, several guilty pleas, and huge confiscations of data and equipment all over the USA.

The Hacker Crackdown of 1990 was larger, better organized, more deliberate, and more resolute than any previous effort in the brave new world of computer crime. The U.S. Secret Service, private telephone security, and state and local law enforcement groups across the country all joined forces in a determined attempt to break the back of America's electronic underground. It was a fascinating effort, with very mixed results.

The Hacker Crackdown had another unprecedented effect; it spurred the creation, within "the computer community," of the Electronic Frontier Foundation, a new and very odd interest group, fiercely dedicated to the establishment and preservation of electronic civil liberties. The crackdown, remarkable in itself, has created a melee of debate over electronic crime, punishment, freedom of the press, and issues of search and seizure. Politics has entered cyberspace. Where people go, politics follow. This is the story of the people of cyberspace.

Part One: Crashing the System.

- A Brief History of Telephony
- Bell’s Golden Vaporware
- Universal Service
- Wild Boys and Wire Women
- The Electronic Communities
- The Ungentle Giant
- The Breakup
- In Defense of the System
- The Crash PostMortem
- Landslides in Cyberspace

On January 15, 1990, AT&T’s long-distance telephone switching system crashed.

This was a strange, dire, huge event. Sixty thousand people lost their telephone service completely. During the nine long hours of frantic effort that it took to restore service, some seventy million telephone calls went uncompleted.

Losses of service, known as “outages” in the telco trade, are a known and accepted hazard of the telephone business. Hurricanes hit, and phone cables get snapped by the thousands. Earthquakes wrench through buried fiber-optic lines. Switching stations catch fire and burn to the ground. These things do happen. There are contingency plans for them, and decades of experience in dealing with them. But the Crash of January 15 was unprecedented. It was unbelievably huge, and it occurred for no apparent physical reason.

The crash started on a Monday afternoon in a single switching-station in Manhattan. But, unlike any merely physical damage, it spread and spread. Station after station across America collapsed in a chain reaction, until fully half of AT&T’s network had gone haywire and the remaining half was hard-put to handle the overflow.

Within nine hours, AT&T software engineers more or less understood what had caused the crash. Replicating the problem exactly, poring over software line by line, took them a couple of weeks. But because it was hard to understand technically, the full truth of the matter and its implications were not widely and thoroughly aired and explained. The root cause of the crash remained obscure, surrounded by rumor and fear. The crash was a grave corporate embarrassment. The “culprit” was a bug in AT&T’s own software - not the sort of admission the telecommunications giant wanted to make, especially in the face of increasing competition. Still, the truth was told, in the baffling technical terms necessary to explain it.

Somehow the explanation failed to persuade American law enforcement officials and even telephone corporate security personnel. These people were not technical experts or software wizards, and they had their own suspicions about the cause of this disaster.

The police and telco security had important sources of information denied to mere software engineers. They had informants in the computer underground and years of experience in dealing with high-tech rascality that seemed to grow ever more sophisticated. For years they had been expecting a direct and savage attack against the American national telephone system. And with the Crash of January 15 - the first month of a new, high-tech decade - their predictions, fears, and suspicions seemed at last to have entered the real world. A world where the telephone system had not merely crashed, but, quite likely, been crashed - by “hackers.”

The crash created a large dark cloud of suspicion that would color certain people’s assumptions and actions for months. The fact that it took place in the realm of software was suspicious on its face. The fact that it occurred on

Martin Luther King Day, still the most politically touchy of American holidays, made it more suspicious yet.

The Crash of January 15 gave the Hacker Crackdown its sense of edge and its sweaty urgency. It made people, powerful people in positions of public authority, willing to believe the worst. And, most fatally, it helped to give investigators a willingness to take extreme measures and the determination to preserve almost total secrecy. An obscure software fault in an aging switching system in New York was to lead to a chain reaction of legal and constitutional trouble all across the country.

Like the crash in the telephone system, this chain reaction was ready and waiting to happen. During the 1980s, the American legal system was extensively patched to deal with the novel issues of computer crime. There was, for instance, the Electronic Communications Privacy Act of 1986 (eloquently described as "a stinking mess" by a prominent law enforcement official). And there was the draconian Computer Fraud and Abuse Act of 1986, passed unanimously by the United States Senate, which later would reveal a large number of flaws. Extensive, wellmeant efforts had been made to keep the legal system up to date. But in the day-to-day grind of the real world, even the most elegant software tends to crumble and suddenly reveal its hidden bugs.

Like the advancing telephone system, the American legal system was certainly not ruined by its temporary crash; but for those caught under the weight of the collapsing system, life became a series of blackouts and anomalies.

In order to understand why these weird events occurred, both in the world of technology and in the world of law, it's not enough to understand the merely technical problems. We will get to those; but first and foremost, we must try to understand the telephone, and the business of telephones, and the community of human beings that telephones have created.

-Section 1-

Technologies have life cycles, like cities do, like institutions do, like laws and governments do.

The first stage of any technology is the Question Mark, often known as the "Golden Vaporware" stage. At this early point, the technology is only a phantom, a mere gleam in the inventor's eye. One such inventor was a speech teacher and electrical tinkerer named Alexander Graham Bell.

Bell's early inventions, while ingenious, failed to move the world. In 1863, the teenage Bell and his brother Melville made an artificial talking mechanism out of wood, rubber, gutta-percha, and tin. This weird device had a rubber-covered "tongue" made of movable wooden segments, with vibrating rubber "vocal cords," and rubber "lips" and "cheeks." While Melville puffed a bellows into a tin tube, imitating the lungs, young Alec Bell would manipulate the "lips," "teeth," and "tongue," causing the thing to emit high-pitched falsetto gibberish.

Another would-be technical breakthrough was the Bell "phonautograph" of 1874, actually made out of a human cadaver's ear. Clamped into place on a tripod, this grisly gadget drew sound-wave images on smoked glass through a thin straw glued to its vibrating earbones.

By 1875, Bell had learned to produce audible sounds - ugly shrieks and squawks - by using magnets, diaphragms, and electrical current. Most "Golden Vaporware" technologies go nowhere.

But the second stage of technology is the Rising Star, or, the "Goofy Prototype," stage. The telephone, Bell's most ambitious gadget yet, reached this stage on March 10, 1876. On that great day, Alexander Graham Bell became the first person to transmit intelligible human speech electrically. As it happened, young Professor Bell, industriously tinkering in his Boston lab, had spattered his trousers with acid. His assistant, Mr. Watson, heard his cry for help - over Bell's experimental audiotelegraph. This was an event without precedent.

Technologies in their "Goofy Prototype" stage rarely work very well. They're experimental, and therefore halfbaked and rather frazzled. The proto-

type may be attractive and novel, and it does look as if it ought to be good for something-or-other. But nobody, including the inventor, is quite sure what. Inventors, and speculators, and pundits may have very firm ideas about its potential use, but those ideas are often very wrong.

The natural habitat of the Goofy Prototype is in trade shows and in the popular press. Infant technologies need publicity and investment money like a tottering calf need milk. This was very true of Bell's machine. To raise research and development money, Bell toured with his device as a stage attraction.

Contemporary press reports of the stage debut of the telephone showed pleased astonishment mixed with considerable dread. Bell's stage telephone was a large wooden box with a crude speaker-nozzle, the whole contraption about the size and shape of an overgrown Brownie camera. Its buzzing steel soundplate, pumped up by powerful electromagnets, was loud enough to fill an auditorium. Bell's assistant Mr. Watson, who could manage on the keyboards fairly well, kicked in by playing the organ from distant rooms, and, later, distant cities. This feat was considered marvellous, but very eerie indeed.

Bell's original notion for the telephone, an idea promoted for a couple of years, was that it would become a mass medium. We might recognize Bell's idea today as something close to modern "cable radio." Telephones at a central source would transmit music, Sunday sermons, and important public speeches to a paying network of wired-up subscribers.

At the time, most people thought this notion made good sense. In fact, Bell's idea was workable. In Hungary, this philosophy of the telephone was successfully put into everyday practice. In Budapest, for decades, from 1893 until after World War I, there was a government-run information service called "Telefon Hirmondo©." Hirmondo© was a centralized source of news and entertainment and culture, including stock reports, plays, concerts, and novels read aloud. At certain hours of the day, the phone would ring, you would plug in a loudspeaker for the use of the family, and Telefon Hirmondo© would be on the air - or rather, on the phone.

Hirmondo© is dead tech today, but Hirmondo© might be considered a spiritual ancestor of the modern telephone-accessed computer data services, such as CompuServe, GEnie or Prodigy. The principle behind Hirmondo© is also not too far from computer "bulletin board systems" or BBS's, which arrived in the late 1970s, spread rapidly across America, and will figure largely in this book.

We are used to using telephones for individual person-to-person speech, because we are used to the Bell system. But this was just one possibility among many. Communication networks are very flexible and protean, especially when their hardware becomes sufficiently advanced. They can be put to all kinds of uses. And they have been - and they will be.

Bell's telephone was bound for glory, but this was a combination of political decisions, canny infighting in court, inspired industrial leadership, receptive local conditions and outright good luck. Much the same is true of communications systems today.

As Bell and his backers struggled to install their newfangled system in the real world of nineteenth-century New England, they had to fight against skepticism and industrial rivalry. There was already a strong electrical communications network present in America: the telegraph. The head of the Western Union telegraph system dismissed Bell's prototype as "an electrical toy" and refused to buy the rights to Bell's patent. The telephone, it seemed, might be all right as a parlor entertainment - but not for serious business.

Telegrams, unlike mere telephones, left a permanent physical record of their messages. Telegrams, unlike telephones, could be answered whenever the recipient had time and convenience. And the telegram had a much longer distance-range than Bell's early telephone. These factors made telegraphy seem a much more sound and businesslike technology - at least to some.

The telegraph system was huge, and well-entrenched. In 1876, the United States had 214,000 miles of telegraph wire, and 8500 telegraph offices. There were specialized telegraphs for businesses and stock traders, government, police and fire departments. And Bell's "toy" was best known as a stage-magic musical device.

The third stage of technology is known as the "Cash Cow" stage. In the "cash cow" stage, a technology finds its place in the world, and matures, and becomes settled and productive. After a year or so, Alexander Graham Bell and his capitalist backers concluded that eerie music piped from nineteenth-century cyberspace was not the real selling-point of his invention. Instead, the telephone was about speech - individual, personal speech, the human voice, human conversation and human interaction. The telephone was not to be managed from any centralized broadcast center. It was to be a personal, intimate technology.

When you picked up a telephone, you were not absorbing the cold output of a machine - you were speaking to another human being. Once people realized this, their instinctive dread of the telephone as an eerie, unnatural device, swiftly vanished. A "telephone call" was not a "call" from a "telephone" itself, but a call from another human being, someone you would generally know and recognize. The real point was not what the machine could do for you (or to you), but what you yourself, a person and citizen, could do through the machine. This decision on the part of the young Bell Company was absolutely vital.

The first telephone networks went up around Boston - mostly among the technically curious and the well-to-do (much the same segment of the American populace that, a hundred years later, would be buying personal computers). Entrenched backers of the telegraph continued to scoff.

But in January 1878, a disaster made the telephone famous. A train crashed in Tarriffville, Connecticut. Forward-looking doctors in the nearby city of Hartford had had Bell's "speaking telephone" installed. An alert local druggist was able to telephone an entire community of local doctors, who rushed to the site to give aid. The disaster, as disasters do, aroused intense press coverage. The phone had proven its usefulness in the real world.

After Tarriffville, the telephone network spread like crabgrass. By 1890 it was all over New England. By '93, out to Chicago. By '97, into Minnesota, Nebraska and Texas. By 1904 it was all over the continent.

The telephone had become a mature technology. Professor Bell (now generally known as "Dr. Bell" despite his lack of a formal degree) became quite wealthy. He lost interest in the tedious day-to-day business muddle of the booming telephone network, and gratefully returned his attention to creatively hacking-around in his various laboratories, which were now much larger, better ventilated, and gratifyingly better-equipped. Bell was never to have another great inventive success, though his speculations and prototypes anticipated fiber-optic transmission, manned flight, sonar, hydrofoil ships, tetrahedral construction, and Montessori education. The "decibel," the standard scientific measure of sound intensity, was named after Bell.

Not all Bell's vaporware notions were inspired. He was fascinated by human eugenics. He also spent many years developing a weird personal system of astrophysics in which gravity did not exist.

Bell was a definite eccentric. He was something of a hypochondriac, and throughout his life he habitually stayed up until four A.M., refusing to rise before noon. But Bell had accomplished a great feat; he was an idol of millions and his influence, wealth, and great personal charm, combined with his eccentricity, made him something of a loose cannon on deck. Bell maintained a thriving scientific salon in his winter mansion in Washington, D.C., which gave him considerable backstage influence in governmental and scientific circles. He was a major financial backer of the magazines Science and National Geographic, both still flourishing today as important organs of the American scientific establishment. Bell's companion Thomas Watson, similarly wealthy and similarly odd, became the ardent political disciple of a 19th-century science-fiction writer and would-be social reformer, Edward Bellamy. Watson also trod the boards briefly as a Shakespearian actor.

There would never be another Alexander Graham Bell, but in years to come there would be surprising numbers of people like him. Bell was a prototype of the high-tech entrepreneur. High-tech entrepreneurs will play a very prominent role in this book: not merely as technicians and businessmen, but as pioneers of the technical frontier, who can carry the power and prestige they derive from high-technology into the political and social arena.

Like later entrepreneurs, Bell was fierce in defense of his own technological territory. As the telephone began to flourish, Bell was soon involved in violent lawsuits in the defense of his patents. Bell's Boston lawyers were excellent, however, and Bell himself, as an elecution teacher and gifted public speaker, was a devastatingly effective legal witness. In the eighteen years of Bell's patents, the Bell company was involved in six hundred separate lawsuits. The legal records printed filled 149 volumes. The Bell Company won every single suit.

After Bell's exclusive patents expired, rival telephone companies sprang up all over America. Bell's company, American Bell Telephone, was soon in deep trouble. In 1907, American Bell Telephone fell into the hands of the rather sinister J.P. Morgan financial cartel, robber-baron speculators who dominated Wall Street.

At this point, history might have taken a different turn. American might well have been served forever by a patchwork of locally owned telephone companies. Many state politicians and local businessmen considered this an excellent solution.

But the new Bell holding company, American Telephone and Telegraph or AT&T, put in a new man at the helm, a visionary industrialist named Theodore Vail. Vail, a former Post Office manager, understood large organizations and had an innate feeling for the nature of large-scale communications. Vail quickly saw to it that AT&T seized the technological edge once again. The Pupin and Campbell "loading coil," and the deForest "audion," are both extinct technology today, but in 1913 they gave Vail's company the best long-distance lines ever built. By controlling long-distance - the links between, and over, and above the smaller local phone companies - AT&T swiftly gained the whip-hand over them, and was soon devouring them right and left.

Vail plowed the profits back into research and development, starting the Bell tradition of huge-scale and brilliant industrial research.

Technically and financially, AT&T gradually steamrollered the opposition. Independent telephone companies never became entirely extinct, and hundreds of them flourish today. But Vail's AT&T became the supreme communications company. At one point, Vail's AT&T bought Western Union itself, the very company that had derided Bell's telephone as a "toy." Vail thoroughly reformed Western Union's hidebound business along his modern principles; but when the federal government grew anxious at this centralization of power, Vail politely gave Western Union back.

This centralizing process was not unique. Very similar events had happened in American steel, oil, and railroads. But AT&T, unlike the other companies, was to remain supreme. The monopoly robber-barons of those other industries were humbled and shattered by government trust-busting. Vail, the former Post Office official, was quite willing to accommodate the US government; in fact he would forge an active alliance with it. AT&T would become almost a wing of the American government, almost another Post Office - though not quite. AT&T would willingly submit to federal regulation, but in return, it would use the government's regulators as its own police, who would keep out competitors and assure the Bell system's profits and preeminence.

This was the second birth - the political birth - of the American telephone system. Vail's arrangement was to persist, with vast success, for many decades, until 1982. His system was an odd kind of American industrial socialism. It was born at about the same time as Leninist Communism, and it lasted almost as long - and, it must be admitted, to considerably better effect.

Vail's system worked. Except perhaps for aerospace, there has been no technology more thoroughly dominated by Americans than the telephone. The telephone was seen from the beginning as a quintessentially American technology. Bell's policy, and the policy of Theodore Vail, was a profoundly democratic policy of universal access. Vail's famous corporate slogan, "One Policy, One System, Universal Service," was a political slogan, with a very American ring to it. The American telephone was not to become the specialized tool of government or business, but a general public utility. At first, it was true, only the wealthy could afford private telephones, and Bell's company pursued the business markets primarily. The American phone system was a capitalist effort, meant to make money; it was not a charity. But from the first,

almost all communities with telephone service had public telephones. And many stores - especially drugstores - offered public use of their phones. You might not own a telephone - but you could always get into the system, if you really needed to.

There was nothing inevitable about this decision to make telephones "public" and "universal." Vail's system involved a profound act of trust in the public. This decision was a political one, informed by the basic values of the American republic. The situation might have been very different; and in other countries, under other systems, it certainly was.

Joseph Stalin, for instance, vetoed plans for a Soviet phone system soon after the Bolshevik revolution. Stalin was certain that publicly accessible telephones would become instruments of anti-Soviet counterrevolution and conspiracy. (He was probably right.) When telephones did arrive in the Soviet Union, they would be instruments of Party authority, and always heavily tapped. (Alexander Solzhenitsyn's prison-camp novel The First Circle describes efforts to develop a phone system more suited to Stalinist purposes.)

France, with its tradition of rational centralized government, had fought bitterly even against the electric telegraph, which seemed to the French entirely too anarchical and frivolous. For decades, nineteenth-century France communicated via the "visual telegraph," a nation-spanning, government-owned semaphore system of huge stone towers that signalled from hilltops, across vast distances, with big windmill-like arms. In 1846, one Dr. Barbay, a semaphore enthusiast, memorably uttered an early version of what might be called "the security expert's argument" against the open media.

"No, the electric telegraph is not a sound invention. It will always be at the mercy of the slightest disruption, wild youths, drunkards, bums, etc… The electric telegraph meets those destructive elements with only a few meters of wire over which supervision is impossible. A single man could, without being seen, cut the telegraph wires leading to Paris, and in twenty-four hours cut in ten different places the wires of the same line, without being arrested. The visual telegraph, on the contrary, has its towers, its high walls, its gates well-guarded from inside by strong armed men. Yes, I declare, substitution of the electric telegraph for the visual one is a dreadful measure, a truly idiotic act."

Dr. Barbay and his high-security stone machines were eventually unsuccessful, but his argument - that communication exists for the safety and convenience of the state, and must be carefully protected from the wild boys and the gutter rabble who might want to crash the system - would be heard again and again.

When the French telephone system finally did arrive, its snarled inadequacy was to be notorious. Devotees of the American Bell System often recommended a trip to France, for skeptics.

In Edwardian Britain, issues of class and privacy were a ball-and-chain for telephonic progress. It was considered outrageous that anyone - any wild fool off the street - could simply barge bellowing into one's office or home, preceded only by the ringing of a telephone bell. In Britain, phones were tolerated for the use of business, but private phones tended be stuffed away into closets, smoking rooms, or servants' quarters. Telephone operators were resented in Britain because they did not seem to "know their place." And no one of breeding would print a telephone number on a business card; this seemed a crass attempt to make the acquaintance of strangers.

But phone access in America was to become a popular right; something like universal suffrage, only more so. American women could not yet vote when the phone system came through; yet from the beginning American women doted on the telephone. This "feminization" of the American telephone was often commented on by foreigners. Phones in America were not censored or stiff or formalized; they were social, private, intimate, and domestic. In America, Mother's Day is by far the busiest day of the year for the phone network.

The early telephone companies, and especially AT&T, were among the foremost employers of American women. They employed the daughters of the American middle-class in great armies: in 1891, eight thousand women; by 1946, almost a quarter of a million. Women seemed to enjoy telephone work; it was respectable, it was steady, it paid fairly well as women's work went, and - not least

- it seemed a genuine contribution to the social good of the community. Women found Vail's ideal of public service attractive. This was especially true in rural areas, where women operators, running extensive rural partylines, enjoyed considerable social power. The operator knew everyone on the party-line, and everyone knew her.

Although Bell himself was an ardent suffragist, the telephone company did not employ women for the sake of advancing female liberation. AT&T did this for sound commercial reasons. The first telephone operators of the Bell system were not women, but teenage American boys. They were telegraphic messenger boys (a group about to be rendered technically obsolescent), who swept up around the phone office, dunned customers for bills, and made phone connections on the switchboard, all on the cheap.

Within the very first year of operation, 1878, Bell's company learned a sharp lesson about combining teenage boys and telephone switchboards. Putting teenage boys in charge of the phone system brought swift and consistent disaster. Bell's chief engineer described them as "Wild Indians." The boys were openly rude to customers. They talked back to subscribers, saucing off, uttering facetious remarks, and generally giving lip. The rascals took Saint Patrick's Day off without permission. And worst of all they played clever tricks with the switchboard plugs: disconnecting calls, crossing lines so that customers found themselves talking to strangers, and so forth.

This combination of power, technical mastery, and effective anonymity seemed to act like catnip on teenage boys.

This wild-kid-on-the-wires phenomenon was not confined to the USA; from the beginning, the same was true of the British phone system. An early British commentator kindly remarked: "No doubt boys in their teens found the work not a little irksome, and it is also highly probable that under the early conditions of employment the adventurous and inquisitive spirits of which the average healthy boy of that age is possessed, were not always conducive to the best attention being given to the wants of the telephone subscribers."

So the boys were flung off the system - or at least, deprived of control of the switchboard. But the "adventurous and inquisitive spirits" of the teenage boys would be heard from in the world of telephony, again and again.

The fourth stage in the technological life-cycle is death: "the Dog," dead tech. The telephone has so far avoided this fate. On the contrary, it is thriving, still spreading, still evolving, and at increasing speed.

The telephone has achieved a rare and exalted state for a technological artifact: it has become a household object. The telephone, like the clock, like pen and paper, like kitchen utensils and running water, has become a technology that is visible only by its absence. The telephone is technologically transparent. The global telephone system is the largest and most complex machine in the world, yet it is easy to use. More remarkable yet, the telephone is almost entirely physically safe for the user.

For the average citizen in the 1870s, the telephone was weirder, more shocking, more "high-tech" and harder to comprehend, than the most outrageous stunts of advanced computing for us Americans in the 1990s. In trying to understand what is happening to us today, with our bulletin board systems, direct overseas dialling, fiberoptic transmissions, computer viruses, hacking stunts, and a vivid tangle of new laws and new crimes, it is important to realize that our society has been through a similar challenge before - and that, all in all, we did rather well by it.

Bell's stage telephone seemed bizarre at first. But the sensations of weirdness vanished quickly, once people began to hear the familiar voices of relatives and friends, in their own homes on their own telephones. The telephone changed from a fearsome high-tech totem to an everyday pillar of human community.

This has also happened, and is still happening, to computer networks. Computer networks such as NSFnet, BITnet, USENET, JANET, are technically advanced, intimidating, and much harder to use than telephones. Even the popular, commercial computer networks, such as GEnie, Prodigy, and CompuServe, cause much head-scratching and have been described as "user-hateful." Nevertheless they too are changing from fancy high-tech items into everyday sources of human community.

The words "community" and "communication" have the same root. Wherever you put a communications network, you put a community as well. And whenever you take away that network - confiscate it, outlaw it, crash it, raise its price beyond affordability - then you hurt that community.

Communities will fight to defend themselves. People will fight harder and more bitterly to defend their communities, than they will fight to defend their own individual selves. And this is very true of the "electronic community" that arose around computer networks in the 1980s - or rather, the various electronic communities, in telephony, law enforcement, computing, and the digital underground that, by the year 1990, were raiding, rallying, arresting, suing, jailing, fining and issuing angry manifestos.

None of the events of 1990 were entirely new. Nothing happened in 1990 that did not have some kind of earlier and more understandable precedent. What gave the Hacker Crackdown its new sense of gravity and importance was the feeling - the community feeling - that the political stakes had been raised; that trouble in cyberspace was no longer mere mischief or inconclusive skirmishing, but a genuine fight over genuine issues, a fight for community survival and the shape of the future. These electronic communities, having flourished throughout the 1980s, were becoming aware of themselves, and increasingly, becoming aware of other, rival communities. Worries were sprouting up right and left, with complaints, rumors, uneasy speculations. But it would take a catalyst, a shock, to make the new world evident. Like Bell's great publicity break, the Tarriffville Rail Disaster of January 1878, it would take a cause celebre.

That cause was the AT&T Crash of January 15, 1990. After the Crash, the wounded and anxious telephone community would come out fighting hard.

-Section 2-

The community of telephone technicians, engineers, operators and researchers is the oldest community in cyberspace. These are the veterans, the most developed group, the richest, the most respectable, in most ways the most powerful. Whole generations have come and gone since Alexander Graham Bell's day, but the community he founded survives; people work for the phone system today whose great-grandparents worked for the phone system. Its specialty magazines, such as Telephony, AT&T Technical Journal, Telephone Engineer and Management, are decades old; they make computer publications like Macworld and PC Week look like amateur johnny-come-latelies.

And the phone companies take no back seat in hightechnology, either. Other companies' industrial researchers may have won new markets; but the researchers of Bell Labs have won seven Nobel Prizes. One potent device that Bell Labs originated, the transistor, has created entire groups of industries. Bell Labs are world-famous for generating "a patent a day," and have even made vital discoveries in astronomy, physics and cosmology.

Throughout its seventy-year history, "Ma Bell" was not so much a company as a way of life. Until the cataclysmic divestiture of the 1980s, Ma Bell was perhaps the ultimate maternalist mega-employer. The AT&T corporate image was the "gentle giant," "the voice with a smile," a vaguely socialist-realist world of cleanshaven linemen in shiny helmets and blandly pretty phone-girls in headsets and nylons. Bell System employees were famous as rock-ribbed Kiwanis and Rotary members, Little-League enthusiasts, school-board people.

During the long heyday of Ma Bell, the Bell employee corps were nurtured top-to-bottom on a corporate ethos of public service. There was good money in Bell, but Bell was not about money; Bell used public relations, but never mere marketeering. People went into the Bell System for a good life, and they had a good life. But it was not mere money that led Bell people out in the midst of storms and earthquakes to fight with toppled phone-poles, to wade in flooded manholes, to pull the redeyed graveyard-shift over collapsing switching-systems. The Bell ethic was the electrical equivalent of the postman's: neither rain, nor snow, nor gloom of night would stop these couriers.

It is easy to be cynical about this, as it is easy to be cynical about any political or social system; but cynicism does not change the fact that thousands of people took these ideals very seriously. And some still do.

The Bell ethos was about public service; and that was gratifying; but it was also about private power, and that was gratifying too. As a corporation, Bell was very special. Bell was privileged. Bell had snuggled up close to the state. In fact, Bell was as close to government as you could get in America and still make a whole lot of legitimate money.

But unlike other companies, Bell was above and beyond the vulgar commercial fray. Through its regional operating companies, Bell was omnipresent, local, and intimate, all over America; but the central ivory towers at its corporate heart were the tallest and the ivoriest around.

There were other phone companies in America, to be sure; the so-called independents. Rural cooperatives, mostly; small fry, mostly tolerated, sometimes warred upon.

For many decades, "independent" American phone companies lived in fear and loathing of the official Bell monopoly (or the "Bell Octopus," as Ma Bell's nineteenth-century enemies described her in many angry newspaper manifestos). Some few of these independent entrepreneurs, while legally in the wrong, fought so bitterly against the Octopus that their illegal phone networks were cast into the street by Bell agents and publicly burned.

The pure technical sweetness of the Bell System gave its operators, inventors and engineers a deeply satisfying sense of power and mastery. They had devoted their lives to improving this vast nation-spanning machine; over years, whole human lives, they had watched it improve and grow. It was like a great technological temple. They were an elite, and they knew it - even if others did not; in fact, they felt even more powerful because others did not understand. The deep attraction of this sensation of elite technical power should never be underestimated. "Technical power" is not for everybody; for many people it simply has no charm at all. But for some people, it becomes the core of their lives. For a few, it is overwhelming, obsessive; it becomes something close to an addiction. People - especially clever teenage boys whose lives are otherwise mostly powerless and put-upon - love this sensation of secret power, and are willing to do all sorts of amazing things to achieve it. The technical power of electronics has motivated many strange acts detailed in this book, which would otherwise be inexplicable.

So Bell had power beyond mere capitalism. The Bell service ethos worked, and was often propagandized, in a rather saccharine fashion. Over the decades, people slowly grew tired of this. And then, openly impatient with it. By the early 1980s, Ma Bell was to find herself with scarcely a real friend in the world. Vail's industrial socialism had become hopelessly out-of-fashion politically. Bell would be punished for that. And that punishment would fall harshly upon the people of the telephone community.

-Section 3-

In 1983, Ma Bell was dismantled by federal court action. The pieces of Bell are now separate corporate entities. The core of the company became AT&T Communications, and also AT&T Industries (formerly Western Electric, Bell's manufacturing arm). AT&T Bell Labs became Bell Communications Research, Bellcore. Then there are the Regional Bell Operating Companies, or RBOCs, pronounced "arbocks."

Bell was a titan and even these regional chunks are gigantic enterprises: Fortune 50 companies with plenty of wealth and power behind them. But the clean lines of "One Policy, One System, Universal Service" have been shattered, apparently forever.

The "One Policy" of the early Reagan Administration was to shatter a system that smacked of noncompetitive socialism. Since that time, there has been no real telephone "policy" on the federal level. Despite the breakup, the remnants of Bell have never been set free to compete in the open marketplace.

The RBOCs are still very heavily regulated, but not from the top. Instead, they struggle politically, economically and legally, in what seems an endless

turmoil, in a patchwork of overlapping federal and state jurisdictions. Increasingly, like other major American corporations, the RBOCs are becoming multinational, acquiring important commercial interests in Europe, Latin America, and the Pacific Rim. But this, too, adds to their legal and political predicament.

The people of what used to be Ma Bell are not happy about their fate. They feel ill-used. They might have been grudgingly willing to make a full transition to the free market; to become just companies amid other companies. But this never happened. Instead, AT&T and the RBOCS ("the Baby Bells") feel themselves wrenched from side to side by state regulators, by Congress, by the FCC, and especially by the federal court of Judge Harold Greene, the magistrate who ordered the Bell breakup and who has been the de facto czar of American telecommunications ever since 1983.

Bell people feel that they exist in a kind of paralegal limbo today. They don't understand what's demanded of them. If it's "service," why aren't they treated like a public service? And if it's money, then why aren't they free to compete for it? No one seems to know, really. Those who claim to know keep changing their minds. Nobody in authority seems willing to grasp the nettle for once and all.

Telephone people from other countries are amazed by the American telephone system today. Not that it works so well; for nowadays even the French telephone system works, more or less. They are amazed that the American telephone system still works at all, under these strange conditions.

Bell's "One System" of long-distance service is now only about eighty percent of a system, with the remainder held by Sprint, MCI, and the midget long-distance companies. Ugly wars over dubious corporate practices such as "slamming" (an underhanded method of snitching clients from rivals) break out with some regularity in the realm of long-distance service. The battle to break Bell's long-distance monopoly was long and ugly, and since the breakup the battlefield has not become much prettier. AT&T's famous shame-and-blame advertisements, which emphasized the shoddy work and purported ethical shadiness of their competitors, were much remarked on for their studied psychological cruelty. There is much bad blood in this industry, and much long-treasured resentment. AT&T's post-breakup corporate logo, a striped sphere, is known in the industry as the "Death Star" (a reference from the movie Star Wars, in which the "Death Star" was the spherical hightech fortress of the harsh-breathing imperial ultra-baddie, Darth Vader.) Even AT&T employees are less than thrilled by the Death Star. A popular (though banned) T-shirt among AT&T employees bears the old-fashioned Bell logo of the Bell System, plus the new-fangled striped sphere, with the before-and-after comments: "This is your brain - This is your brain on drugs!" AT&T made a very well-financed and determined effort to break into the personal computer market; it was disastrous, and telco computer experts are derisively known by their competitors as "the pole-climbers." AT&T and the Baby Bell arbocks still seem to have few friends. Under conditions of sharp commercial competition, a crash like that of January 15, 1990 was a major embarrassment to AT&T. It was a direct blow against their much-treasured reputation for reliability. Within days of the crash AT&T's Chief Executive Officer, Bob Allen, officially apologized, in terms of deeply pained humility: "AT&T had a major service disruption last Monday. We didn't live up to our own standards of quality, and we didn't live up to yours. It's as simple as that. And that's not acceptable to us. Or to you… We understand how much people have come to depend upon AT&T service, so our AT&T Bell Laboratories scientists and our network engineers are doing everything possible to guard against a recurrence… We know there's no way to make up for the inconvenience this problem may have caused you."

Mr Allen's "open letter to customers" was printed in lavish ads all over the country: in the Wall Street Journal, USA Today, New York Times, Los Angeles Times, Chicago Tribune, Philadelphia Inquirer, San Francisco Chronicle Examiner, Boston Globe, Dallas Morning News, Detroit Free Press, Washington Post, Houston Chronicle, Cleveland Plain Dealer, Atlanta Journal Constitution, Minneapolis Star Tribune, St. Paul Pioneer Press Dispatch, Seattle Times/Post Intelligencer, Tacoma News Tribune, Miami Herald, Pittsburgh Press, St. Louis Post Dispatch, Denver Post, Phoenix Republic Gazette and Tampa Tribune.

In another press release, AT&T went to some pains to suggest that this "software glitch" might have happened just as easily to MCI, although, in fact, it hadn't. (MCI's switching software was quite different from AT&T's - though not necessarily any safer.) AT&T also announced their plans to offer a rebate of service on Valentine's Day to make up for the loss during the Crash.

"Every technical resource available, including Bell Labs scientists and engineers, has been devoted to assuring it will not occur again," the public was told. They were further assured that "The chances of a recurrence are small - a problem of this magnitude never occurred before."

In the meantime, however, police and corporate security maintained their own suspicions about "the chances of recurrence" and the real reason why a "problem of this magnitude" had appeared, seemingly out of nowhere. Police and security knew for a fact that hackers of unprecedented sophistication were illegally entering, and reprogramming, certain digital switching stations. Rumors of hidden "viruses" and secret "logic bombs" in the switches ran rampant in the underground, with much chortling over AT&T's predicament, and idle speculation over what unsung hacker genius was responsible for it. Some hackers, including police informants, were trying hard to finger one another as the true culprits of the Crash.

Telco people found little comfort in objectivity when they contemplated these possibilities. It was just too close to the bone for them; it was embarrassing; it hurt so much; it was hard even to talk about.

There has always been thieving and misbehavior in the phone system. There has always been trouble with the rival independents, and in the local loops. But to have such trouble in the core of the system, the long-distance switching stations, is a horrifying affair. To telco people, this is all the difference between finding roaches in your kitchen and big horrid sewer-rats in your bedroom.

From the outside, to the average citizen, the telcos still seem gigantic and impersonal. The American public seems to regard them as something akin to Soviet apparats. Even when the telcos do their best corporatecitizen routine, subsidizing magnet high-schools and sponsoring news-shows on public television, they seem to win little except public suspicion.

But from the inside, all this looks very different. There's harsh competition. A legal and political system that seems baffled and bored, when not actively hostile to telco interests. There's a loss of morale, a deep sensation of having somehow lost the upper hand. Technological change has caused a loss of data and revenue to other, newer forms of transmission. There's theft, and new forms of theft, of growing scale and boldness and sophistication. With all these factors, it was no surprise to see the telcos, large and small, break out in a litany of bitter complaint.

In late '88 and throughout 1989, telco representatives grew shrill in their complaints to those few American law enforcement officials who make it their business to try to understand what telephone people are talking about. Telco security officials had discovered the computerhacker underground, infiltrated it thoroughly, and become deeply alarmed at its growing expertise. Here they had found a target that was not only loathsome on its face, but clearly ripe for counterattack.

Those bitter rivals: AT&T, MCI and Sprint - and a crowd of Baby Bells: PacBell, Bell South, Southwestern Bell, NYNEX, USWest, as well as the Bell research consortium Bellcore, and the independent long-distance carrier Mid-American - all were to have their role in the great hacker dragnet of 1990. After years of being battered and pushed around, the telcos had, at least in a small way, seized the initiative again. After years of turmoil, telcos and government officials were once again to work smoothly in concert in defense of the System. Optimism blossomed; enthusiasm grew on all sides; the prospective taste of vengeance was sweet.

-Section 4-

From the beginning - even before the crackdown had a name - secrecy was a big problem. There were many good reasons for secrecy in the hacker crackdown.

Hackers and code-thieves were wily prey, slinking back to their bedrooms and basements and destroying vital incriminating evidence at the first hint of trouble. Furthermore, the crimes themselves were heavily technical and difficult to describe, even to police - much less to the general public.

When such crimes had been described intelligibly to the public, in the past, that very publicity had tended to increase the crimes enormously. Telco officials, while painfully aware of the vulnerabilities of their systems, were anxious not to publicize those weaknesses. Experience showed them that those weaknesses, once discovered, would be pitilessly exploited by tens of thousands of people - not only by professional grifters and by underground hackers and phone phreaks, but by many otherwise more-or-less honest everyday folks, who regarded stealing service from the faceless, soulless "Phone Company" as a kind of harmless indoor sport. When it came to protecting their interests, telcos had long since given up on general public sympathy for "the Voice with a Smile." Nowadays the telco's "Voice" was very likely to be a computer's; and the American public showed much less of the proper respect and gratitude due the fine public service bequeathed them by Dr. Bell and Mr. Vail. The more efficient, high-tech, computerized, and impersonal the telcos became, it seemed, the more they were met by sullen public resentment and amoral greed.

Telco officials wanted to punish the phone-phreak underground, in as public and exemplary a manner as possible. They wanted to make dire examples of the worst offenders, to seize the ringleaders and intimidate the small fry, to discourage and frighten the wacky hobbyists, and send the professional grifters to jail. To do all this, publicity was vital.

Yet operational secrecy was even more so. If word got out that a nationwide crackdown was coming, the hackers might simply vanish; destroy the evidence, hide their computers, go to earth, and wait for the campaign to blow over. Even the young hackers were crafty and suspicious, and as for the professional grifters, they tended to split for the nearest state-line at the first sign of trouble. For the crackdown to work well, they would all have to be caught red-handed, swept upon suddenly, out of the blue, from every corner of the compass. And there was another strong motive for secrecy. In the worst-case scenario, a blown campaign might leave the telcos open to a devastating hacker counter-attack. If there were indeed hackers loose in America who had caused the January 15 Crash - if there were truly gifted hackers, loose in the nation's long-distance switching systems, and enraged or frightened by the crackdown - then they might react unpredictably to an attempt to collar them. Even if caught, they might have talented and vengeful friends still running around loose. Conceivably, it could turn ugly. Very ugly. In fact, it was hard to imagine just how ugly things might turn, given that possibility. Counter-attack from hackers was a genuine concern for the telcos. In point of fact, they would never suffer any such counter-attack. But in months to come, they would be at some pains to publicize this notion and to utter grim warnings about it.

Still, that risk seemed well worth running. Better to run the risk of vengeful attacks, than to live at the mercy of potential crashers. Any cop would tell you that a protection racket had no real future.

And publicity was such a useful thing. Corporate security officers, including telco security, generally work under conditions of great discretion. And corporate security officials do not make money for their companies. Their job is to prevent the loss of money, which is much less glamorous than actually winning profits. If you are a corporate security official, and you do your job brilliantly, then nothing bad happens to your company at all. Because of this, you appear completely superfluous. This is one of the many unattractive aspects of security work. It's rare that these folks have the chance to draw some healthy attention to their own efforts.

Publicity also served the interest of their friends in law enforcement. Public officials, including law enforcement officials, thrive by attracting favorable public interest. A brilliant prosecution in a matter of vital public interest can make the career of a prosecuting attorney. And for a police officer, good publicity opens the purses of the legislature; it may bring a citation, or a promotion, or at least a rise in status and the respect of one's peers.

But to have both publicity and secrecy is to have one's cake and eat it too. In months to come, as we will show, this impossible act was to cause great pain to the agents of the crackdown. But early on, it seemed possible - maybe even likely - that the crackdown could successfully combine the best of both worlds. The arrest of hackers would be heavily publicized. The actual deeds of the hackers, which were technically hard to explain and also a security risk, would be left decently obscured. The threat hackers posed would be heavily trumpeted; the likelihood of their actually committing such fearsome crimes would be left to the public's imagination. The spread of the computer underground, and its growing technical sophistication, would be heavily promoted; the actual hackers themselves, mostly bespectacled middle-class white suburban teenagers, would be denied any personal publicity.

It does not seem to have occurred to any telco official that the hackers accused would demand a day in court; that journalists would smile upon the hackers as "good copy;" that wealthy high-tech entrepreneurs would offer moral and financial support to crackdown victims; that constitutional lawyers would show up with briefcases, frowning mightily. This possibility does not seem to have ever entered the game-plan.

And even if it had, it probably would not have slowed the ferocious pursuit of a stolen phone-company document, mellifluously known as "Control Office Administration of Enhanced 911 Services for Special Services and Major Account Centers."

In the chapters to follow, we will explore the worlds of police and the computer underground, and the large shadowy area where they overlap. But first, we must explore the battleground. Before we leave the world of the telcos, we must understand what a switching system actually is and how your telephone actually works.

-Section 5-

To the average citizen, the idea of the telephone is represented by, well, a telephone: a device that you talk into.

To a telco professional, however, the telephone itself is known, in lordly fashion, as a "subset." The "subset" in your house is a mere adjunct, a distant nerve ending, of the central switching stations, which are ranked in levels of hierarchy, up to the long-distance electronic switching stations, which are some of the largest computers on earth. Let us imagine that it is, say, 1925, before the introduction of computers, when the phone system was simpler and somewhat easier to grasp. Let's further imagine that you are Miss Leticia Luthor, a fictional operator for Ma Bell in New York City of the 20s. Basically, you, Miss Luthor, are the "switching system." You are sitting in front of a large vertical switchboard, known as a "cordboard," made of shiny wooden panels, with ten thousand metal-rimmed holes punched in them, known as jacks. The engineers would have put more holes into your switchboard, but ten thousand is as many as you can reach without actually having to get up out of your chair.

Each of these ten thousand holes has its own little electric lightbulb, known as a "lamp," and its own neatly printed number code.

With the ease of long habit, you are scanning your board for lit-up bulbs. This is what you do most of the time, so you are used to it.

A lamp lights up. This means that the phone at the end of that line has been taken off the hook. Whenever a handset is taken off the hook, that closes a circuit inside the phone which then signals the local office, i.e. you, automatically. There might be somebody calling, or then again the phone might be simply off the hook, but this does not matter to you yet. The first thing you do, is record that number in your logbook, in your fine American public-school handwriting. This comes first, naturally, since it is done for billing purposes.

You now take the plug of your answering cord, which goes directly to your headset, and plug it into the lit-up hole. "Operator," you announce.

In operator's classes, before taking this job, you have been issued a large pamphlet full of canned operator's responses for all kinds of contingen-

cies, which you had to memorize. You have also been trained in a proper nonregional, non-ethnic pronunciation and tone of voice. You rarely have the occasion to make any spontaneous remark to a customer, and in fact this is frowned upon (except out on the rural lines where people have time on their hands and get up to all kinds of mischief).

A tough-sounding user's voice at the end of the line gives you a number. Immediately, you write that number down in your logbook, next to the caller's number, which you just wrote earlier. You then look and see if the number this guy wants is in fact on your switchboard, which it generally is, since it's generally a local call. Long distance costs so much that people use it sparingly.

Only then do you pick up a calling-cord from a shelf at the base of the switchboard. This is a long elastic cord mounted on a kind of reel so that it will zip back in when you unplug it. There are a lot of cords down there, and when a bunch of them are out at once they look like a nest of snakes. Some of the girls think there are bugs living in those cable-holes. They're called "cable mites" and are supposed to bite your hands and give you rashes. You don't believe this, yourself.

Gripping the head of your calling-cord, you slip the tip of it deftly into the sleeve of the jack for the called person. Not all the way in, though. You just touch it. If you hear a clicking sound, that means the line is busy and you can't put the call through. If the line is busy, you have to stick the calling-cord into a "busy-tone jack," which will give the guy a busy-tone. This way you don't have to talk to him yourself and absorb his natural human frustration.

But the line isn't busy. So you pop the cord all the way in. Relay circuits in your board make the distant phone ring, and if somebody picks it up off the hook, then a phone conversation starts. You can hear this conversation on your answering cord, until you unplug it. In fact you could listen to the whole conversation if you wanted, but this is sternly frowned upon by management, and frankly, when you've overheard one, you've pretty much heard 'em all.

You can tell how long the conversation lasts by the glow of the calling-cord's lamp, down on the calling-cord's shelf. When it's over, you unplug and the calling-cord zips back into place.

Having done this stuff a few hundred thousand times, you become quite good at it. In fact you're plugging, and connecting, and disconnecting, ten, twenty, forty cords at a time. It's a manual handicraft, really, quite satisfying in a way, rather like weaving on an upright loom.

Should a long-distance call come up, it would be different, but not all that different. Instead of connecting the call through your own local switchboard, you have to go up the hierarchy, onto the long-distance lines, known as "trunklines." Depending on how far the call goes, it may have to work its way through a whole series of operators, which can take quite a while. The caller doesn't wait on the line while this complex process is negotiated across the country by the gaggle of operators. Instead, the caller hangs up, and you call him back yourself when the call has finally worked its way through.

After four or five years of this work, you get married, and you have to quit your job, this being the natural order of womanhood in the American 1920s. The phone company has to train somebody else - maybe two people, since the phone system has grown somewhat in the meantime. And this costs money.

In fact, to use any kind of human being as a switching system is a very expensive proposition. Eight thousand Leticia Luthors would be bad enough, but a quarter of a million of them is a military-scale proposition and makes drastic measures in automation financially worthwhile.

Although the phone system continues to grow today, the number of human beings employed by telcos has been dropping steadily for years. Phone "operators" now deal with nothing but unusual contingencies, all routine operations having been shrugged off onto machines. Consequently, telephone operators are considerably less machine-like nowadays, and have been known to have accents and actual character in their voices. When you reach a human operator today, the operators are rather more "human" than they were in Leticia's day - but on

the other hand, human beings in the phone system are much harder to reach in the first place.

Over the first half of the twentieth century, "electromechanical" switching systems of growing complexity were cautiously introduced into the phone system. In certain backwaters, some of these hybrid systems are still in use. But after 1965, the phone system began to go completely electronic, and this is by far the dominant mode today. Electromechanical systems have "crossbars," and "brushes," and other large moving mechanical parts, which, while faster and cheaper than Leticia, are still slow, and tend to wear out fairly quickly.

But fully electronic systems are inscribed on silicon chips, and are lightning-fast, very cheap, and quite durable. They are much cheaper to maintain than even the best electromechanical systems, and they fit into half the space. And with every year, the silicon chip grows smaller, faster, and cheaper yet. Best of all, automated electronics work around the clock and don't have salaries or health insurance.

There are, however, quite serious drawbacks to the use of computer-chips. When they do break down, it is a daunting challenge to figure out what the heck has gone wrong with them. A broken cordboard generally had a problem in it big enough to see. A broken chip has invisible, microscopic faults. And the faults in bad software can be so subtle as to be practically theological. If you want a mechanical system to do something new, then you must travel to where it is, and pull pieces out of it, and wire in new pieces. This costs money. However, if you want a chip to do something new, all you have to do is change its software, which is easy, fast and dirt-cheap. You don't even have to see the chip to change its program. Even if you did see the chip, it wouldn't look like much. A chip with program X doesn't look one whit different from a chip with program Y. With the proper codes and sequences, and access to specialized phone-lines, you can change electronic switching systems all over America from anywhere you please.

And so can other people. If they know how, and if they want to, they can sneak into a microchip via the special phonelines and diddle with it, leaving no physical trace at all. If they broke into the operator's station and held Leticia at gunpoint, that would be very obvious. If they broke into a telco building and went after an electromechanical switch with a toolbelt, that would at least leave many traces. But people can do all manner of amazing things to computer switches just by typing on a keyboard, and keyboards are everywhere today. The extent of this vulnerability is deep, dark, broad, almost mind-boggling, and yet this is a basic, primal fact of life about any computer on a network.

Security experts over the past twenty years have insisted, with growing urgency, that this basic vulnerability of computers represents an entirely new level of risk, of unknown but obviously dire potential to society. And they are right.

An electronic switching station does pretty much everything Letitia did, except in nanoseconds and on a much larger scale. Compared to Miss Luthor's ten thousand jacks, even a primitive 1ESS switching computer, 60s vintage, has a 128,000 lines. And the current AT&T system of choice is the monstrous fifth-generation 5ESS.

An Electronic Switching Station can scan every line on its "board" in a tenth of a second, and it does this over and over, tirelessly, around the clock. Instead of eyes, it uses "ferrod scanners" to check the condition of local lines and trunks. Instead of hands, it has "signal distributors," "central pulse distributors," "magnetic latching relays," and "reed switches," which complete and break the calls. Instead of a brain, it has a "central processor." Instead of an instruction manual, it has a program. Instead of a handwritten logbook for recording and billing calls, it has magnetic tapes. And it never has to talk to anybody. Everything a customer might say to it is done by punching the direct-dial tone buttons on your subset.

Although an Electronic Switching Station can't talk, it does need an interface, some way to relate to its, er, employers. This interface is known as the "master control center." (This interface might be better known simply as "the interface," since it doesn't actually "control" phone calls directly. However, a term like "Master Control Center" is just the kind of rhetoric that

telco maintenance engineers - and hackers - find particularly satisfying.) Using the master control center, a phone engineer can test local and trunk lines for malfunctions. He (rarely she) can check various alarm displays, measure traffic on the lines, examine the records of telephone usage and the charges for those calls, and change the programming.

And, of course, anybody else who gets into the master control center by remote control can also do these things, if he (rarely she) has managed to figure them out, or, more likely, has somehow swiped the knowledge from people who already know.

In 1989 and 1990, one particular RBOC, BellSouth, which felt particularly troubled, spent a purported $1.2 million on computer security. Some think it spent as much as two million, if you count all the associated costs. Two million dollars is still very little compared to the great cost-saving utility of telephonic computer systems.

Unfortunately, computers are also stupid. Unlike human beings, computers possess the truly profound stupidity of the inanimate.

In the 1960s, in the first shocks of spreading computerization, there was much easy talk about the stupidity of computers - how they could "only follow the program" and were rigidly required to do "only what they were told." There has been rather less talk about the stupidity of computers since they began to achieve grandmaster status in chess tournaments, and to manifest many other impressive forms of apparent cleverness.

Nevertheless, computers still are profoundly brittle and stupid; they are simply vastly more subtle in their stupidity and brittleness. The computers of the 1990s are much more reliable in their components than earlier computer systems, but they are also called upon to do far more complex things, under far more challenging conditions.

On a basic mathematical level, every single line of a software program offers a chance for some possible screwup. Software does not sit still when it works; it "runs," it interacts with itself and with its own inputs and outputs. By analogy, it stretches like putty into millions of possible shapes and conditions, so many shapes that they can never all be successfully tested, not even in the lifespan of the universe. Sometimes the putty snaps.

The stuff we call "software" is not like anything that human society is used to thinking about. Software is something like a machine, and something like mathematics, and something like language, and something like thought, and art, and information… but software is not in fact any of those other things. The protean quality of software is one of the great sources of its fascination. It also makes software very powerful, very subtle, very unpredictable, and very risky.

Some software is bad and buggy. Some is "robust," even "bulletproof." The best software is that which has been tested by thousands of users under thousands of different conditions, over years. It is then known as "stable." This does not mean that the software is now flawless, free of bugs. It generally means that there are plenty of bugs in it, but the bugs are well-identified and fairly well understood.

There is simply no way to assure that software is free of flaws. Though software is mathematical in nature, it cannot be "proven" like a mathematical theorem; software is more like language, with inherent ambiguities, with different definitions, different assumptions, different levels of meaning that can conflict.

Human beings can manage, more or less, with human language because we can catch the gist of it.

Computers, despite years of effort in "artificial intelligence," have proven spectacularly bad in "catching the gist" of anything at all. The tiniest bit of semantic grit may still bring the mightiest computer tumbling down. One of the most hazardous things you can do to a computer program is try to improve it - to try to make it safer. Software "patches" represent new, untried un"stable" software, which is by definition riskier.

The modern telephone system has come to depend, utterly and irretrievably, upon software. And the System Crash of January 15, 1990, was caused by an improvement in software. Or rather, an attempted improvement.

As it happened, the problem itself - the problem per se - took this form. A piece of telco software had been written in C language, a standard language of the telco field. Within the C software was a long "do… while" construct. The "do… while" construct contained a "switch" statement. The "switch" statement contained an "if" clause. The "if" clause contained a "break." The "break" was supposed to "break" the "if" clause. Instead, the "break" broke the "switch" statement.

That was the problem, the actual reason why people picking up phones on January 15, 1990, could not talk to one another.

Or at least, that was the subtle, abstract, cyberspatial seed of the problem. This is how the problem manifested itself from the realm of programming into the realm of real life.

The System 7 software for AT&T's 4ESS switching station, the "Generic 44E14 Central Office Switch Software," had been extensively tested, and was considered very stable. By the end of 1989, eighty of AT&T's switching systems nationwide had been programmed with the new software. Cautiously, thirty four stations were left to run the slower, less-capable System 6, because AT&T suspected there might be shakedown problems with the new and unprecedently sophisticated System 7 network.

The stations with System 7 were programmed to switch over to a backup net in case of any problems. In mid-December 1989, however, a new high-velocity, high security software patch was distributed to each of the 4ESS switches that would enable them to switch over even more quickly, making the System 7 network that much more secure.

Unfortunately, every one of these 4ESS switches was now in possession of a small but deadly flaw.

In order to maintain the network, switches must monitor the condition of other switches - whether they are up and running, whether they have temporarily shut down, whether they are overloaded and in need of assistance, and so forth. The new software helped control this bookkeeping function by monitoring the status calls from other switches.

It only takes four to six seconds for a troubled 4ESS switch to rid itself of all its calls, drop everything temporarily, and re-boot its software from scratch. Starting over from scratch will generally rid the switch of any software problems that may have developed in the course of running the system. Bugs that arise will be simply wiped out by this process. It is a clever idea. This process of automatically re-booting from scratch is known as the "normal fault recovery routine." Since AT&T's software is in fact exceptionally stable, systems rarely have to go into "fault recovery" in the first place; but AT&T has always boasted of its "real world" reliability, and this tactic is a belt-and-suspenders routine.

The 4ESS switch used its new software to monitor its fellow switches as they recovered from faults. As other switches came back on line after recovery, they would send their "OK" signals to the switch. The switch would make a little note to that effect in its "status map," recognizing that the fellow switch was back and ready to go, and should be sent some calls and put back to regular work.

Unfortunately, while it was busy bookkeeping with the status map, the tiny flaw in the brand-new software came into play. The flaw caused the 4ESS switch to interacted, subtly but drastically, with incoming telephone calls from human users. If - and only if - two incoming phone-calls happened to hit the switch within a hundredth of a second, then a small patch of data would be garbled by the flaw.

But the switch had been programmed to monitor itself constantly for any possible damage to its data. When the switch perceived that its data had been somehow garbled, then it too would go down, for swift repairs to its software. It would signal its fellow switches not to send any more work. It would go into the fault recovery mode for four to six seconds. And then the switch would be fine again, and would send out its "OK, ready for work" signal.

However, the "OK, ready for work" signal was the very thing that had caused the switch to go down in the first place. And all the System 7 switches had the same flaw in their status-map software. As soon as they stopped to make the bookkeeping note that their fellow switch was "OK," then they too

would become vulnerable to the slight chance that two phone-calls would hit them within a hundredth of a second.

At approximately 2:25 p.m. EST on Monday, January 15, one of AT&T's 4ESS toll switching systems in New York City had an actual, legitimate, minor problem. It went into fault recovery routines, announced "I'm going down," then announced, "I'm back, I'm OK." And this cheery message then blasted throughout the network to many of its fellow 4ESS switches. Many of the switches, at first, completely escaped trouble. These lucky switches were not hit by the coincidence of two phone calls within a hundredth of a second. Their software did not fail - at first. But three switches - in Atlanta, St. Louis, and Detroit - were unlucky, and were caught with their hands full. And they went down. And they came back up, almost immediately. And they too began to broadcast the lethal message that they, too, were "OK" again, activating the lurking software bug in yet other switches.

As more and more switches did have that bit of bad luck and collapsed, the call-traffic became more and more densely packed in the remaining switches, which were groaning to keep up with the load. And of course, as the calls became more densely packed, the switches were much more likely to be hit twice within a hundredth of a second. It only took four seconds for a switch to get well. There was no physical damage of any kind to the switches, after all. Physically, they were working perfectly. This situation was "only" a software problem. But the 4ESS switches were leaping up and down every four to six seconds, in a virulent spreading wave all over America, in utter, manic, mechanical stupidity. They kept knocking one another down with their contagious "OK" messages. It took about ten minutes for the chain reaction to cripple the network. Even then, switches would periodically luck-out and manage to resume their normal work. Many calls - millions of them - were managing to get through. But millions weren't.

The switching stations that used System 6 were not directly affected. Thanks to these old-fashioned switches, AT&T's national system avoided complete collapse. This fact also made it clear to engineers that System 7 was at fault.

Bell Labs engineers, working feverishly in New Jersey, Illinois, and Ohio, first tried their entire repertoire of standard network remedies on the malfunctioning System 7. None of the remedies worked, of course, because nothing like this had ever happened to any phone system before.

By cutting out the backup safety network entirely, they were able to reduce the frenzy of "OK" messages by about half. The system then began to recover, as the chain reaction slowed. By 11:30 pm on Monday January 15, sweating engineers on the midnight shift breathed a sigh of relief as the last switch cleared-up.

By Tuesday they were pulling all the brand-new 4ESS software and replacing it with an earlier version of System 7. If these had been human operators, rather than computers at work, someone would simply have eventually stopped screaming. It would have been obvious that the situation was not "OK," and common sense would have kicked in. Humans possess common sense - at least to some extent. Computers simply don't. On the other hand, computers can handle hundreds of calls per second. Humans simply can't. If every single human being in America worked for the phone company, we couldn't match the performance of digital switches: direct-dialling, three-way calling, speed-calling, callwaiting, Caller ID, all the rest of the cornucopia of digital bounty. Replacing computers with operators is simply not an option any more.

And yet we still, anachronistically, expect humans to be running our phone system. It is hard for us to understand that we have sacrificed huge amounts of initiative and control to senseless yet powerful machines. When the phones fail, we want somebody to be responsible. We want somebody to blame.

When the Crash of January 15 happened, the American populace was simply not prepared to understand that enormous landslides in cyberspace, like the Crash itself, can happen, and can be nobody's fault in particular. It was easier to believe, maybe even in some odd way more reassuring to believe, that some evil person, or evil group, had done this to us. "Hackers" had done it. With a virus. A trojan horse. A software bomb. A dirty plot of some kind.

People believed this, responsible people. In 1990, they were looking hard for evidence to confirm their heartfelt suspicions.

And they would look in a lot of places. Come 1991, however, the outlines of an apparent new reality would begin to emerge from the fog.

On July 1 and 2, 1991, computer-software collapses in telephone switching stations disrupted service in Washington DC, Pittsburgh, Los Angeles and San Francisco. Once again, seemingly minor maintenance problems had crippled the digital System 7. About twelve million people were affected in the Crash of July 1, 1991.

Said the New York Times Service: "Telephone company executives and federal regulators said they were not ruling out the possibility of sabotage by computer hackers, but most seemed to think the problems stemmed from some unknown defect in the software running the networks."

And sure enough, within the week, a red-faced software company, DSC Communications Corporation of Plano, Texas, owned up to "glitches" in the "signal transfer point" software that DSC had designed for Bell Atlantic and Pacific Bell. The immediate cause of the July 1 Crash was a single mistyped character: one tiny typographical flaw in one single line of the software. One mistyped letter, in one single line, had deprived the nation's capital of phone service. It was not particularly surprising that this tiny flaw had escaped attention: a typical System 7 station requires ten million lines of code.

On Tuesday, September 17, 1991, came the most spectacular outage yet. This case had nothing to do with software failures - at least, not directly. Instead, a group of AT&T's switching stations in New York City had simply run out of electrical power and shut down cold. Their back-up batteries had failed. Automatic warning systems were supposed to warn of the loss of battery power, but those automatic systems had failed as well.

This time, Kennedy, La Guardia, and Newark airports all had their voice and data communications cut. This horrifying event was particularly ironic, as attacks on airport computers by hackers had long been a standard nightmare scenario, much trumpeted by computer-security experts who feared the computer underground. There had even been a Hollywood thriller about sinister hackers ruining airport computers - Die Hard II.

Now AT&T itself had crippled airports with computer malfunctions - not just one airport, but three at once, some of the busiest in the world.

Air traffic came to a standstill throughout the Greater New York area, causing more than 500 flights to be cancelled, in a spreading wave all over America and even into Europe. Another 500 or so flights were delayed, affecting, all in all, about 85,000 passengers. (One of these passengers was the chairman of the Federal Communications Commission.)

Stranded passengers in New York and New Jersey were further infuriated to discover that they could not even manage to make a long distance phone call, to explain their delay to loved ones or business associates. Thanks to the crash, about four and a half million domestic calls, and half a million international calls, failed to get through. The September 17 NYC Crash, unlike the previous ones, involved not a whisper of "hacker" misdeeds. On the contrary, by 1991, AT&T itself was suffering much of the vilification that had formerly been directed at hackers. Congressmen were grumbling. So were state and federal regulators. And so was the press.

For their part, ancient rival MCI took out snide fullpage newspaper ads in New York, offering their own longdistance services for the "next time that AT&T goes down." "You wouldn't find a classy company like AT&T using such advertising," protested AT&T Chairman Robert Allen, unconvincingly. Once again, out came the full-page AT&T apologies in newspapers, apologies for "an inexcusable culmination of both human and mechanical failure." (This time, however, AT&T offered no discount on later calls. Unkind critics suggested that AT&T were worried about setting any precedent for refunding the financial losses caused by telephone crashes.)

Industry journals asked publicly if AT&T was "asleep at the switch." The telephone network, America's purported marvel of high-tech reliability, had gone down three times in 18 months. Fortune magazine listed the Crash of September 17 among the "Biggest Business Goofs of 1991," cruelly parodying

AT&T's ad campaign in an article entitled "AT&T Wants You Back (Safely On the Ground, God Willing)."

Why had those New York switching systems simply run out of power? Because no human being had attended to the alarm system. Why did the alarm systems blare automatically, without any human being noticing? Because the three telco technicians who should have been listening were absent from their stations in the power-room, on another floor of the building - attending a training class. A training class about the alarm systems for the power room!

"Crashing the System" was no longer "unprecedented" by late 1991. On the contrary, it no longer even seemed an oddity. By 1991, it was clear that all the policemen in the world could no longer "protect" the phone system from crashes. By far the worst crashes the system had ever had, had been inflicted, by the system, upon itself. And this time nobody was making cocksure statements that this was an anomaly, something that would never happen again. By 1991 the System's defenders had met their nebulous Enemy, and the Enemy was - the System.

Part Two: The Digital Underground.

- Steal This Phone
- Phreaking and Hacking
- The View From Under the Floorboards
- Boards: Core of the Underground
- Phile Phun
- The Rake's Progress
- Strongholds of the Elite
- Sting Boards
- Hot Potatoes
- War on the Legion
- Terminus
- Phile 9-1-1
- War Games
- Real Cyberpunk.

The date was May 9, 1990. The Pope was touring Mexico City. Hustlers from the Medellin Cartel were trying to buy black-market Stinger missiles in Florida. On the comics page, Doonesbury character Andy was dying of AIDS.

And then… a highly unusual item whose novelty and calculated rhetoric won it headscratching attention in newspapers all over America. The US Attorney's office in Phoenix, Arizona, had issued a press release announcing a nationwide law enforcement crackdown against "illegal computer hacking activities." The sweep was officially known as "Operation Sundevil."

Eight paragraphs in the press release gave the bare facts: twenty-seven search warrants carried out on May 8, with three arrests, and a hundred and fifty agents on the prowl in "twelve" cities across America. (Different counts in local press reports yielded "thirteen," "fourteen," and "sixteen" cities.) Officials estimated that criminal losses of revenue to telephone companies "may run into millions of dollars." Credit for the Sundevil investigations was taken by the US Secret Service, Assistant US Attorney Tim Holtzen of Phoenix, and the Assistant Attorney General of Arizona, Gail Thackeray.

The prepared remarks of Garry M. Jenkins, appearing in a U.S. Department of Justice press release, were of particular interest. Mr. Jenkins was the Assistant Director of the US Secret Service, and the highest-ranking federal official to take any direct public role in the hacker crackdown of 1990.

"Today, the Secret Service is sending a clear message to those computer hackers who have decided to violate the laws of this nation in the mistaken belief that they can successfully avoid detection by hiding behind the relative anonymity of their computer terminals.(…) "Underground groups have been formed for the purpose of exchanging information relevant to their criminal activities. These groups often communicate with each other through message systems between computers called 'bulletin boards.' "Our experience shows that many computer hacker suspects are no longer misguided teenagers, mischievously playing games with their computers in their bedrooms. Some are now high tech computer operators using computers to engage in unlawful conduct."

Who were these "underground groups" and "hightech operators?" Where had they come from? What did they want? Who were they? Were they "mischievous?" Were they dangerous? How had "misguided teenagers" managed to alarm the United States Secret Service? And just how widespread was this sort of thing? Of all the major players in the Hacker Crackdown: the phone companies, law enforcement, the civil libertarians, and the "hackers" themselves - the "hackers" are by far the most mysterious, by far the hardest to understand, by far the weirdest.

Not only are "hackers" novel in their activities, but they come in a variety of odd subcultures, with a variety of languages, motives and values.

The earliest proto-hackers were probably those unsung mischievous telegraph boys who were summarily fired by the Bell Company in 1878.

Legitimate "hackers," those computer enthusiasts who are independent-minded but law-abiding, generally trace their spiritual ancestry to elite technical universities, especially M.I.T. and Stanford, in the 1960s.

But the genuine roots of the modern hacker underground can probably be traced most successfully to a now much-obscured hippie anarchist movement known as the Yippies. The Yippies, who took their name from the largely fictional "Youth International Party," carried out a loud and lively policy of surrealistic subversion and outrageous political mischief. Their basic tenets were flagrant sexual promiscuity, open and copious drug use, the political overthrow of any powermonger over thirty years of age, and an immediate end to the war in Vietnam, by any means necessary, including the psychic levitation of the Pentagon. The two most visible Yippies were Abbie Hoffman and Jerry Rubin. Rubin eventually became a Wall Street broker. Hoffman, ardently sought by federal authorities, went into hiding for seven years, in Mexico, France, and the United States. While on the lam, Hoffman continued to write and publish, with help from sympathizers in the American anarcho-leftist underground. Mostly, Hoffman survived through false ID and odd jobs. Eventually he underwent facial plastic surgery and adopted an entirely new identity as one "Barry Freed." After surrendering himself to authorities in 1980, Hoffman spent a year in prison on a cocaine conviction.

Hoffman's worldview grew much darker as the glory days of the 1960s faded. In 1989, he purportedly committed suicide, under odd and, to some, rather suspicious circumstances.

Abbie Hoffman is said to have caused the Federal Bureau of Investigation to amass the single largest investigation file ever opened on an individual American citizen. (If this is true, it is still questionable whether the FBI regarded Abbie Hoffman a serious public threat - quite possibly, his file was enormous simply because Hoffman left colorful legendry wherever he went). He was a gifted publicist, who regarded electronic media as both playground and weapon. He actively enjoyed manipulating network TV and other gullible, image-hungry media, with various weird lies, mindboggling rumors, impersonation scams, and other sinister distortions, all absolutely guaranteed to upset cops, Presidential candidates, and federal judges. Hoffman's most famous work was a book self-reflexively known as Steal This Book, which publicized a number of methods by which young, penniless hippie agitators might live off the fat of a system supported by humorless drones. Steal This Book, whose title urged readers to damage the very means of distribution which had put it into their hands, might be described as a spiritual ancestor of a computer virus.

Hoffman, like many a later conspirator, made extensive use of pay-phones for his agitation work - in his case, generally through the use of cheap brass washers as coin-slugs.

During the Vietnam War, there was a federal surtax imposed on telephone service; Hoffman and his cohorts could, and did, argue that in systematically stealing phone service they were engaging in civil disobedience: virtuously denying tax funds to an illegal and immoral war. But this thin veil of decency was soon dropped entirely. Ripping-off the System found its own justification in deep alienation and a basic outlaw contempt for conventional bourgeois values. Ingenious, vaguely politicized varieties of rip-off, which might be described as "anarchy by convenience," became very popular in Yippie circles, and because rip-off was so useful, it was to survive the Yippie movement itself. In the early 1970s, it required fairly limited expertise and ingenuity to cheat payphones, to divert "free" electricity and gas service, or to rob vending machines and parking meters for handy pocket change. It also required a conspiracy to spread this knowledge, and the gall and nerve actually to commit petty theft, but the Yippies had these qualifications in plenty. In June 1971, Abbie Hoffman and a telephone enthusiast sarcastically known as "Al Bell" began publishing a newsletter called Youth International Party Line. This newsletter was dedicated to collating and spreading Yippie rip-off techniques, especially of phones, to the joy of the freewheeling underground and the insensate rage of all straight people.

As a political tactic, phone-service theft ensured that Yippie advocates would always have ready access to the long-distance telephone as a medium, despite the Yippies' chronic lack of organization, discipline, money, or even a steady home address.

Party Linewas run out of Greenwich Village for a couple of years, then "Al Bell" more or less defected from the faltering ranks of Yippiedom, changing the newsletter's name to TAP or Technical Assistance Program. After the Vietnam War ended, the steam began leaking rapidly out of American radical dissent. But by this time, "Bell" and his dozen or so core contributors had the bit between their teeth, and had begun to derive tremendous gut-level satisfaction from the sensation of pure technical power.

TAParticles, once highly politicized, became pitilessly jargonized and technical, in homage or parody to the Bell System's own technical documents, which TAP studied closely, gutted, and reproduced without permission. The TAP elite revelled in gloating possession of the specialized knowledge necessary to beat the system.

"Al Bell" dropped out of the game by the late 70s, and "Tom Edison" took over; TAP readers (some 1400 of them, all told) now began to show more interest in telex switches and the growing phenomenon of computer systems. In 1983, "Tom Edison" had his computer stolen and his house set on fire by an arsonist. This was an eventually mortal blow to TAP (though the legendary name was to be resurrected in 1990 by a young Kentuckian computer outlaw named "Predat0r.")

-Section 1-

Ever since telephones began to make money, there have been people willing to rob and defraud phone companies. The legions of petty phone thieves vastly outnumber those "phone phreaks" who "explore the system" for the sake of the intellectual challenge. The New York metropolitan area (long in the vanguard of American crime) claims over 150,000 physical attacks on pay telephones every year! Studied carefully, a modern payphone reveals itself as a little fortress, carefully designed and redesigned over generations, to resist coinslugs, zaps of electricity, chunks of coin-shaped ice, prybars, magnets, lockpicks, blasting caps. Public pay-phones must survive in a world of unfriendly, greedy people, and a modern payphone is as exquisitely evolved as a cactus.

Because the phone network pre-dates the computer network, the scofflaws known as "phone phreaks" pre-date the scofflaws known as "computer hackers." In practice, today, the line between "phreaking" and "hacking" is very blurred, just as the distinction between telephones and computers has blurred. The phone system has been digitized, and computers have learned to "talk" over phone-lines. What's worse - and this was the point of the Mr. Jenkins of the Secret Service - some hackers have learned to steal, and some thieves have learned to hack.

Despite the blurring, one can still draw a few useful behavioral distinctions between "phreaks" and "hackers." Hackers are intensely interested in the "system" per se, and enjoy relating to machines. "Phreaks" are more social, manipulating the system in a rough-and-ready fashion in order to get through to other human beings, fast, cheap and under the table.

Phone phreaks love nothing so much as "bridges," illegal conference calls of ten or twelve chatting conspirators, seaboard to seaboard, lasting for many hours - and running, of course, on somebody else's tab, preferably a large corporation's. As phone-phreak conferences wear on, people drop out (or simply leave the phone off the hook, while they sashay off to work or school or babysitting), and new people are phoned up and invited to join in, from some other continent, if possible. Technical trivia, boasts, brags, lies, head-trip deceptions, weird rumors, and cruel gossip are all freely exchanged. The lowest rung of phone-phreaking is the theft of telephone access codes. Charging a phone call to somebody else's stolen number is, of course, a pig-easy way of stealing phone service, requiring practically no technical expertise. This practice has been very widespread, especially among lonely people without much

money who are far from home. Code theft has flourished especially in college dorms, military bases, and, notoriously, among roadies for rock bands. Of late, code theft has spread very rapidly among Third Worlders in the US, who pile up enormous unpaid long-distance bills to the Caribbean, South America, and Pakistan.

The simplest way to steal phone-codes is simply to look over a victim's shoulder as he punches-in his own code-number on a public payphone. This technique is known as "shoulder-surfing," and is especially common in airports, bus terminals, and train stations. The code is then sold by the thief for a few dollars. The buyer abusing the code has no computer expertise, but calls his Mom in New York, Kingston or Caracas and runs up a huge bill with impunity. The losses from this primitive phreaking activity are far, far greater than the monetary losses caused by computer-intruding hackers. In the mid-to-late 1980s, until the introduction of sterner telco security measures, computerized code theft worked like a charm, and was virtually omnipresent throughout the digital underground, among phreaks and hackers alike. This was accomplished through programming one's computer to try random code numbers over the telephone until one of them worked. Simple programs to do this were widely available in the underground; a computer running all night was likely to come up with a dozen or so useful hits. This could be repeated week after week until one had a large library of stolen codes.

Nowadays, the computerized dialling of hundreds of numbers can be detected within hours and swiftly traced. If a stolen code is repeatedly abused, this too can be detected within a few hours. But for years in the 1980s, the publication of stolen codes was a kind of elementary etiquette for fledgling hackers. The simplest way to establish your bona-fides as a raider was to steal a code through repeated random dialling and offer it to the "community" for use. Codes could be both stolen, and used, simply and easily from the safety of one's own bedroom, with very little fear of detection or punishment.

Before computers and their phone-line modems entered American homes in gigantic numbers, phone phreaks had their own special telecommunications hardware gadget, the famous "blue box." This fraud device (now rendered increasingly useless by the digital evolution of the phone system) could trick switching systems into granting free access to long-distance lines. It did this by mimicking the system's own signal, a tone of 2600 hertz.

Steven Jobs and Steve Wozniak, the founders of Apple Computer, Inc., once dabbled in selling blue-boxes in college dorms in California. For many, in the early days of phreaking, blue-boxing was scarcely perceived as "theft," but rather as a fun (if sneaky) way to use excess phone capacity harmlessly. After all, the long-distance lines were just sitting there… Whom did it hurt, really? If you're not damaging the system, and you're not using up any tangible resource, and if nobody finds out what you did, then what real harm have you done? What exactly have you "stolen," anyway? If a tree falls in the forest and nobody hears it, how much is the noise worth? Even now this remains a rather dicey question.

Blue-boxing was no joke to the phone companies, however. Indeed, when Ramparts magazine, a radical publication in California, printed the wiring schematics necessary to create a mute box in June 1972, the magazine was seized by police and Pacific Bell phonecompany officials. The mute box, a blue-box variant, allowed its user to receive long-distance calls free of charge to the caller. This device was closely described in a Ramparts article wryly titled "Regulating the Phone Company In Your Home." Publication of this article was held to be in violation of Californian State Penal Code section 502.7, which outlaws ownership of wire-fraud devices and the selling of "plans or instructions for any instrument, apparatus, or device intended to avoid telephone toll charges."

Issues of Ramparts were recalled or seized on the newsstands, and the resultant loss of income helped put the magazine out of business. This was an ominous precedent for free-expression issues, but the telco's crushing of a radical-fringe magazine passed without serious challenge at the time. Even in the freewheeling California 1970s, it was widely felt that there was something sacrosanct about what the phone company knew; that the telco had a legal and moral right to protect itself by shutting off the flow of such illicit inform-

ation. Most telco information was so "specialized" that it would scarcely be understood by any honest member of the public. If not published, it would not be missed. To print such material did not seem part of the legitimate role of a free press.

In 1990 there would be a similar telco-inspired attack on the electronic phreak/hacking "magazine" Phrack. The Phrack legal case became a central issue in the Hacker Crackdown, and gave rise to great controversy. Phrack would also be shut down, for a time, at least, but this time both the telcos and their law enforcement allies would pay a much larger price for their actions. The Phrack case will be examined in detail, later.

Phone-phreaking as a social practice is still very much alive at this moment. Today, phone-phreaking is thriving much more vigorously than the better-known and worse-feared practice of "computer hacking." New forms of phreaking are spreading rapidly, following new vulnerabilities in sophisticated phone services.

Cellular phones are especially vulnerable; their chips can be re-programmed to present a false caller ID and avoid billing. Doing so also avoids police tapping, making cellular-phone abuse a favorite among drug-dealers. "Call-sell operations" using pirate cellular phones can, and have, been run right out of the backs of cars, which move from "cell" to "cell" in the local phone system, retailing stolen long-distance service, like some kind of demented electronic version of the neighborhood ice-cream truck.

Private branch-exchange phone systems in large corporations can be penetrated; phreaks dial-up a local company, enter its internal phone-system, hack it, then use the company's own PBX system to dial back out over the public network, causing the company to be stuck with the resulting long-distance bill. This technique is known as "diverting." "Diverting" can be very costly, especially because phreaks tend to travel in packs and never stop talking. Perhaps the worst by-product of this "PBX fraud" is that victim companies and telcos have sued one another over the financial responsibility for the stolen calls, thus enriching not only shabby phreaks but well-paid lawyers.

"Voice-mail systems" can also be abused; phreaks can seize their own sections of these sophisticated electronic answering machines, and use them for trading codes or knowledge of illegal techniques. Voice-mail abuse does not hurt the company directly, but finding supposedly empty slots in your company's answering machine all crammed with phreaks eagerly chattering and hey-duding one another in impenetrable jargon can cause sensations of almost mystical repulsion and dread.

Worse yet, phreaks have sometimes been known to react truculently to attempts to "clean up" the voice-mail system. Rather than humbly acquiescing to being thrown out of their playground, they may very well call up the company officials at work (or at home) and loudly demand free voice-mail addresses of their very own. Such bullying is taken very seriously by spooked victims.

Acts of phreak revenge against straight people are rare, but voice-mail systems are especially tempting and vulnerable, and an infestation of angry phreaks in one's voice-mail system is no joke. They can erase legitimate messages; or spy on private messages; or harass users with recorded taunts and obscenities. They've even been known to seize control of voice-mail security, and lock out legitimate users, or even shut down the system entirely.

Cellular phone-calls, cordless phones, and ship-to-shore telephony can all be monitored by various forms of radio; this kind of "passive monitoring" is spreading explosively today. Technically eavesdropping on other people's cordless and cellular phone-calls is the fastest growing area in phreaking today. This practice strongly appeals to the lust for power and conveys gratifying sensations of technical superiority over the eavesdropping victim. Monitoring is rife with all manner of tempting evil mischief. Simple prurient snooping is by far the most common activity. But credit-card numbers unwarily spoken over the phone can be recorded, stolen and used. And tapping people's phone-calls (whether through active telephone taps or passive radio monitors) does lend itself conveniently to activities like blackmail, industrial espionage, and political dirty tricks. It should be repeated that telecommunications fraud, the theft of phone service, causes vastly greater monetary losses than the practice of entering into computers by stealth. Hackers are mostly young sub-

urban American white males, and exist in their hundreds - but “phreaks” come from both sexes and from many nationalities, ages and ethnic backgrounds, and are flourishing in the thousands.

-Section 2-

The term “hacker” has had an unfortunate history. This book, The Hacker Crackdown, has little to say about “hacking” in its finer, original sense. The term can signify the free-wheeling intellectual exploration of the highest and deepest potential of computer systems. Hacking can describe the determination to make access to computers and information as free and open as possible. Hacking can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit. This is “hacking” as it was defined in Steven Levy’s much-praised history of the pioneer computer milieu, Hackers, published in 1984.

Hackers of all kinds are absolutely soaked through with heroic anti-bureaucratic sentiment. Hackers long for recognition as a praiseworthy cultural archetype, the postmodern electronic equivalent of the cowboy and mountain man. Whether they deserve such a reputation is something for history to decide. But many hackers - including those outlaw hackers who are computer intruders, and whose activities are defined as criminal - actually attempt to live up to this techno-cowboy reputation. And given that electronics and telecommunications are still largely unexplored territories, there is simply no telling what hackers might uncover.

For some people, this freedom is the very breath of oxygen, the inventive spontaneity that makes life worth living and that flings open doors to marvellous possibility and individual empowerment. But for many people - and increasingly so - the hacker is an ominous figure, a smart aleck sociopath ready to burst out of his basement wilderness and savage other people’s lives for his own anarchical convenience.

Any form of power without responsibility, without direct and formal checks and balances, is frightening to people - and reasonably so. It should be frankly admitted that hackers are frightening, and that the basis of this fear is not irrational. Fear of hackers goes well beyond the fear of merely criminal activity.

Subversion and manipulation of the phone system is an act with disturbing political overtones. In America, computers and telephones are potent symbols of organized authority and the technocratic business elite.

But there is an element in American culture that has always strongly rebelled against these symbols; rebelled against all large industrial computers and all phone companies. A certain anarchical tinge deep in the American soul delights in causing confusion and pain to all bureaucracies, including technological ones.

There is sometimes malice and vandalism in this attitude, but it is a deep and cherished part of the American national character. The outlaw, the rebel, the rugged individual, the pioneer, the sturdy Jeffersonian yeoman, the private citizen resisting interference in his pursuit of happiness - these are figures that all Americans recognize, and that many will strongly applaud and defend.

Many scrupulously law-abiding citizens today do cutting-edge work with electronics - work that has already had tremendous social influence and will have much more in years to come. In all truth, these talented, hardworking, law-abiding, mature, adult people are far more disturbing to the peace and order of the current status quo than any scofflaw group of romantic teenage punk kids. These law-abiding hackers have the power, ability, and willingness to influence other people’s lives quite unpredictably. They have means, motive, and opportunity to meddle drastically with the American social order. When corralled into governments, universities, or large multinational companies, and forced to follow rulebooks and wear suits and ties, they at least have some conventional halters on their freedom of action. But when loosed alone, or in small groups, and fired by imagination and the entrepreneurial spirit,

they can move mountains - causing landslides that will likely crash directly into your office and living room.

These people, as a class, instinctively recognize that a public, politicized attack on hackers will eventually spread to them - that the term "hacker," once demonized, might be used to knock their hands off the levers of power and choke them out of existence. There are hackers today who fiercely and publicly resist any besmirching of the noble title of hacker. Naturally and understandably, they deeply resent the attack on their values implicit in using the word "hacker" as a synonym for computer-criminal.

This book, sadly but in my opinion unavoidably, rather adds to the degradation of the term. It concerns itself mostly with "hacking" in its commonest latter-day definition, i.e., intruding into computer systems by stealth and without permission. The term "hacking" is used routinely today by almost all law enforcement officials with any professional interest in computer fraud and abuse. American police describe almost any crime committed with, by, through, or against a computer as hacking.

Most importantly, "hacker" is what computer intruders choose to call themselves. Nobody who "hacks" into systems willingly describes himself (rarely, herself) as a "computer intruder," "computer trespasser," "cracker," "wormer," "darkside hacker" or "high tech street gangster." Several other demeaning terms have been invented in the hope that the press and public will leave the original sense of the word alone. But few people actually use these terms. (I exempt the term "cyberpunk," which a few hackers and law enforcement people actually do use. The term "cyberpunk" is drawn from literary criticism and has some odd and unlikely resonances, but, like hacker, cyberpunk too has become a criminal pejorative today.)

In any case, breaking into computer systems was hardly alien to the original hacker tradition. The first tottering systems of the 1960s required fairly extensive internal surgery merely to function day-by-day. Their users "invaded" the deepest, most arcane recesses of their operating software almost as a matter of routine. "Computer security" in these early, primitive systems was at best an afterthought. What security there was, was entirely physical, for it was assumed that anyone allowed near this expensive, arcane hardware would be a fully qualified professional expert.

In a campus environment, though, this meant that grad students, teaching assistants, undergraduates, and eventually, all manner of dropouts and hangers-on ended up accessing and often running the works.

Universities, even modern universities, are not in the business of maintaining security over information. On the contrary, universities, as institutions, pre-date the "information economy" by many centuries and are not-for-profit cultural entities, whose reason for existence (purportedly) is to discover truth, codify it through techniques of scholarship, and then teach it. Universities are meant to pass the torch of civilization, not just download data into student skulls, and the values of the academic community are strongly at odds with those of all would-be information empires. Teachers at all levels, from kindergarten up, have proven to be shameless and persistent software and data pirates. Universities do not merely "leak information" but vigorously broadcast free thought.

This clash of values has been fraught with controversy. Many hackers of the 1960s remember their professional apprenticeship as a long guerilla war against the uptight mainframe-computer "information priesthood." These computer-hungry youngsters had to struggle hard for access to computing power, and many of them were not above certain, er, shortcuts. But, over the years, this practice freed computing from the sterile reserve of lab-coated technocrats and was largely responsible for the explosive growth of computing in general society - especially personal computing.

Access to technical power acted like catnip on certain of these youngsters. Most of the basic techniques of computer intrusion: password cracking, trapdoors, backdoors, trojan horses - were invented in college environments in the 1960s, in the early days of network computing. Some off-the-cuff experience at computer intrusion was to be in the informal resume of most "hackers" and many future industry giants. Outside of the tiny cult of computer enthusiasts, few people thought much about the implications of "breaking into" com-

puters. This sort of activity had not yet been publicized, much less criminalized.

In the 1960s, definitions of "property" and "privacy" had not yet been extended to cyberspace. Computers were not yet indispensable to society. There were no vast databanks of vulnerable, proprietary information stored in computers, which might be accessed, copied without permission, erased, altered, or sabotaged. The stakes were low in the early days - but they grew every year, exponentially, as computers themselves grew.

By the 1990s, commercial and political pressures had become overwhelming, and they broke the social boundaries of the hacking subculture. Hacking had become too important to be left to the hackers. Society was now forced to tackle the intangible nature of cyberspace as property, cyberspace as privately-owned unreal-estate. In the new, severe, responsible, highstakes context of the "Information Society" of the 1990s, "hacking" was called into question.

What did it mean to break into a computer without permission and use its computational power, or look around inside its files without hurting anything? What were computer-intruding hackers, anyway - how should society, and the law, best define their actions? Were they just browsers, harmless intellectual explorers? Were they voyeurs, snoops, invaders of privacy? Should they be sternly treated as potential agents of espionage, or perhaps as industrial spies? Or were they best defined as trespassers, a very common teenage misdemeanor? Was hacking theft of service? (After all, intruders were getting someone else's computer to carry out their orders, without permission and without paying). Was hacking fraud? Maybe it was best described as impersonation. The commonest mode of computer intrusion was (and is) to swipe or snoop somebody else's password, and then enter the computer in the guise of another person - who is commonly stuck with the blame and the bills.

Perhaps a medical metaphor was better - hackers should be defined as "sick," as computer addicts unable to control their irresponsible, compulsive behavior.

But these weighty assessments meant little to the people who were actually being judged. From inside the underground world of hacking itself, all these perceptions seem quaint, wrongheaded, stupid, or meaningless. The most important self-perception of underground hackers - from the 1960s, right through to the present day - is that they are an elite. The day-to-day struggle in the underground is not over sociological definitions - who cares? - but for power, knowledge, and status among one's peers.

When you are a hacker, it is your own inner conviction of your elite status that enables you to break, or let us say "transcend," the rules. It is not that all rules go by the board. The rules habitually broken by hackers are unimportant rules - the rules of dopey greedhead telco bureaucrats and pig-ignorant government pests. Hackers have their own rules, which separate behavior which is cool and elite, from behavior which is rodentlike, stupid and losing. These "rules," however, are mostly unwritten and enforced by peer pressure and tribal feeling. Like all rules that depend on the unspoken conviction that everybody else is a good old boy, these rules are ripe for abuse. The mechanisms of hacker peer-pressure, "teletrials" and ostracism, are rarely used and rarely work. Back-stabbing slander, threats, and electronic harassment are also freely employed in down-and-dirty intrahacker feuds, but this rarely forces a rival out of the scene entirely. The only real solution for the problem of an utterly losing, treacherous and rodentlike hacker is to turn him in to the police. Unlike the Mafia or Medellin Cartel, the hacker elite cannot simply execute the bigmouths, creeps and troublemakers among their ranks, so they turn one another in with astonishing frequency.

There is no tradition of silence or omerta in the hacker underworld. Hackers can be shy, even reclusive, but when they do talk, hackers tend to brag, boast and strut. Almost everything hackers do is invisible; if they don't brag, boast, and strut about it, then nobody will ever know. If you don't have something to brag, boast, and strut about, then nobody in the underground will recognize you and favor you with vital cooperation and respect.

The way to win a solid reputation in the underground is by telling other hackers things that could only have been learned by exceptional cunning and

stealth. Forbidden knowledge, therefore, is the basic currency of the digital underground, like seashells among Trobriand Islanders. Hackers hoard this knowledge, and dwell upon it obsessively, and refine it, and bargain with it, and talk and talk about it. Many hackers even suffer from a strange obsession to teach - to spread the ethos and the knowledge of the digital underground. They'll do this even when it gains them no particular advantage and presents a grave personal risk.

And when that risk catches up with them, they will go right on teaching and preaching - to a new audience this time, their interrogators from law enforcement. Almost every hacker arrested tells everything he knows - all about his friends, his mentors, his disciples - legends, threats, horror stories, dire rumors, gossip, hallucinations. This is, of course, convenient for law enforcement - except when law enforcement begins to believe hacker legendry.

Phone phreaks are unique among criminals in their willingness to call up law enforcement officials - in the office, at their homes - and give them an extended piece of their mind. It is hard not to interpret this as begging for arrest, and in fact it is an act of incredible foolhardiness. Police are naturally nettled by these acts of chutzpah and will go well out of their way to bust these flaunting idiots. But it can also be interpreted as a product of a world-view so elitist, so closed and hermetic, that electronic police are simply not perceived as "police," but rather as enemy phone phreaks who should be scolded into behaving "decently."

Hackers at their most grandiloquent perceive themselves as the elite pioneers of a new electronic world. Attempts to make them obey the democratically established laws of contemporary American society are seen as repression and persecution. After all, they argue, if Alexander Graham Bell had gone along with the rules of the Western Union telegraph company, there would have been no telephones. If Jobs and Wozniak had believed that IBM was the be-all and end-all, there would have been no personal computers. If Benjamin Franklin and Thomas Jefferson had tried to "work within the system" there would have been no United States.

Not only do hackers privately believe this as an article of faith, but they have been known to write ardent manifestos about it. Here are some revealing excerpts from an especially vivid hacker manifesto: "The TechnoRevolution" by "Dr. Crash," which appeared in electronic form in Phrack Volume 1, Issue 6, Phile 3.

"To fully explain the true motives behind hacking, we must first take a quick look into the past. In the 1960s, a group of MIT students built the first modern computer system. This wild, rebellious group of young men were the first to bear the name `hackers.' The systems that they developed were intended to be used to solve world problems and to benefit all of mankind.

"As we can see, this has not been the case. The computer system has been solely in the hands of big businesses and the government. The wonderful device meant to enrich life has become a weapon which dehumanizes people. To the government and large businesses, people are no more than disk space, and the government doesn't use computers to arrange aid for the poor, but to control nuclear death weapons. The average American can only have access to a small microcomputer which is worth only a fraction of what they pay for it. The businesses keep the true state-of-the-art equipment away from the people behind a steel wall of incredibly high prices and bureaucracy. It is because of this state of affairs that hacking was born.(…)

"Of course, the government doesn't want the monopoly of technology broken, so they have outlawed hacking and arrest anyone who is caught.(…) The phone company is another example of technology abused and kept from people with high prices.(…)

"Hackers often find that their existing equipment, due to the monopoly tactics of computer companies, is inefficient for their purposes. Due to the exorbitantly high prices, it is impossible to legally purchase the necessary equipment. This need has given still another segment of the fight: Credit Carding. Carding is a way of obtaining the necessary goods without paying for them. It is again due to the companies' stupidity that Carding is so easy, and shows that the world's businesses are in the hands of those with considerably less technical know-how than we, the hackers. (…) "Hacking must continue. We

must train newcomers to the art of hacking.(…) And whatever you do, continue the fight. Whether you know it or not, if you are a hacker, you are a revolutionary. Don't worry, you're on the right side."

The defense of "carding" is rare. Most hackers regard credit-card theft as "poison" to the underground, a sleazy and immoral effort that, worse yet, is hard to get away with. Nevertheless, manifestos advocating credit card theft, the deliberate crashing of computer systems, and even acts of violent physical destruction such as vandalism and arson do exist in the underground. These boasts and threats are taken quite seriously by the police. And not every hacker is an abstract, Platonic computer nerd. Some few are quite experienced at picking locks, robbing phone-trucks, and breaking and entering buildings.

Hackers vary in their degree of hatred for authority and the violence of their rhetoric. But, at a bottom line, they are scofflaws. They don't regard the current rules of electronic behavior as respectable efforts to preserve law and order and protect public safety. They regard these laws as immoral efforts by soulless corporations to protect their profit margins and to crush dissidents. "Stupid" people, including police, businessmen, politicians, and journalists, simply have no right to judge the actions of those possessed of genius, techno-revolutionary intentions, and technical expertise.

-Section 3-

Hackers are generally teenagers and college kids not engaged in earning a living. They often come from fairly well-to-do middle-class backgrounds, and are markedly anti-materialistic (except, that is, when it comes to computer equipment). Anyone motivated by greed for mere money (as opposed to the greed for power, knowledge and status) is swiftly written-off as a narrowminded breadhead whose interests can only be corrupt and contemptible.

Having grown up in the 1970s and 1980s, the young Bohemians of the digital underground regard straight society as awash in plutocratic corruption, where everyone from the President down is for sale and whoever has the gold makes the rules.

Interestingly, there's a funhouse-mirror image of this attitude on the other side of the conflict. The police are also one of the most markedly anti-materialistic groups in American society, motivated not by mere money but by ideals of service, justice, esprit-de-corps, and, of course, their own brand of specialized knowledge and power. Remarkably, the propaganda war between cops and hackers has always involved angry allegations that the other side is trying to make a sleazy buck. Hackers consistently sneer that anti-phreak prosecutors are angling for cushy jobs as telco lawyers and that computer crime police are aiming to cash in later as well-paid computer-security consultants in the private sector.

For their part, police publicly conflate all hacking crimes with robbing payphones with crowbars. Allegations of "monetary losses" from computer intrusion are notoriously inflated. The act of illicitly copying a document from a computer is morally equated with directly robbing a company of, say, half a million dollars. The teenage computer intruder in possession of this "proprietary" document has certainly not sold it for such a sum, would likely have little idea how to sell it at all, and quite probably doesn't even understand what he has. He has not made a cent in profit from his felony but is still morally equated with a thief who has robbed the church poorbox and lit out for Brazil.

Police want to believe that all hackers are thieves. It is a tortuous and almost unbearable act for the American justice system to put people in jail because they want to learn things which are forbidden for them to know. In an American context, almost any pretext for punishment is better than jailing people to protect certain restricted kinds of information. Nevertheless, policing information is part and parcel of the struggle against hackers.

This dilemma is well exemplified by the remarkable activities of "Emmanuel Goldstein," editor and publisher of a print magazine known as 2600: The Hacker Quarterly. Goldstein was an English major at Long Island's State University of New York in the '70s, when he became involved with the local college radio

station. His growing interest in electronics caused him to drift into Yippie TAP circles and thus into the digital underground, where he became a self-described techno-rat. His magazine publishes techniques of computer intrusion and telephone "exploration" as well as gloating exposes of telco misdeeds and governmental failings.

Goldstein lives quietly and very privately in a large, crumbling Victorian mansion in Setauket, New York. The seaside house is decorated with telco decals, chunks of driftwood, and the basic bric-a-brac of a hippie crash-pad. He is unmarried, mildly unkempt, and survives mostly on TV dinners and turkey-stuffing eaten straight out of the bag. Goldstein is a man of considerable charm and fluency, with a brief, disarming smile and the kind of pitiless, stubborn, thoroughly recidivist integrity that America's electronic police find genuinely alarming.

Goldstein took his nom-de-plume, or "handle," from a character in Orwell's 1984, which may be taken, correctly, as a symptom of the gravity of his socio-opolitical worldview. He is not himself a practicing computer intruder, though he vigorously abets these actions, especially when they are pursued against large corporations or governmental agencies. Nor is he a thief, for he loudly scorns mere theft of phone service, in favor of `exploring and manipulating the system.' He is probably best described and understood as a dissident.

Weirdly, Goldstein is living in modern America under conditions very similar to those of former East European intellectual dissidents. In other words, he flagrantly espouses a value-system that is deeply and irrevocably opposed to the system of those in power and the police. The values in 2600 are generally expressed in terms that are ironic, sarcastic, paradoxical, or just downright confused. But there's no mistaking their radically anti-authoritarian tenor. 2600 holds that technical power and specialized knowledge, of any kind obtainable, belong by right in the hands of those individuals brave and bold enough to discover them - by whatever means necessary. Devices, laws, or systems that forbid access, and the free spread of knowledge, are provocations that any free and self-respecting hacker should relentlessly attack. The "privacy" of governments, corporations and other soulless technocratic organizations should never be protected at the expense of the liberty and free initiative of the individual techno-rat.

However, in our contemporary workaday world, both governments and corporations are very anxious indeed to police information which is secret, proprietary, restricted, confidential, copyrighted, patented, hazardous, illegal, unethical, embarrassing, or otherwise sensitive. This makes Goldstein persona non grata, and his philosophy a threat.

Very little about the conditions of Goldstein's daily life would astonish, say, Vaclav Havel. (We may note in passing that President Havel once had his word-processor confiscated by the Czechoslovak police.) Goldstein lives by samizdat, acting semi-openly as a data-center for the underground, while challenging the powers-that-be to abide by their own stated rules: freedom of speech and the First Amendment.

Goldstein thoroughly looks and acts the part of techno-rat, with shoulder-length ringlets and a piratical black fisherman's-cap set at a rakish angle. He often shows up like Banquo's ghost at meetings of computer professionals, where he listens quietly, half-smiling and taking thorough notes.

Computer professionals generally meet publicly, and find it very difficult to rid themselves of Goldstein and his ilk without extralegal and unconstitutional actions. Sympathizers, many of them quite respectable people with responsible jobs, admire Goldstein's attitude and surreptitiously pass him information. An unknown but presumably large proportion of Goldstein's 2,000-plus readership are telco security personnel and police, who are forced to subscribe to 2600 to stay abreast of new developments in hacking. They thus find themselves paying this guy's rent while grinding their teeth in anguish, a situation that would have delighted Abbie Hoffman (one of Goldstein's few idols).

Goldstein is probably the best-known public representative of the hacker underground today, and certainly the best-hated. Police regard him as a Fagin, a corrupter of youth, and speak of him with untempered loathing. He is quite an accomplished gadfly.

After the Martin Luther King Day Crash of 1990, Goldstein, for instance, adeptly rubbed salt into the wound in the pages of 2600. "Yeah, it was fun for the phone phreaks as we watched the network crumble," he admitted cheerfully. "But it was also an ominous sign of what's to come… Some AT&T people, aided by well-meaning but ignorant media, were spreading the notion that many companies had the same software and therefore could face the same problem someday. Wrong. This was entirely an AT&T software deficiency. Of course, other companies could face entirely different software problems. But then, so too could AT&T."

After a technical discussion of the system's failings, the Long Island techno-rat went on to offer thoughtful criticism to the gigantic multinational's hundreds of professionally qualified engineers. "What we don't know is how a major force in communications like AT&T could be so sloppy. What happened to backups? Sure, computer systems go down all the time, but people making phone calls are not the same as people logging on to computers. We must make that distinction. It's not acceptable for the phone system or any other essential service to `go down.' If we continue to trust technology without understanding it, we can look forward to many variations on this theme.

"AT&T owes it to its customers to be prepared to instantly switch to another network if something strange and unpredictable starts occurring. The news here isn't so much the failure of a computer program, but the failure of AT&T's entire structure."

The very idea of this… this person… offering "advice" about "AT&T's entire structure" is more than some people can easily bear. How dare this near-criminal dictate what is or isn't "acceptable" behavior from AT&T? Especially when he's publishing, in the very same issue, detailed schematic diagrams for creating various switching-network signalling tones unavailable to the public.

"See what happens when you drop a `silver box' tone or two down your local exchange or through different long-distance service carriers," advises 2600 contributor "Mr. Upsetter" in "How To Build a Signal Box." "If you experiment systematically and keep good records, you will surely discover something interesting."

This is, of course, the scientific method, generally regarded as a praiseworthy activity and one of the flowers of modern civilization. One can indeed learn a great deal with this sort of structured intellectual activity. Telco employees regard this mode of "exploration" as akin to flinging sticks of dynamite into their pond to see what lives on the bottom.

2600has been published consistently since 1984. It has also run a bulletin board computer system, printed 2600 T-shirts, taken fax calls… The Spring 1991 issue has an interesting announcement on page 45: "We just discovered an extra set of wires attached to our fax line and heading up the pole. (They've since been clipped.) Your faxes to us and to anyone else could be monitored."

In the worldview of 2600, the tiny band of technorat brothers (rarely, sisters) are a beseiged vanguard of the truly free and honest. The rest of the world is a maelstrom of corporate crime and high-level governmental corruption, occasionally tempered with well-meaning ignorance. To read a few issues in a row is to enter a nightmare akin to Solzhenitsyn's, somewhat tempered by the fact that 2600 is often extremely funny.

Goldstein did not become a target of the Hacker Crackdown, though he protested loudly, eloquently, and publicly about it, and it added considerably to his fame. It was not that he is not regarded as dangerous, because he is so regarded. Goldstein has had brushes with the law in the past: in 1985, a 2600 bulletin board computer was seized by the FBI, and some software on it was formally declared "a burglary tool in the form of a computer program." But Goldstein escaped direct repression in 1990, because his magazine is printed on paper, and recognized as subject to Constitutional freedom of the press protection. As was seen in the Ramparts case, this is far from an absolute guarantee. Still, as a practical matter, shutting down 2600 by court-order would create so much legal hassle that it is simply unfeasible, at least for the present. Throughout 1990, both Goldstein and his magazine were peevishly thriving.

Instead, the Crackdown of 1990 would concern itself with the computerized version of forbidden data. The crackdown itself, first and foremost, was about

bulletin board systems. Bulletin Board Systems, most often known by the ugly and un-pluralizable acronym "BBS," are the life-blood of the digital underground. Boards were also central to law enforcement's tactics and strategy in the Hacker Crackdown.

A "bulletin board system" can be formally defined as a computer which serves as an information and messagepassing center for users dialing-up over the phone-lines through the use of modems. A "modem," or modulatordemodulator, is a device which translates the digital impulses of computers into audible analog telephone signals, and vice versa. Modems connect computers to phones and thus to each other.

Large-scale mainframe computers have been connected since the 1960s, but personal computers, run by individuals out of their homes, were first networked in the late 1970s. The "board" created by Ward Christensen and Randy Suess in February 1978, in Chicago, Illinois, is generally regarded as the first personal-computer bulletin board system worthy of the name. Boards run on many different machines, employing many different kinds of software. Early boards were crude and buggy, and their managers, known as "system operators" or "sysops," were hard-working technical experts who wrote their own software. But like most everything else in the world of electronics, boards became faster, cheaper, better-designed, and generally far more sophisticated throughout the 1980s. They also moved swiftly out of the hands of pioneers and into those of the general public. By 1985 there were something in the neighborhood of 4,000 boards in America. By 1990 it was calculated, vaguely, that there were about 30,000 boards in the US, with uncounted thousands overseas.

Computer bulletin boards are unregulated enterprises. Running a board is a rough-and-ready, catch-as-catch-can proposition. Basically, anybody with a computer, modem, software and a phone-line can start a board. With second-hand equipment and public-domain free software, the price of a board might be quite small - less than it would take to publish a magazine or even a decent pamphlet. Entrepreneurs eagerly sell bulletin-board software, and will coach non-technical amateur sysops in its use.

Boards are not "presses." They are not magazines, or libraries, or phones, or CB radios, or traditional cork bulletin boards down at the local laundry, though they have some passing resemblance to those earlier media. Boards are a new medium - they may even be a large number of new media.

Consider these unique characteristics: boards are cheap, yet they can have a national, even global reach. Boards can be contacted from anywhere in the global telephone network, at no cost to the person running the board - the caller pays the phone bill, and if the caller is local, the call is free. Boards do not involve an editorial elite addressing a mass audience. The "sysop" of a board is not an exclusive publisher or writer - he is managing an electronic salon, where individuals can address the general public, play the part of the general public, and also exchange private mail with other individuals. And the "conversation" on boards, though fluid, rapid, and highly interactive, is not spoken, but written. It is also relatively anonymous, sometimes completely so.

And because boards are cheap and ubiquitous, regulations and licensing requirements would likely be practically unenforceable. It would almost be easier to "regulate," "inspect" and "license" the content of private mail - probably more so, since the mail system is operated by the federal government. Boards are run by individuals, independently, entirely at their own whim.

For the sysop, the cost of operation is not the primary limiting factor. Once the investment in a computer and modem has been made, the only steady cost is the charge for maintaining a phone line (or several phone lines). The primary limits for sysops are time and energy. Boards require upkeep. New users are generally "validated" - they must be issued individual passwords, and called at home by voice-phone, so that their identity can be verified. Obnoxious users, who exist in plenty, must be chided or purged. Proliferating messages must be deleted when they grow old, so that the capacity of the system is not overwhelmed. And software programs (if such things are kept on the board) must be examined for possible computer viruses. If there is a financial charge to use the board (increasingly common, especially in larger and fancier

systems) then accounts must be kept, and users must be billed. And if the board crashes - a very common occurrence - then repairs must be made.

Boards can be distinguished by the amount of effort spent in regulating them. First, we have the completely open board, whose sysop is off chugging brews and watching re-runs while his users generally degenerate over time into peevish anarchy and eventual silence. Second comes the supervised board, where the sysop breaks in every once in a while to tidy up, calm brawls, issue announcements, and rid the community of dolts and troublemakers. Third is the heavily supervised board, which sternly urges adult and responsible behavior and swiftly edits any message considered offensive, impertinent, illegal or irrelevant. And last comes the completely edited "electronic publication," which is presented to a silent audience which is not allowed to respond directly in any way.

Boards can also be grouped by their degree of anonymity. There is the completely anonymous board, where everyone uses pseudonyms - "handles" - and even the sysop is unaware of the user's true identity. The sysop himself is likely pseudonymous on a board of this type. Second, and rather more common, is the board where the sysop knows (or thinks he knows) the true names and addresses of all users, but the users don't know one another's names and may not know his. Third is the board where everyone has to use real names, and roleplaying and pseudonymous posturing are forbidden.

Boards can be grouped by their immediacy. "Chatlines" are boards linking several users together over several different phone-lines simultaneously, so that people exchange messages at the very moment that they type. (Many large boards feature "chat" capabilities along with other services.) Less immediate boards, perhaps with a single phoneline, store messages serially, one at a time. And some boards are only open for business in daylight hours or on weekends, which greatly slows response. A network of boards, such as "FidoNet," can carry electronic mail from board to board, continent to continent, across huge distances - but at a relative snail's pace, so that a message can take several days to reach its target audience and elicit a reply.

Boards can be grouped by their degree of community. Some boards emphasize the exchange of private, person-to-person electronic mail. Others emphasize public postings and may even purge people who "lurk," merely reading posts but refusing to openly participate. Some boards are intimate and neighborly. Others are frosty and highly technical. Some are little more than storage dumps for software, where users "download" and "upload" programs, but interact among themselves little if at all.

Boards can be grouped by their ease of access. Some boards are entirely public. Others are private and restricted only to personal friends of the sysop. Some boards divide users by status. On these boards, some users, especially beginners, strangers or children, will be restricted to general topics, and perhaps forbidden to post. Favored users, though, are granted the ability to post as they please, and to stay "on-line" as long as they like, even to the disadvantage of other people trying to call in. High-status users can be given access to hidden areas in the board, such as off-color topics, private discussions, and/or valuable software. Favored users may even become "remote sysops" with the power to take remote control of the board through their own home computers. Quite often "remote sysops" end up doing all the work and taking formal control of the enterprise, despite the fact that it's physically located in someone else's house. Sometimes several "co-sysops" share power.

And boards can also be grouped by size. Massive, nationwide commercial networks, such as CompuServe, Delphi, GEnie and Prodigy, are run on mainframe computers and are generally not considered "boards," though they share many of their characteristics, such as electronic mail, discussion topics, libraries of software, and persistent and growing problems with civil-liberties issues. Some private boards have as many as thirty phone-lines and quite sophisticated hardware. And then there are tiny boards.

Boards vary in popularity. Some boards are huge and crowded, where users must claw their way in against a constant busy-signal. Others are huge and empty - there are few things sadder than a formerly flourishing board where no one posts any longer, and the dead conversations of vanished users lie about gathering digital dust. Some boards are tiny and intimate, their telephone

numbers intentionally kept confidential so that only a small number can log on.

And some boards are underground.

Boards can be mysterious entities. The activities of their users can be hard to differentiate from conspiracy. Sometimes they are conspiracies. Boards have harbored, or have been accused of harboring, all manner of fringe groups, and have abetted, or been accused of abetting, every manner of frowned-upon, sleazy, radical, and criminal activity. There are Satanist boards. Nazi boards. Pornographic boards. Pedophile boards. Drugdealing boards. Anarchist boards. Communist boards. Gay and Lesbian boards (these exist in great profusion, many of them quite lively with well-established histories). Religious cult boards. Evangelical boards. Witchcraft boards, hippie boards, punk boards, skateboarder boards. Boards for UFO believers. There may well be boards for serial killers, airline terrorists and professional assassins. There is simply no way to tell. Boards spring up, flourish, and disappear in large numbers, in most every corner of the developed world. Even apparently innocuous public boards can, and sometimes do, harbor secret areas known only to a few. And even on the vast, public, commercial services, private mail is very private - and quite possibly criminal.

Boards cover most every topic imaginable and some that are hard to imagine. They cover a vast spectrum of social activity. However, all board users do have something in common: their possession of computers and phones. Naturally, computers and phones are primary topics of conversation on almost every board.

And hackers and phone phreaks, those utter devotees of computers and phones, live by boards. They swarm by boards. They are bred by boards. By the late 1980s, phone-phreak groups and hacker groups, united by boards, had proliferated fantastically.

As evidence, here is a list of hacker groups compiled by the editors of Phrack on August 8, 1988.

- The Administration. Advanced Telecommunications, Inc. ALIAS. American Tone Travelers. Anarchy Inc. Apple Mafia. The Association. Atlantic Pirates Guild.
- Bad Ass Mother Fuckers. Bellcore. Bell Shock Force. Black Bag.
- Camorra. C&M Productions. Catholics Anonymous. Chaos Computer Club. Chief Executive Officers. Circle Of Death. Circle Of Deneb. Club X. Coalition of Hi-Tech Pirates. Coast-To-Coast. Corrupt Computing. Cult Of The Dead Cow. Custom Retaliations.
- Damage Inc. D&B Communications. The Dange Gang. Dec Hunters. Digital Gang. DPAK.
- Eastern Alliance. The Elite Hackers Guild. Elite Phreakers and Hackers Club. The Elite Society Of America. EPG. Executives Of Crime. Extasyy Elite.
- Fargo 4A. Farmers Of Doom. The Federation. Feds R Us. First Class. Five O. Five Star. Force Hackers. The 414s.
- Hack-A-Trip. Hackers Of America. High Mountain Hackers. High Society. The Hitchhikers.
- IBM Syndicate. The Ice Pirates. Imperial Warlords. Inner Circle. Inner Circle II. Insanity Inc. International Computer Underground Bandits.
- Justice League of America. Kaos Inc. Knights Of Shadow. Knights Of The Round Table.
- League Of Adepts. Legion Of Doom. Legion Of Hackers. Lords Of Chaos. Lunatic Labs, Unlimited.
- Master Hackers. MAD! The Marauders. MD/PhD. Metal Communications, Inc. MetalliBashers, Inc. MBI. Metro Communications. Midwest Pirates Guild.
- NASA Elite. The NATO Association. Neon Knights. Nihilist Order. Order Of The Rose. OSS.
- Pacific Pirates Guild. Phantom Access Associates. PHido PHreaks. The Phirm. Phlash. PhoneLine Phantoms. Phone Phreakers Of America. Phortune 500. Phreak Hack Delinquents. Phreak Hack Destroyers. Phreakers, Hackers, And Laundromat Employees Gang (PHALSE Gang).

- Phreaks Against Geeks. Phreaks Against Phreaks Against Geeks. Phreaks and Hackers of America. Phreaks Anonymous World Wide. Project Genesis. The Punk Mafia. The Racketeers. Red Dawn Text Files. Roscoe Gang.
- SABRE. Secret Circle of Pirates. Secret Service. 707 Club. Shadow Brotherhood. Sharp Inc. 65C02 Elite. Spectral Force. Star League. Stowaways. Strata-Crackers.
- Team Hackers '86. Team Hackers '87. TeleComputist Newsletter Staff. Tribunal Of Knowledge. Triple Entente. Turn Over And Die Syndrome (TOADS). 300 Club. 1200 Club. 2300 Club. 2600 Club. 2601 Club. 2AF. The United Soft WareZ Force. United Technical Underground.
- Ware Brigade. The Warelords. WASP.

Contemplating this list is an impressive, almost humbling business. As a cultural artifact, the thing approaches poetry.

Underground groups - subcultures - can be distinguished from independent cultures by their habit of referring constantly to the parent society. Undergrounds by their nature constantly must maintain a membrane of differentiation. Funny/distinctive clothes and hair, specialized jargon, specialized ghettoized areas in cities, different hours of rising, working, sleeping… The digital underground, which specializes in information, relies very heavily on language to distinguish itself. As can be seen from this list, they make heavy use of parody and mockery. It's revealing to see who they choose to mock.

First, large corporations. We have the Phortune 500, The Chief Executive Officers, Bellcore, IBM Syndicate, SABRE (a computerized reservation service maintained by airlines). The common use of "Inc." is telling - none of these groups are actual corporations, but take clear delight in mimicking them.

Second, governments and police. NASA Elite, NATO Association. "Feds R Us" and "Secret Service" are fine bits of fleering boldness. OSS - the Office of Strategic Services was the forerunner of the CIA.

Third, criminals. Using stigmatizing pejoratives as a perverse badge of honor is a time-honored tactic for subcultures: punks, gangs, delinquents, mafias, pirates, bandits, racketeers.

Specialized orthography, especially the use of "ph" for "f" and "z" for the plural "s," are instant recognition symbols. So is the use of the numeral "0" for the letter "O" - computer-software orthography generally features a slash through the zero, making the distinction obvious.

Some terms are poetically descriptive of computer intrusion: the Stowaways, the Hitchhikers, the PhoneLine Phantoms, Coast-to-Coast. Others are simple bravado and vainglorious puffery. (Note the insistent use of the terms "elite" and "master.") Some terms are blasphemous, some obscene, others merely cryptic - anything to puzzle, offend, confuse, and keep the straights at bay.

Many hacker groups further re-encrypt their names by the use of acronyms: United Technical Underground becomes UTU, Farmers of Doom become FoD, the United SoftWareZ Force becomes, at its own insistence, "TuSwF," and woe to the ignorant rodent who capitalizes the wrong letters.

It should be further recognized that the members of these groups are themselves pseudonymous. If you did, in fact, run across the "PhoneLine Phantoms," you would find them to consist of "Carrier Culprit," "The Executioner," "Black Majik," "Egyptian Lover," "Solid State," and "Mr Icom." "Carrier Culprit" will likely be referred to by his friends as "CC," as in, "I got these dialups from CC of PLP."

It's quite possible that this entire list refers to as few as a thousand people. It is not a complete list of underground groups - there has never been such a list, and there never will be. Groups rise, flourish, decline, share membership, maintain a cloud of wannabes and casual hangers-on. People pass in and out, are ostracized, get bored, are busted by police, or are cornered by telco security and presented with huge bills. Many "underground groups" are software pirates, "warez d00dz," who might break copy protection and pirate programs, but likely wouldn't dare to intrude on a computer-system. It is hard to estimate the true population of the digital underground. There is constant turnover. Most hackers start young, come and go, then drop out at age 22 - the age of college graduation. And a large majority of "hackers" access pirate

boards, adopt a handle, swipe software and perhaps abuse a phone-code or two, while never actually joining the elite.

Some professional informants, who make it their business to retail knowledge of the underground to paymasters in private corporate security, have estimated the hacker population at as high as fifty thousand. This is likely highly inflated, unless one counts every single teenage software pirate and petty phone-booth thief. My best guess is about 5,000 people. Of these, I would guess that as few as a hundred are truly "elite" - active computer intruders, skilled enough to penetrate sophisticated systems and truly to worry corporate security and law enforcement.

Another interesting speculation is whether this group is growing or not. Young teenage hackers are often convinced that hackers exist in vast swarms and will soon dominate the cybernetic universe. Older and wiser veterans, perhaps as wizened as 24 or 25 years old, are convinced that the glory days are long gone, that the cops have the underground's number now, and that kids these days are dirt-stupid and just want to play Nintendo.

My own assessment is that computer intrusion, as a non-profit act of intellectual exploration and mastery, is in slow decline, at least in the United States; but that electronic fraud, especially telecommunication crime, is growing by leaps and bounds.

One might find a useful parallel to the digital underground in the drug underground. There was a time, now much-obscured by historical revisionism, when Bohemians freely shared joints at concerts, and hip, smallscale marijuana dealers might turn people on just for the sake of enjoying a long stoned conversation about the Doors and Allen Ginsberg. Now drugs are increasingly verboten, except in a high-stakes, highly-criminal world of highly addictive drugs. Over years of disenchantment and police harassment, a vaguely ideological, free-wheeling drug underground has relinquished the business of drug-dealing to a far more savage criminal hard-core. This is not a pleasant prospect to contemplate, but the analogy is fairly compelling.

What does an underground board look like? What distinguishes it from a standard board? It isn't necessarily the conversation - hackers often talk about common board topics, such as hardware, software, sex, science fiction, current events, politics, movies, personal gossip. Underground boards can best be distinguished by their files, or "philes," pre-composed texts which teach the techniques and ethos of the underground. These are prized reservoirs of forbidden knowledge. Some are anonymous, but most proudly bear the handle of the "hacker" who has created them, and his group affiliation, if he has one. Here is a partial table-of-contents of philes from an underground board, somewhere in the heart of middle America, circa 1991. The descriptions are mostly self-explanatory.

Table of contents

- 5406 06-11-91 Hacking Bank America BANKAMER.ZIP
- 4481 06-11-91 Chilton Hacking CHHACK.ZIP
- 4118 06-11-91 Hacking Citibank CITIBANK.ZIP
- 3241 06-11-91 Hacking Mtc Credit Company CREDIMTC.ZIP
- 5159 06-11-91 Hackers Digest DIGEST.ZIP
- 14031 06-11-91 How To Hack HACK.ZIP
- 5073 06-11-91 Basics Of Hacking HACKBAS.ZIP
- 42774 06-11-91 Hackers Dictionary HACKDICT.ZIP
- 57938 06-11-91 Hacker Info HACKER.ZIP
- 3148 06-11-91 Hackers Manual HACKERME.ZIP
- 4814 06-11-91 Hackers Handbook HACKHAND.ZIP
- 48290 06-11-91 Hackers Thesis HACKTHES.ZIP
- 4696 06-11-91 Hacking Vms Systems HACKVMS.ZIP
- 3830 06-11-91 Hacking Macdonalds (Home Of The Archs) MCDON.ZIP
- 15525 06-11-91 Phortune 500 Guide To Unix P500UNIX.ZIP
- 8411 06-11-91 Radio Hacking RADHACK.ZIP

- 4096 12-25-89 Suggestions For Trashing TAOTRASH.DOC
- 5063 06-11-91 Technical Hacking TECHHACK.ZIP

The files above are do-it-yourself manuals about computer intrusion. The above is only a small section of a much larger library of hacking and phreaking techniques and history. We now move into a different and perhaps surprising area.

Anarchy

- 3641 06-11-91 Anarchy Files ANARC.ZIP
- 63703 06-11-91 Anarchist Book ANARCHST.ZIP
- 2076 06-11-91 Anarchy At Home ANARCHY.ZIP
- 6982 06-11-91 Anarchy No 3 ANARCHY3.ZIP
- 2361 06-11-91 Anarchy Toys ANARCTOY.ZIP
- 2877 06-11-91 Anti-modem Weapons ANTIMODM.ZIP
- 4494 06-11-91 How To Make An Atom Bomb ATOM.ZIP
- 3982 06-11-91 Barbiturate Formula BARBITUA.ZIP
- 2810 06-11-91 Black Powder Formulas BLCKPWDR.ZIP
- 3765 06-11-91 How To Make Bombs BOMB.ZIP
- 2036 06-11-91 Things That Go Boom BOOM.ZIP
- 1926 06-11-91 Chlorine Bomb CHLORINE.ZIP
- 1500 06-11-91 Anarchy Cook Book COOKBOOK.ZIP
- 3947 06-11-91 Destroy Stuff DESTROY.ZIP
- 2576 06-11-91 Dust Bomb DUSTBOMB.ZIP
- 3230 06-11-91 Electronic Terror ELECTERR.ZIP
- 2598 06-11-91 Explosives 1 EXPLOS1.ZIP
- 18051 06-11-91 More Explosives EXPLOSIV.ZIP
- 4521 06-11-91 Ez-stealing EZSTEAL.ZIP
- 2240 06-11-91 Flame Thrower FLAME.ZIP
- 2533 06-11-91 Flashlight Bomb FLASHLT.ZIP
- 2906 06-11-91 How To Make An Fm Bug FMBUG.ZIP
- 2139 06-11-91 Home Explosives OMEEXPL.ZIP
- 3332 06-11-91 How To Break In HOW2BRK.ZIP
- 2990 06-11-91 Letter Bomb LETTER.ZIP
- 2199 06-11-91 How To Pick Locks LOCK.ZIP
- 3991 06-11-91 Briefcase Locks MRSHIN.ZIP
- 3563 06-11-91 Napalm At Home NAPALM.ZIP
- 3158 06-11-91 Fun With Nitro NITRO.ZIP
- 2962 06-11-91 Paramilitary Info PARAMIL.ZIP
- 3398 06-11-91 Picking Locks PICKING.ZIP
- 2137 06-11-91 Pipe Bomb PIPEBOMB.ZIP
- 3987 06-11-91 Formulas With Potassium POTASS.ZIP
- 11074 08-03-90 More Pranks To Pull On Idiots! PRANK.TXT
- 4447 06-11-91 Revenge Tactics REVENGE.ZIP
- 2590 06-11-91 Rockets For Fun ROCKET.ZIP
- 3385 06-11-91 How To Smuggle SMUGGLE.ZIP

Holy Cow! The damned thing is full of stuff about bombs!

What are we to make of this?

First, it should be acknowledged that spreading knowledge about demolitions to teenagers is a highly and deliberately antisocial act.

It is not, however, illegal.

Second, it should be recognized that most of these philes were in fact written by teenagers. Most adult American males who can remember their teenage years will recognize that the notion of building a flamethrower in your garage is an incredibly neat-o idea. Actually building a flamethrower in your garage,

however, is fraught with discouraging difficulty. Stuffing gunpowder into a booby-trapped flashlight, so as to blow the arm off your high-school vice-principal, can be a thing of dark beauty to contemplate. Actually committing assault by explosives will earn you the sustained attention of the federal Bureau of Alcohol, Tobacco and Firearms.

Some people, however, will actually try these plans. A determinedly murderous American teenager can probably buy or steal a handgun far more easily than he can brew fake "napalm" in the kitchen sink. Nevertheless, if temptation is spread before people a certain number will succumb, and a small minority will actually attempt these stunts. A large minority of that small minority will either fail or, quite likely, maim themselves, since these "philes" have not been checked for accuracy, are not the product of professional experience, and are often highly fanciful. But the gloating menace of these philes is not to be entirely dismissed.

Hackers may not be "serious" about bombing; if they were, we would hear far more about exploding flashlights, homemade bazookas, and gym teachers poisoned by chlorine and potassium. However, hackers are very serious about forbidden knowledge. They are possessed not merely by curiosity, but by a positive lust to know. The desire to know what others don't is scarcely new. But the intensity of this desire, as manifested by these young technophilic denizens of the Information Age, may in fact be new, and may represent some basic shift in social values - a harbinger of what the world may come to, as society lays more and more value on the possession, assimilation and retailing of information as a basic commodity of daily life.

There have always been young men with obsessive interests in these topics. Never before, however, have they been able to network so extensively and easily, and to propagandize their interests with impunity to random passers-by. High-school teachers will recognize that there's always one in a crowd, but when the one in a crowd escapes control by jumping into the phone-lines, and becomes a hundred such kids all together on a board, then trouble is brewing visibly. The urge of authority to do something, even something drastic, is hard to resist. And in 1990, authority did something. In fact authority did a great deal

-Section 4-

The process by which boards create hackers goes something like this. A youngster becomes interested in computers - usually, computer games. He hears from friends that "bulletin boards" exist where games can be obtained for free. (Many computer games are "freeware," not copyrighted - invented simply for the love of it and given away to the public; some of these games are quite good.) He bugs his parents for a modem, or quite often, uses his parents' modem.

The world of boards suddenly opens up. Computer games can be quite expensive, real budget-breakers for a kid, but pirated games, stripped of copy protection, are cheap or free. They are also illegal, but it is very rare, almost unheard of, for a small-scale software pirate to be prosecuted. Once "cracked" of its copy protection, the program, being digital data, becomes infinitely reproducible. Even the instructions to the game, any manuals that accompany it, can be reproduced as text files, or photocopied from legitimate sets. Other users on boards can give many useful hints in game-playing tactics. And a youngster with an infinite supply of free computer games can certainly cut quite a swath among his modemless friends. And boards are pseudonymous. No one need know that you're fourteen years old - with a little practice at subterfuge, you can talk to adults about adult things, and be accepted and taken seriously! You can even pretend to be a girl, or an old man, or anybody you can imagine. If you find this kind of deception gratifying, there is ample opportunity to hone your ability on boards. But local boards can grow stale. And almost every board maintains a list of phone-numbers to other boards, some in distant, tempting, exotic locales. Who knows what they're up to, in Oregon or Alaska or Florida or California? It's very easy to find out - just order the modem to call through its software - nothing to this, just typing on a key-

board, the same thing you would do for most any computer game. The machine reacts swiftly and in a few seconds you are talking to a bunch of interesting people on another seaboard.

And yet the bills for this trivial action can be staggering! Just by going tippety-tap with your fingers, you may have saddled your parents with four hundred bucks in long-distance charges, and gotten chewed out but good. That hardly seems fair.

How horrifying to have made friends in another state and to be deprived of their company - and their software - just because telephone companies demand absurd amounts of money! How painful, to be restricted to boards in one's own area code - what the heck is an "area code" anyway, and what makes it so special? A few grumbles, complaints, and innocent questions of this sort will often elicit a sympathetic reply from another board user - someone with some stolen codes to hand. You dither a while, knowing this isn't quite right, then you make up your mind to try them anyhow - and they work! Suddenly you're doing something even your parents can't do. Six months ago you were just some kid - now, you're the Crimson Flash of Area Code 512! You're bad - you're nationwide! Maybe you'll stop at a few abused codes. Maybe you'll decide that boards aren't all that interesting after all, that it's wrong, not worth the risk - but maybe you won't. The next step is to pick up your own repeat-dialling program - to learn to generate your own stolen codes. (This was dead easy five years ago, much harder to get away with nowadays, but not yet impossible.) And these dialling programs are not complex or intimidating - some are as small as twenty lines of software. Now, you too can share codes. You can trade codes to learn other techniques. If you're smart enough to catch on, and obsessive enough to want to bother, and ruthless enough to start seriously bending rules, then you'll get better, fast. You start to develop a rep. You move up to a heavier class of board - a board with a bad attitude, the kind of board that naive dopes like your classmates and your former self have never even heard of! You pick up the jargon of phreaking and hacking from the board. You read a few of those anarchy philes - and man, you never realized you could be a real outlaw without ever leaving your bedroom.

You still play other computer games, but now you have a new and bigger game. This one will bring you a different kind of status than destroying even eight zillion lousy space invaders.

Hacking is perceived by hackers as a "game." This is not an entirely unreasonable or sociopathic perception. You can win or lose at hacking, succeed or fail, but it never feels "real." It's not simply that imaginative youngsters sometimes have a hard time telling "make-believe" from "real life." Cyberspace is not real! "Real" things are physical objects like trees and shoes and cars. Hacking takes place on a screen. Words aren't physical, numbers (even telephone numbers and credit card numbers) aren't physical. Sticks and stones may break my bones, but data will never hurt me. Computers simulate reality, like computer games that simulate tank battles or dogfights or spaceships. Simulations are just makebelieve, and the stuff in computers is not real.

Consider this: if "hacking" is supposed to be so serious and real-life and dangerous, then how come nine-year-old kids have computers and modems? You wouldn't give a nine year old his own car, or his own rifle, or his own chainsaw - those things are "real."

People underground are perfectly aware that the "game" is frowned upon by the powers that be. Word gets around about busts in the underground. Publicizing busts is one of the primary functions of pirate boards, but they also promulgate an attitude about them, and their own idiosyncratic ideas of justice. The users of underground boards won't complain if some guy is busted for crashing systems, spreading viruses, or stealing money by wirefraud. They may shake their heads with a sneaky grin, but they won't openly defend these practices. But when a kid is charged with some theoretical amount of theft: $233,846.14, for instance, because he sneaked into a computer and copied something, and kept it in his house on a floppy disk - this is regarded as a sign of near insanity from prosecutors, a sign that they've drastically mistaken the immaterial game of computing for their real and boring everyday world of fatcat corporate money.

It's as if big companies and their suck-up lawyers think that computing belongs to them, and they can retail it with price stickers, as if it were boxes of laundry soap! But pricing "information" is like trying to price air or price dreams. Well, anybody on a pirate board knows that computing can be, and ought to be, free. Pirate boards are little independent worlds in cyberspace, and they don't belong to anybody but the underground. Underground boards aren't "brought to you by Procter & Gamble."

To log on to an underground board can mean to experience liberation, to enter a world where, for once, money isn't everything and adults don't have all the answers.

Let's sample another vivid hacker manifesto. Here are some excerpts from "The Conscience of a Hacker," by "The Mentor," from Phrack Volume One, Issue 7, Phile 3.

"I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me.(…)

"And then it happened… a door opened to a world… rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from day-to-day incompetencies is sought… a board is found. `This is it… this is where I belong…' "I know everyone here… even if I've never met them, never talked to them, may never hear from them again… I know you all…(…) "This is our world now… the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore… and you call us criminals. We seek after knowledge… and you call us criminals. We exist without skin color, without nationality, without religious bias… and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat and lie to us and try to make us believe that it's for our own good, yet we're the criminals.

"Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for."

-Section 5-

There have been underground boards almost as long as there have been boards. One of the first was 8BBS, which became a stronghold of the West Coast phonephreak elite. After going on-line in March 1980, 8BBS sponsored "Susan Thunder," and "Tuc," and, most notoriously, "the Condor." "The Condor" bore the singular distinction of becoming the most vilified American phreak and hacker ever. Angry underground associates, fed up with Condor's peevish behavior, turned him in to police, along with a heaping double-helping of outrageous hacker legendry. As a result, Condor was kept in solitary confinement for seven months, for fear that he might start World War Three by triggering missile silos from the prison payphone. (Having served his time, Condor is now walking around loose; WWIII has thus far conspicuously failed to occur.)

The sysop of 8BBS was an ardent free-speech enthusiast who simply felt that any attempt to restrict the expression of his users was unconstitutional and immoral. Swarms of the technically curious entered 8BBS and emerged as phreaks and hackers, until, in 1982, a friendly 8BBS alumnus passed the sysop a new modem which had been purchased by credit card fraud. Police took this opportunity to seize the entire board and remove what they considered an attractive nuisance.

Plovernet was a powerful East Coast pirate board that operated in both New York and Florida. Owned and operated by teenage hacker "Quasi Moto," Plovernet attracted five hundred eager users in 1983. "Emmanuel Goldstein" was one-time co-sysop of Plovernet, along with "Lex Luthor," founder of the "Legion of Doom" group. Plovernet bore the signal honor of being the original home of the "Legion of Doom," about which the reader will be hearing a great deal, soon.

"Pirate-80," or "P-80," run by a sysop known as "Scan Man," got into the game very early in Charleston, and continued steadily for years. P-80 flourished so flagrantly that even its most hardened users became nervous, and some

slanderously speculated that "Scan Man" must have ties to corporate security, a charge he vigorously denied.

"414 Private" was the home board for the first group to attract conspicuous trouble, the teenage "414 Gang," whose intrusions into Sloan-Kettering Cancer Center and Los Alamos military computers were to be a nine-days wonder in 1982.

At about this time, the first software piracy boards began to open up, trading cracked games for the Atari 800 and the Commodore C64. Naturally these boards were heavily frequented by teenagers. And with the 1983 release of the hacker-thriller movie War Games, the scene exploded. It seemed that every kid in America had demanded and gotten a modem for Christmas. Most of these dabbler wannabes put their modems in the attic after a few weeks, and most of the remainder minded their P's and Q's and stayed well out of hot water. But some stubborn and talented diehards had this hacker kid in War Games figured for a happening dude. They simply could not rest until they had contacted the underground - or, failing that, created their own.

In the mid-80s, underground boards sprang up like digital fungi. ShadowSpawn Elite. Sherwood Forest I, II, and III. Digital Logic Data Service in Florida, sysoped by no less a man than "Digital Logic" himself; Lex Luthor of the Legion of Doom was prominent on this board, since it was in his area code. Lex's own board, "Legion of Doom," started in 1984. The Neon Knights ran a network of Applehacker boards: Neon Knights North, South, East and West. Free World II was run by "Major Havoc." Lunatic Labs is still in operation as of this writing. Dr. Ripco in Chicago, an anything-goes anarchist board with an extensive and raucous history, was seized by Secret Service agents in 1990 on Sundevil day, but up again almost immediately, with new machines and scarcely diminished vigor.

The St. Louis scene was not to rank with major centers of American hacking such as New York and L.A. But St. Louis did rejoice in possession of "Knight Lightning" and "Taran King," two of the foremost journalists native to the underground. Missouri boards like Metal Shop, Metal Shop Private, Metal Shop Brewery, may not have been the heaviest boards around in terms of illicit expertise. But they became boards where hackers could exchange social gossip and try to figure out what the heck was going on nationally - and internationally. Gossip from Metal Shop was put into the form of news files, then assembled into a general electronic publication, Phrack, a portmanteau title coined from "phreak" and "hack." The Phrack editors were as obsessively curious about other hackers as hackers were about machines.

Phrack, being free of charge and lively reading, began to circulate throughout the underground. As Taran King and Knight Lightning left high school for college, Phrack began to appear on mainframe machines linked to BITNET, and, through BITNET to the "Internet," that loose but extremely potent not-for-profit network where academic, governmental and corporate machines trade data through the UNIX TCP/IP protocol. (The "Internet Worm" of November 2-3,1988, created by Cornell grad student Robert Morris, was to be the largest and bestpublicized computer intrusion scandal to date. Morris claimed that his ingenious "worm" program was meant to harmlessly explore the Internet, but due to bad programming, the Worm replicated out of control and crashed some six thousand Internet computers. Smaller scale and less ambitious Internet hacking was a standard for the underground elite.) Most any underground board not hopelessly lame and out-of-it would feature a complete run of Phrack - and, possibly, the lesser-known standards of the underground: the Legion of Doom Technical Journal, the obscene and raucous Cult of the Dead Cow files, P/HUN magazine, Pirate, the Syndicate Reports, and perhaps the highly anarcho-political Activist Times Incorporated.

Possession of Phrack on one's board was prima facie evidence of a bad attitude. Phrack was seemingly everywhere, aiding, abetting, and spreading the underground ethos. And this did not escape the attention of corporate security or the police.

We now come to the touchy subject of police and boards. Police, do, in fact, own boards. In 1989, there were police-sponsored boards in California, Colorado, Florida, Georgia, Idaho, Michigan, Missouri, Texas, and Virginia: boards such as "Crime Bytes," "Crimestoppers," "All Points" and "Bullet-N-

Board." Police officers, as private computer enthusiasts, ran their own boards in Arizona, California, Colorado, Connecticut, Florida, Missouri, Maryland, New Mexico, North Carolina, Ohio, Tennessee and Texas. Police boards have often proved helpful in community relations. Sometimes crimes are reported on police boards.

Sometimes crimes are committed on police boards. This has sometimes happened by accident, as naive hackers blunder onto police boards and blithely begin offering telephone codes. Far more often, however, it occurs through the now almost-traditional use of "sting boards." The first police sting-boards were established in 1985: "Underground Tunnel" in Austin, Texas, whose sysop Sgt. Robert Ansley called himself "Pluto" - "The Phone Company" in Phoenix, Arizona, run by Ken MacLeod of the Maricopa County Sheriff's office - and Sgt. Dan Pasquale's board in Fremont, California. Sysops posed as hackers, and swiftly garnered coteries of ardent users, who posted codes and loaded pirate software with abandon, and came to a sticky end.

Sting boards, like other boards, are cheap to operate, very cheap by the standards of undercover police operations. Once accepted by the local underground, sysops will likely be invited into other pirate boards, where they can compile more dossiers. And when the sting is announced and the worst offenders arrested, the publicity is generally gratifying. The resultant paranoia in the underground - perhaps more justly described as a "deterrence effect" - tends to quell local lawbreaking for quite a while.

Obviously police do not have to beat the underbrush for hackers. On the contrary, they can go trolling for them. Those caught can be grilled. Some become useful informants. They can lead the way to pirate boards all across the country.

And boards all across the country showed the sticky fingerprints of Phrack, and of that loudest and most flagrant of all underground groups, the "Legion of Doom."

The term "Legion of Doom" came from comic books. The Legion of Doom, a conspiracy of costumed supervillains headed by the chrome-domed criminal ultramastermind Lex Luthor, gave Superman a lot of four-color graphic trouble for a number of decades. Of course, Superman, that exemplar of Truth, Justice, and the American Way, always won in the long run. This didn't matter to the hacker Doomsters - "Legion of Doom" was not some thunderous and evil Satanic reference, it was not meant to be taken seriously. "Legion of Doom" came from funny-books and was supposed to be funny. "Legion of Doom" did have a good mouthfilling ring to it, though. It sounded really cool. Other groups, such as the "Farmers of Doom," closely allied to LoD, recognized this grandiloquent quality, and made fun of it. There was even a hacker group called "Justice League of America," named after Superman's club of true-blue crimefighting superheros.

But they didn't last; the Legion did. The original Legion of Doom, hanging out on Quasi Moto's Plovernet board, were phone phreaks. They weren't much into computers. "Lex Luthor" himself (who was under eighteen when he formed the Legion) was a COSMOS expert, COSMOS being the "Central System for Mainframe Operations," a telco internal computer network. Lex would eventually become quite a dab hand at breaking into IBM mainframes, but although everyone liked Lex and admired his attitude, he was not considered a truly accomplished computer intruder. Nor was he the "mastermind" of the Legion of Doom - LoD were never big on formal leadership. As a regular on Plovernet and sysop of his "Legion of Doom BBS," Lex was the Legion's cheerleader and recruiting officer.

Legion of Doom began on the ruins of an earlier phreak group, The Knights of Shadow. Later, LoD was to subsume the personnel of the hacker group "Tribunal of Knowledge." People came and went constantly in LoD; groups split up or formed offshoots.

Early on, the LoD phreaks befriended a few computer-intrusion enthusiasts, who became the associated "Legion of Hackers." Then the two groups conflated into the "Legion of Doom/Hackers," or LoD/H. When the original "hacker" wing, Messrs. "CompuPhreak" and "Phucked Agent 04," found other matters to occupy their time, the extra "/H" slowly atrophied out of the name; but by this time the phreak wing, Messrs. Lex Luthor, "Blue Archer," "Gary Seven," "Kerrang

Khan," "Master of Impact," "Silver Spy," "The Marauder," and "The Videosmith," had picked up a plethora of intrusion expertise and had become a force to be reckoned with.

LoD members seemed to have an instinctive understanding that the way to real power in the underground lay through covert publicity. LoD were flagrant. Not only was it one of the earliest groups, but the members took pains to widely distribute their illicit knowledge. Some LoD members, like "The Mentor," were close to evangelical about it. Legion of Doom Technical Journal began to show up on boards throughout the underground.

LoD Technical Journalwas named in cruel parody of the ancient and honored AT&T Technical Journal. The material in these two publications was quite similar - much of it, adopted from public journals and discussions in the telco community. And yet, the predatory attitude of LoD made even its most innocuous data seem deeply sinister; an outrage; a clear and present danger.

To see why this should be, let's consider the following (invented) paragraphs, as a kind of thought experiment.

(A) "W. Fred Brown, AT&T Vice President for Advanced Technical Development, testified May 8 at a Washington hearing of the National Telecommunications and Information Administration (NTIA), regarding Bellcore's GARDEN project. GARDEN (Generalized Automatic Remote Distributed Electronic Network) is a telephone-switch programming tool that makes it possible to develop new telecom services, including hold-on-hold and customized message transfers, from any keypad terminal, within seconds. The GARDEN prototype combines centrex lines with a minicomputer using UNIX operating system software."

(B) "Crimson Flash 512 of the Centrex Mobsters reports: D00dz, you wouldn't believe this GARDEN bullshit Bellcore's just come up with! Now you don't even need a lousy Commodore to reprogram a switch - just log on to GARDEN as a technician, and you can reprogram switches right off the keypad in any public phone booth! You can give yourself hold-on-hold and customized message transfers, and best of all, the thing is run off (notoriously insecure) centrex lines using - get this - standard UNIX software! Ha ha ha ha!"

Message (A), couched in typical technobureaucratese, appears tedious and almost unreadable. (A) scarcely seems threatening or menacing. Message (B), on the other hand, is a dreadful thing, prima facie evidence of a dire conspiracy, definitely not the kind of thing you want your teenager reading. The information, however, is identical. It is public information, presented before the federal government in an open hearing. It is not "secret." It is not "proprietary." It is not even "confidential." On the contrary, the development of advanced software systems is a matter of great public pride to Bellcore. However, when Bellcore publicly announces a project of this kind, it expects a certain attitude from the public - something along the lines of gosh wow, you guys are great, keep that up, whatever it is - certainly not cruel mimickry, one-upmanship and outrageous speculations about possible security holes.

Now put yourself in the place of a policeman confronted by an outraged parent, or telco official, with a copy of Version (B). This well-meaning citizen, to his horror, has discovered a local bulletin-board carrying outrageous stuff like (B), which his son is examining with a deep and unhealthy interest. If (B) were printed in a book or magazine, you, as an American law enforcement officer, would know that it would take a hell of a lot of trouble to do anything about it; but it doesn't take technical genius to recognize that if there's a computer in your area harboring stuff like (B), there's going to be trouble.

In fact, if you ask around, any computer-literate cop will tell you straight out that boards with stuff like (B) are the source of trouble. And the worst source of trouble on boards are the ringleaders inventing and spreading stuff like (B). If it weren't for these jokers, there wouldn't be any trouble.

And Legion of Doom were on boards like nobody else. Plovernet. The Legion of Doom Board. The Farmers of Doom Board. Metal Shop. OSUNY. Blottoland. Private Sector. Atlantis. Digital Logic. Hell Phrozen Over.

LoD members also ran their own boards. "Silver Spy" started his own board, "Catch-22," considered one of the heaviest around. So did "Mentor," with his "Phoenix Project." When they didn't run boards themselves, they showed up on

other people's boards, to brag, boast, and strut. And where they themselves didn't go, their philes went, carrying evil knowledge and an even more evil attitude. As early as 1986, the police were under the vague impression that everyone in the underground was Legion of Doom. LoD was never that large - considerably smaller than either "Metal Communications" or "The Administration," for instance - but LoD got tremendous press. Especially in Phrack, which at times read like an LoD fan magazine; and Phrack was everywhere, especially in the offices of telco security. You couldn't get busted as a phone phreak, a hacker, or even a lousy codes kid or warez dood, without the cops asking if you were LoD.

This was a difficult charge to deny, as LoD never distributed membership badges or laminated ID cards. If they had, they would likely have died out quickly, for turnover in their membership was considerable. LoD was less a high-tech street-gang than an ongoing state of mind. LoD was the Gang That Refused to Die. By 1990, LoD had ruled for ten years, and it seemed weird to police that they were continually busting people who were only sixteen years old. All these teenage small-timers were pleading the tiresome hacker litany of "just curious, no criminal intent." Somewhere at the center of this conspiracy there had to be some serious adult masterminds, not this seemingly endless supply of myopic suburban white kids with high SATs and funny haircuts.

There was no question that most any American hacker arrested would "know" LoD. They knew the handles of contributors to LoD Tech Journal, and were likely to have learned their craft through LoD boards and LoD activism. But they'd never met anyone from LoD. Even some of the rotating cadre who were actually and formally "in LoD" knew one another only by board-mail and pseudonyms. This was a highly unconventional profile for a criminal conspiracy. Computer networking, and the rapid evolution of the digital underground, made the situation very diffuse and confusing.

Furthermore, a big reputation in the digital underground did not coincide with one's willingness to commit "crimes." Instead, reputation was based on cleverness and technical mastery. As a result, it often seemed that the heavier the hackers were, the less likely they were to have committed any kind of common, easily prosecutable crime. There were some hackers who could really steal. And there were hackers who could really hack. But the two groups didn't seem to overlap much, if at all. For instance, most people in the underground looked up to "Emmanuel Goldstein" of 2600 as a hacker demigod. But Goldstein's publishing activities were entirely legal - Goldstein just printed dodgy stuff and talked about politics, he didn't even hack. When you came right down to it, Goldstein spent half his time complaining that computer security wasn't strong enough and ought to be drastically improved across the board!

Truly heavy-duty hackers, those with serious technical skills who had earned the respect of the underground, never stole money or abused credit cards. Sometimes they might abuse phone-codes - but often, they seemed to get all the free phone-time they wanted without leaving a trace of any kind.

The best hackers, the most powerful and technically accomplished, were not professional fraudsters. They raided computers habitually, but wouldn't alter anything, or damage anything. They didn't even steal computer equipment - most had day-jobs messing with hardware, and could get all the cheap secondhand equipment they wanted. The hottest hackers, unlike the teenage wannabes, weren't snobs about fancy or expensive hardware. Their machines tended to be raw second-hand digital hot-rods full of custom add-ons that they'd cobbled together out of chickenwire, memory chips and spit. Some were adults, computer software writers and consultants by trade, and making quite good livings at it. Some of them actually worked for the phone company - and for those, the "hackers" actually found under the skirts of Ma Bell, there would be little mercy in 1990.

It has long been an article of faith in the underground that the "best" hackers never get caught. They're far too smart, supposedly. They never get caught because they never boast, brag, or strut. These demigods may read underground boards (with a condescending smile), but they never say anything there. The "best" hackers, according to legend, are adult computer professionals, such as mainframe system administrators, who already know the ins and

outs of their particular brand of security. Even the "best" hacker can't break in to just any computer at random: the knowledge of security holes is too specialized, varying widely with different software and hardware. But if people are employed to run, say, a UNIX mainframe or a VAX/VMS machine, then they tend to learn security from the inside out. Armed with this knowledge, they can look into most anybody else's UNIX or VMS without much trouble or risk, if they want to. And, according to hacker legend, of course they want to, so of course they do. They just don't make a big deal of what they've done. So nobody ever finds out.

It is also an article of faith in the underground that professional telco people "phreak" like crazed weasels. Of course they spy on Madonna's phone calls - I mean, wouldn't you? Of course they give themselves free long-distance - why the hell should they pay, they're running the whole shebang! It has, as a third matter, long been an article of faith that any hacker caught can escape serious punishment if he confesses how he did it. Hackers seem to believe that governmental agencies and large corporations are blundering about in cyberspace like eyeless jellyfish or cave salamanders. They feel that these large but pathetically stupid organizations will proffer up genuine gratitude, and perhaps even a security post and a big salary, to the hot-shot intruder who will deign to reveal to them the supreme genius of his modus operandi. In the case of longtime LoD member "Control-C," this actually happened, more or less. Control-C had led Michigan Bell a merry chase, and when captured in 1987, he turned out to be a bright and apparently physically harmless young fanatic, fascinated by phones. There was no chance in hell that Control-C would actually repay the enormous and largely theoretical sums in long-distance service that he had accumulated from Michigan Bell. He could always be indicted for fraud or computer-intrusion, but there seemed little real point in this - he hadn't physically damaged any computer. He'd just plead guilty, and he'd likely get the usual slap-on-the-wrist, and in the meantime it would be a big hassle for Michigan Bell just to bring up the case. But if kept on the payroll, he might at least keep his fellow hackers at bay.

There were uses for him. For instance, a contrite Control-C was featured on Michigan Bell internal posters, sternly warning employees to shred their trash. He'd always gotten most of his best inside info from "trashing" - raiding telco dumpsters, for useful data indiscreetly thrown away. He signed these posters, too. Control-C had become something like a Michigan Bell mascot. And in fact, Control-C did keep other hackers at bay. Little hackers were quite scared of Control-C and his heavy-duty Legion of Doom friends. And big hackers were his friends and didn't want to screw up his cushy situation.

No matter what one might say of LoD, they did stick together. When "Wasp," an apparently genuinely malicious New York hacker, began crashing Bellcore machines, Control-C received swift volunteer help from "the Mentor" and the Georgia LoD wing made up of "The Prophet," "Urvile," and "Leftist." Using Mentor's Phoenix Project board to coordinate, the Doomsters helped telco security to trap Wasp, by luring him into a machine with a tap and line-trace installed. Wasp lost. LoD won! And my, did they brag.

Urvile, Prophet and Leftist were well-qualified for this activity, probably more so even than the quite accomplished Control-C. The Georgia boys knew all about phone switching-stations. Though relative johnny-come-latelies in the Legion of Doom, they were considered some of LoD's heaviest guys, into the hairiest systems around. They had the good fortune to live in or near Atlanta, home of the sleepy and apparently tolerant BellSouth RBOC.

As RBOC security went, BellSouth were "cake." US West (of Arizona, the Rockies and the Pacific Northwest) were tough and aggressive, probably the heaviest RBOC around. Pacific Bell, California's PacBell, were sleek, high-tech, and longtime veterans of the LA phone-phreak wars. NYNEX had the misfortune to run the New York City area, and were warily prepared for most anything. Even Michigan Bell, a division of the Ameritech RBOC, at least had the elementary sense to hire their own hacker as a useful scarecrow. But BellSouth, even though their corporate P.R. proclaimed them to have "Everything You Expect From a Leader," were pathetic.

When rumor about LoD's mastery of Georgia's switching network got around to BellSouth through Bellcore and telco security scuttlebutt, they at first

refused to believe it. If you paid serious attention to every rumor out and about these hacker kids, you would hear all kinds of wacko saucer-nut nonsense: that the National Security Agency monitored all American phone calls, that the CIA and DEA tracked traffic on bulletin-boards with wordanalysis programs, that the Condor could start World War III from a payphone.

If there were hackers into BellSouth switching stations, then how come nothing had happened? Nothing had been hurt. BellSouth's machines weren't crashing. BellSouth wasn't suffering especially badly from fraud. BellSouth's customers weren't complaining. BellSouth was headquartered in Atlanta, ambitious metropolis of the new high-tech Sunbelt; and BellSouth was upgrading its network by leaps and bounds, digitizing the works left, right and center. They could hardly be considered sluggish or naive. BellSouth's technical expertise was second to none, thank you kindly.

But then came the Florida business.

On June 13, 1989, callers to the Palm Beach County Probation Department, in Delray Beach, Florida, found themselves involved in a remarkable discussion with a phone sex worker named "Tina" in New York State. Somehow, any call to this probation office near Miami was instantly and magically transported across state lines, at no extra charge to the user, to a pornographic phone sex hotline hundreds of miles away!

This practical joke may seem utterly hilarious at first hearing, and indeed there was a good deal of chuckling about it in phone phreak circles, including the Autumn 1989 issue of 2600. But for Southern Bell (the division of the BellSouth RBOC supplying local service for Florida, Georgia, North Carolina and South Carolina), this was a smoking gun. For the first time ever, a computer intruder had broken into a BellSouth central office switching station and re-programmed it!

Or so BellSouth thought in June 1989. Actually, LoD members had been frolicking harmlessly in BellSouth switches since September 1987. The stunt of June 13 - call-forwarding a number through manipulation of a switching station - was child's play for hackers as accomplished as the Georgia wing of LoD. Switching calls interstate sounded like a big deal, but it took only four lines of code to accomplish this. An easy, yet more discreet, stunt, would be to call-forward another number to your own house. If you were careful and considerate, and changed the software back later, then not a soul would know.

Except you. And whoever you had bragged to about it.

As for BellSouth, what they didn't know wouldn't hurt them. Except now somebody had blown the whole thing wide open, and BellSouth knew. A now alerted and considerably paranoid BellSouth began searching switches right and left for signs of impropriety, in that hot summer of 1989. No fewer than forty-two BellSouth employees were put on 12-hour shifts, twenty-four hours a day, for two solid months, poring over records and monitoring computers for any sign of phony access. These forty-two overworked experts were known as BellSouth's "Intrusion Task Force."

Part Three: Law and Order.

- Crooked Boards
- The World's Biggest Hacker Bust
- Teach Them a Lesson
- The U.S. Secret Service
- The Secret Service Battles the Boodlers
- A Walk Downtown
- FCIC: The Cutting-Edge Mess
- Cyberspace Rangers
- FLETC: Training the Hacker-Trackers

Of the various anti-hacker activities of 1990, "Operation Sundevil" had by far the highest public profile. The sweeping, nationwide computer seizures of May 8, 1990 were unprecedented in scope and highly, if rather selectively, publicized.

Unlike the efforts of the Chicago Computer Fraud and Abuse Task Force, "Operation Sundevil" was not intended to combat "hacking" in the sense of computer intrusion or sophisticated raids on telco switching stations. Nor did it have anything to do with hacker misdeeds with AT&T's software, or with Southern Bell's proprietary documents.

Instead, "Operation Sundevil" was a crackdown on those traditional scourges of the digital underground: credit card theft and telephone code abuse. The ambitious activities out of Chicago, and the somewhat lesser-known but vigorous antihacker actions of the New York State Police in 1990, were never a part of "Operation Sundevil" per se, which was based in Arizona.

Nevertheless, after the spectacular May 8 raids, the public, misled by police secrecy, hacker panic, and a puzzled national press-corps, conflated all aspects of the nationwide crackdown in 1990 under the blanket term "Operation Sundevil." "Sundevil" is still the best-known synonym for the crackdown of 1990. But the Arizona organizers of "Sundevil" did not really deserve this reputation - any more, for instance, than all hackers deserve a reputation as "hackers."

There was some justice in this confused perception, though. For one thing, the confusion was abetted by the Washington office of the Secret Service, who responded to Freedom of Information Act requests on "Operation Sundevil" by referring investigators to the publicly known cases of Knight Lightning and the Atlanta Three. And "Sundevil" was certainly the largest aspect of the Crackdown, the most deliberate and the best-organized. As a crackdown on electronic fraud, "Sundevil" lacked the frantic pace of the war on the Legion of Doom; on the contrary, Sundevil's targets were picked out with cool deliberation over an elaborate investigation lasting two full years.

And once again the targets were bulletin board systems.

Boards can be powerful aids to organized fraud. Underground boards carry lively, extensive, detailed, and often quite flagrant "discussions" of lawbreaking techniques and lawbreaking activities. "Discussing" crime in the abstract, or "discussing" the particulars of criminal cases, is not illegal - but there are stern state and federal laws against coldbloodedly conspiring in groups in order to commit crimes.

In the eyes of police, people who actively conspire to break the law are not regarded as "clubs," "debating salons," "users' groups," or "free speech advocates." Rather, such people tend to find themselves formally indicted by prosecutors as "gangs," "racketeers," "corrupt organizations" and "organized crime figures."

What's more, the illicit data contained on outlaw boards goes well beyond mere acts of speech and/or possible criminal conspiracy. As we have seen, it was common practice in the digital underground to post purloined telephone codes on boards, for any phreak or hacker who cared to abuse them. Is posting

digital booty of this sort supposed to be protected by the First Amendment? Hardly - though the issue, like most issues in cyberspace, is not entirely resolved. Some theorists argue that to merely recite a number publicly is not illegal - only its use is illegal. But anti-hacker police point out that magazines and newspapers (more traditional forms of free expression) never publish stolen telephone codes (even though this might well raise their circulation).

Stolen credit card numbers, being riskier and more valuable, were less often publicly posted on boards - but there is no question that some underground boards carried "carding" traffic, generally exchanged through private mail.

Underground boards also carried handy programs for "scanning" telephone codes and raiding credit card companies, as well as the usual obnoxious galaxy of pirated software, cracked passwords, blue-box schematics, intrusion manuals, anarchy files, porn files, and so forth.

But besides their nuisance potential for the spread of illicit knowledge, bulletin boards have another vitally interesting aspect for the professional investigator. Bulletin boards are cram-full of evidence. All that busy trading of electronic mail, all those hacker boasts, brags and struts, even the stolen codes and cards, can be neat, electronic, realtime recordings of criminal activity. As an investigator, when you seize a pirate board, you have scored a coup as effective as tapping phones or intercepting mail. However, you have not actually tapped a phone or intercepted a letter. The rules of evidence regarding phone-taps and mail interceptions are old, stern and well understood by police, prosecutors and defense attorneys alike. The rules of evidence regarding boards are new, waffling, and understood by nobody at all.

Sundevil was the largest crackdown on boards in world history. On May 7, 8, and 9, 1990, about forty-two computer systems were seized. Of those forty-two computers, about twenty-five actually were running boards. (The vagueness of this estimate is attributable to the vagueness of (a) what a "computer system" is, and (b) what it actually means to "run a board" with one - or with two computers, or with three.)

About twenty-five boards vanished into police custody in May 1990. As we have seen, there are an estimated 30,000 boards in America today. If we assume that one board in a hundred is up to no good with codes and cards (which rather flatters the honesty of the board-using community), then that would leave 2,975 outlaw boards untouched by Sundevil. Sundevil seized about one tenth of one percent of all computer bulletin boards in America. Seen objectively, this is something less than a comprehensive assault. In 1990, Sundevil's organizers - the team at the Phoenix Secret Service office, and the Arizona Attorney General's office - had a list of at least three hundred boards that they considered fully deserving of search and seizure warrants. The twenty-five boards actually seized were merely among the most obvious and egregious of this much larger list of candidates. All these boards had been examined beforehand - either by informants, who had passed printouts to the Secret Service, or by Secret Service agents themselves, who not only come equipped with modems but know how to use them.

There were a number of motives for Sundevil. First, it offered a chance to get ahead of the curve on wire-fraud crimes. Tracking back credit card rip-offs to their perpetrators can be appallingly difficult. If these miscreants have any kind of electronic sophistication, they can snarl their tracks through the phone network into a mind-boggling, untraceable mess, while still managing to "reach out and rob someone." Boards, however, full of brags and boasts, codes and cards, offer evidence in the handy congealed form.

Seizures themselves - the mere physical removal of machines - tends to take the pressure off. During Sundevil, a large number of code kids, warez d00dz, and credit card thieves would be deprived of those boards - their means of community and conspiracy - in one swift blow. As for the sysops themselves (commonly among the boldest offenders) they would be directly stripped of their computer equipment, and rendered digitally mute and blind.

And this aspect of Sundevil was carried out with great success. Sundevil seems to have been a complete tactical surprise - unlike the fragmentary and continuing seizures of the war on the Legion of Doom, Sundevil was precisely timed and utterly overwhelming. At least forty "computers" were seized during

May 7, 8 and 9, 1990, in Cincinnati, Detroit, Los Angeles, Miami, Newark, Phoenix, Tucson, Richmond, San Diego, San Jose, Pittsburgh and San Francisco. Some cities saw multiple raids, such as the five separate raids in the New York City environs. Plano, Texas (essentially a suburb of the Dallas/Fort Worth metroplex, and a hub of the telecommunications industry) saw four computer seizures. Chicago, ever in the forefront, saw its own local Sundevil raid, briskly carried out by Secret Service agents Timothy Foley and Barbara Golden.

Many of these raids occurred, not in the cities proper, but in associated white-middle class suburbs - places like Mount Lebanon, Pennsylvania and Clark Lake, Michigan. There were a few raids on offices; most took place in people's homes, the classic hacker basements and bedrooms.

The Sundevil raids were searches and seizures, not a group of mass arrests. There were only four arrests during Sundevil. "Tony the Trashman," a longtime teenage bete noire of the Arizona Racketeering unit, was arrested in Tucson on May 9. "Dr. Ripco," sysop of an outlaw board with the misfortune to exist in Chicago itself, was also arrested - on illegal weapons charges. Local units also arrested a 19-year-old female phone phreak named "Electra" in Pennsylvania, and a male juvenile in California. Federal agents however were not seeking arrests, but computers.

Hackers are generally not indicted (if at all) until the evidence in their seized computers is evaluated - a process that can take weeks, months - even years. When hackers are arrested on the spot, it's generally an arrest for other reasons. Drugs and/or illegal weapons show up in a good third of anti-hacker computer seizures (though not during Sundevil). That scofflaw teenage hackers (or their parents) should have marijuana in their homes is probably not a shocking revelation, but the surprisingly common presence of illegal firearms in hacker dens is a bit disquieting. A Personal Computer can be a great equalizer for the techno-cowboy - much like that more traditional American "Great Equalizer," the Personal Sixgun. Maybe it's not all that surprising that some guy obsessed with power through illicit technology would also have a few illicit high-velocity-impact devices around. An element of the digital underground particularly dotes on those "anarchy philes," and this element tends to shade into the crackpot milieu of survivalists, gun-nuts, anarcho-leftists and the ultra-libertarian right-wing.

This is not to say that hacker raids to date have uncovered any major crack-dens or illegal arsenals; but Secret Service agents do not regard "hackers" as "just kids." They regard hackers as unpredictable people, bright and slippery. It doesn't help matters that the hacker himself has been "hiding behind his keyboard" all this time. Commonly, police have no idea what he looks like. This makes him an unknown quantity, someone best treated with proper caution.

To date, no hacker has come out shooting, though they do sometimes brag on boards that they will do just that. Threats of this sort are taken seriously. Secret Service hacker raids tend to be swift, comprehensive, well-manned (even overmanned); and agents generally burst through every door in the home at once, sometimes with drawn guns. Any potential resistance is swiftly quelled. Hacker raids are usually raids on people's homes. It can be a very dangerous business to raid an American home; people can panic when strangers invade their sanctum. Statistically speaking, the most dangerous thing a policeman can do is to enter someone's home. (The second most dangerous thing is to stop a car in traffic.) People have guns in their homes. More cops are hurt in homes than are ever hurt in biker bars or massage parlors.

But in any case, no one was hurt during Sundevil, or indeed during any part of the Hacker Crackdown.

Nor were there any allegations of any physical mistreatment of a suspect. Guns were pointed, interrogations were sharp and prolonged; but no one in 1990 claimed any act of brutality by any crackdown raider.

In addition to the forty or so computers, Sundevil reaped floppy disks in particularly great abundance - an estimated 23,000 of them, which naturally included every manner of illegitimate data: pirated games, stolen codes, hot credit card numbers, the complete text and software of entire pirate bulletin-boards. These floppy disks, which remain in police custody today, offer a gi-

gantic, almost embarrassingly rich source of possible criminal indictments. These 23,000 floppy disks also include a thus-far unknown quantity of legitimate computer games, legitimate software, purportedly "private" mail from boards, business records, and personal correspondence of all kinds.

Standard computer crime search warrants lay great emphasis on seizing written documents as well as computers - specifically including photocopies, computer printouts, telephone bills, address books, logs, notes, memoranda and correspondence. In practice, this has meant that diaries, gaming magazines, software documentation, nonfiction books on hacking and computer security, sometimes even science fiction novels, have all vanished out the door in police custody. A wide variety of electronic items have been known to vanish as well, including telephones, televisions, answering machines, Sony Walkmans, desktop printers, compact disks, and audiotapes.

No fewer than 150 members of the Secret Service were sent into the field during Sundevil. They were commonly accompanied by squads of local and/or state police. Most of these officers - especially the locals - had never been on an anti-hacker raid before. (This was one good reason, in fact, why so many of them were invited along in the first place.) Also, the presence of a uniformed police officer assures the raidees that the people entering their homes are, in fact, police. Secret Service agents wear plain clothes. So do the telco security experts who commonly accompany the Secret Service on raids (and who make no particular effort to identify themselves as mere employees of telephone companies).

A typical hacker raid goes something like this. First, police storm in rapidly, through every entrance, with overwhelming force, in the assumption that this tactic will keep casualties to a minimum. Second, possible suspects are immediately removed from the vicinity of any and all computer systems, so that they will have no chance to purge or destroy computer evidence. Suspects are herded into a room without computers, commonly the living room, and kept under guard - not armed guard, for the guns are swiftly holstered, but under guard nevertheless. They are presented with the search warrant and warned that anything they say may be held against them. Commonly they have a great deal to say, especially if they are unsuspecting parents.

Somewhere in the house is the "hot spot" - a computer tied to a phone line (possibly several computers and several phones). Commonly it's a teenager's bedroom, but it can be anywhere in the house; there may be several such rooms. This "hot spot" is put in charge of a two-agent team, the "finder" and the "recorder." The "finder" is computer-trained, commonly the case agent who has actually obtained the search warrant from a judge. He or she understands what is being sought, and actually carries out the seizures: unplugs machines, opens drawers, desks, files, floppy-disk containers, etc. The "recorder" photographs all the equipment, just as it stands - especially the tangle of wired connections in the back, which can otherwise be a real nightmare to restore. The recorder will also commonly photograph every room in the house, lest some wily criminal claim that the police had robbed him during the search. Some recorders carry videocams or tape recorders; however, it's more common for the recorder to simply take written notes. Objects are described and numbered as the finder seizes them, generally on standard preprinted police inventory forms.

Even Secret Service agents were not, and are not, expert computer users. They have not made, and do not make, judgements on the fly about potential threats posed by various forms of equipment. They may exercise discretion; they may leave Dad his computer, for instance, but they don't have to. Standard computer crime search warrants, which date back to the early 80s, use a sweeping language that targets computers, most anything attached to a computer, most anything used to operate a computer - most anything that remotely resembles a computer - plus most any and all written documents surrounding it. Computer crime investigators have strongly urged agents to seize the works.

In this sense, Operation Sundevil appears to have been a complete success. Boards went down all over America, and were shipped en masse to the computer investigation lab of the Secret Service, in Washington DC, along with the 23,000 floppy disks and unknown quantities of printed material.

But the seizure of twenty-five boards, and the multi-megabyte mountains of possibly useful evidence contained in these boards (and in their owners' other computers, also out the door), were far from the only motives for Operation Sundevil. An unprecedented action of great ambition and size, Sundevil's motives can only be described as political. It was a public-relations effort, meant to pass certain messages, meant to make certain situations clear: both in the mind of the general public, and in the minds of various constituencies of the electronic community.

First - and this motivation was vital - a "message" would be sent from law enforcement to the digital underground. This very message was recited in so many words by Garry M. Jenkins, the Assistant Director of the US Secret Service, at the Sundevil press conference in Phoenix on May 9, 1990, immediately after the raids. In brief, hackers were mistaken in their foolish belief that they could hide behind the "relative anonymity of their computer terminals." On the contrary, they should fully understand that state and federal cops were actively patrolling the beat in cyberspace - that they were on the watch everywhere, even in those sleazy and secretive dens of cybernetic vice, the underground boards.

This is not an unusual message for police to publicly convey to crooks. The message is a standard message; only the context is new. In this respect, the Sundevil raids were the digital equivalent of the standard vice-squad crackdown on massage parlors, porno bookstores, head-shops, or floating crap-games. There may be few or no arrests in a raid of this sort; no convictions, no trials, no interrogations. In cases of this sort, police may well walk out the door with many pounds of sleazy magazines, X-rated videotapes, sex toys, gambling equipment, baggies of marijuana…

Of course, if something truly horrendous is discovered by the raiders, there will be arrests and prosecutions. Far more likely, however, there will simply be a brief but sharp disruption of the closed and secretive world of the nogoodniks. There will be "street hassle." "Heat." "Deterrence." And, of course, the immediate loss of the seized goods. It is very unlikely that any of this seized material will ever be returned. Whether charged or not, whether convicted or not, the perpetrators will almost surely lack the nerve ever to ask for this stuff to be given back.

Arrests and trials - putting people in jail - may involve all kinds of formal legalities; but dealing with the justice system is far from the only task of police. Police do not simply arrest people. They don't simply put people in jail. That is not how the police perceive their jobs. Police "protect and serve." Police "keep the peace," they "keep public order." Like other forms of public relations, keeping public order is not an exact science. Keeping public order is something of an art-form.

If a group of tough-looking teenage hoodlums was loitering on a street-corner, no one would be surprised to see a street-cop arrive and sternly order them to "break it up." On the contrary, the surprise would come if one of these ne'er-do-wells stepped briskly into a phone-booth, called a civil rights lawyer, and instituted a civil suit in defense of his Constitutional rights of free speech and free assembly. But something much along this line was one of the many anomalous outcomes of the Hacker Crackdown.

Sundevil also carried useful "messages" for other constituents of the electronic community. These messages may not have been read aloud from the Phoenix podium in front of the press corps, but there was little mistaking their meaning. There was a message of reassurance for the primary victims of coding and carding: the telcos, and the credit companies. Sundevil was greeted with joy by the security officers of the electronic business community. After years of high-tech harassment and spiralling revenue losses, their complaints of rampant outlawry were being taken seriously by law enforcement. No more head-scratching or dismissive shrugs; no more feeble excuses about "lack of computer-trained officers" or the low priority of "victimless" white-collar telecommunication crimes.

Computer crime experts have long believed that computer-related offenses are drastically under-reported. They regard this as a major open scandal of their field. Some victims are reluctant to come forth, because they believe that police and prosecutors are not computer-literate, and can and will do

nothing. Others are embarrassed by their vulnerabilities, and will take strong measures to avoid any publicity; this is especially true of banks, who fear a loss of investor confidence should an embezzlement-case or wire-fraud surface. And some victims are so helplessly confused by their own high technology that they never even realize that a crime has occurred - even when they have been fleeced to the bone.

The results of this situation can be dire. Criminals escape apprehension and punishment. The computer crime units that do exist, can't get work. The true scope of computer crime: its size, its real nature, the scope of its threats, and the legal remedies for it - all remain obscured. Another problem is very little publicized, but it is a cause of genuine concern. Where there is persistent crime, but no effective police protection, then vigilantism can result. Telcos, banks, credit companies, the major corporations who maintain extensive computer networks vulnerable to hacking - these organizations are powerful, wealthy, and politically influential. They are disinclined to be pushed around by crooks (or by most anyone else, for that matter). They often maintain well-organized private security forces, commonly run by experienced veterans of military and police units, who have left public service for the greener pastures of the private sector. For police, the corporate security manager can be a powerful ally; but if this gentleman finds no allies in the police, and the pressure is on from his board-of-directors, he may quietly take certain matters into his own hands.

Nor is there any lack of disposable hired-help in the corporate security business. Private security agencies - the `security business' generally - grew explosively in the 1980s. Today there are spooky gumshoed armies of "security consultants," "rent-a-cops," "private eyes," "outside experts" - every manner of shady operator who retails in "results" and discretion. Of course, many of these gentlemen and ladies may be paragons of professional and moral rectitude. But as anyone who has read a hard-boiled detective novel knows, police tend to be less than fond of this sort of private-sector competition.

Companies in search of computer-security have even been known to hire hackers. Police shudder at this prospect.

Police treasure good relations with the business community. Rarely will you see a policeman so indiscreet as to allege publicly that some major employer in his state or city has succumbed to paranoia and gone off the rails. Nevertheless, police - and computer police in particular - are aware of this possibility. computer crime police can and do spend up to half of their business hours just doing public relations: seminars, "dog and pony shows," sometimes with parents' groups or computer users, but generally with their core audience: the likely victims of hacking crimes. These, of course, are telcos, credit card companies and large computerequipped corporations. The police strongly urge these people, as good citizens, to report offenses and press criminal charges; they pass the message that there is someone in authority who cares, understands, and, best of all, will take useful action should a computer crime occur. But reassuring talk is cheap. Sundevil offered action.

The final message of Sundevil was intended for internal consumption by law enforcement. Sundevil was offered as proof that the community of American computer crime police had come of age. Sundevil was proof that enormous things like Sundevil itself could now be accomplished. Sundevil was proof that the Secret Service and its local law enforcement allies could act like a well oiled machine - (despite the hampering use of those scrambled phones). It was also proof that the Arizona Organized Crime and Racketeering Unit - the spark-plug of Sundevil - ranked with the best in the world in ambition, organization, and sheer conceptual daring.

And, as a final fillip, Sundevil was a message from the Secret Service to their longtime rivals in the Federal Bureau of Investigation. By Congressional fiat, both USSS and FBI formally share jurisdiction over federal computer crimebusting activities. Neither of these groups has ever been remotely happy with this muddled situation. It seems to suggest that Congress cannot make up its mind as to which of these groups is better qualified. And there is scarcely a G-man or a Special Agent anywhere without a very firm opinion on that topic.

-Section 1-

For the neophyte, one of the most puzzling aspects of the crackdown on hackers is why the United States Secret Service has anything at all to do with this matter.

The Secret Service is best known for its primary public role: its agents protect the President of the United States. They also guard the President's family, the Vice President and his family, former Presidents, and Presidential candidates. They sometimes guard foreign dignitaries who are visiting the United States, especially foreign heads of state, and have been known to accompany American officials on diplomatic missions overseas.

Special Agents of the Secret Service don't wear uniforms, but the Secret Service also has two uniformed police agencies. There's the former White House Police (now known as the Secret Service Uniformed Division, since they currently guard foreign embassies in Washington, as well as the White House itself). And there's the uniformed Treasury Police Force.

The Secret Service has been charged by Congress with a number of little-known duties. They guard the precious metals in Treasury vaults. They guard the most valuable historical documents of the United States: originals of the Constitution, the Declaration of Independence, Lincoln's Second Inaugural Address, an American-owned copy of the Magna Carta, and so forth. Once they were assigned to guard the Mona Lisa, on her American tour in the 1960s.

The entire Secret Service is a division of the Treasury Department. Secret Service Special Agents (there are about 1,900 of them) are bodyguards for the President et al, but they all work for the Treasury. And the Treasury (through its divisions of the U.S. Mint and the Bureau of Engraving and Printing) prints the nation's money.

As Treasury police, the Secret Service guards the nation's currency; it is the only federal law enforcement agency with direct jurisdiction over counterfeiting and forgery. It analyzes documents for authenticity, and its fight against fake cash is still quite lively (especially since the skilled counterfeiters of Medellin, Columbia have gotten into the act). Government checks, bonds, and other obligations, which exist in untold millions and are worth untold billions, are common targets for forgery, which the Secret Service also battles. It even handles forgery of postage stamps. But cash is fading in importance today as money has become electronic. As necessity beckoned, the Secret Service moved from fighting the counterfeiting of paper currency and the forging of checks, to the protection of funds transferred by wire.

From wire-fraud, it was a simple skip-and-jump to what is formally known as "access device fraud." Congress granted the Secret Service the authority to investigate "access device fraud" under Title 18 of the United States Code (U.S.C. Section 1029).

The term "access device" seems intuitively simple. It's some kind of high-tech gizmo you use to get money with. It makes good sense to put this sort of thing in the charge of counterfeiting and wirefraud experts.

However, in Section 1029, the term "access device" is very generously defined. An access device is: "any card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds."

"Access device" can therefore be construed to include credit cards themselves (a popular forgery item nowadays). It also includes credit card account numbers, those standards of the digital underground. The same goes for telephone charge cards (an increasingly popular item with telcos, who are tired of being robbed of pocket change by phone-booth thieves). And also telephone access codes, those other standards of the digital underground. (Stolen telephone codes may not "obtain money," but they certainly do obtain valuable "services," which is specifically forbidden by Section 1029.)

We can now see that Section 1029 already pits the United States Secret Service directly against the digital underground, without any mention at all of the word "computer."

Standard phreaking devices, like "blue boxes," used to steal phone service from old-fashioned mechanical switches, are unquestionably "counterfeit access devices." Thanks to Sec. 1029, it is not only illegal to use counterfeit access devices, but it is even illegal to build them. "Producing," "designing," "duplicating," or "assembling" blue boxes are all federal crimes today, and if you do this, the Secret Service has been charged by Congress to come after you.

Automatic Teller Machines, which replicated all over America during the 1980s, are definitely "access devices," too, and an attempt to tamper with their punch-in codes and plastic bank cards falls directly under Sec. 1029.

Section 1029 is remarkably elastic. Suppose you find a computer password in somebody's trash. That password might be a "code" - it's certainly a "means of account access." Now suppose you log on to a computer and copy some software for yourself. You've certainly obtained "service" (computer service) and a "thing of value" (the software). Suppose you tell a dozen friends about your swiped password, and let them use it, too. Now you're "trafficking in unauthorized access devices." And when the Prophet, a member of the Legion of Doom, passed a stolen telephone company document to Knight Lightning at Phrack magazine, they were both charged under Sec. 1029!

There are two limitations on Section 1029. First, the offense must "affect interstate or foreign commerce" in order to become a matter of federal jurisdiction. The term "affecting commerce" is not well defined; but you may take it as a given that the Secret Service can take an interest if you've done most anything that happens to cross a state line. State and local police can be touchy about their jurisdictions, and can sometimes be mulish when the feds show up. But when it comes to computer crime, the local police are pathetically grateful for federal help - in fact they complain that they can't get enough of it. If you're stealing long-distance service, you're almost certainly crossing state lines, and you're definitely "affecting the interstate commerce" of the telcos. And if you're abusing credit cards by ordering stuff out of glossy catalogs from, say, Vermont, you're in for it. The second limitation is money. As a rule, the feds don't pursue penny-ante offenders. Federal judges will dismiss cases that appear to waste their time. Federal crimes must be serious; Section 1029 specifies a minimum loss of a thousand dollars. We now come to the very next section of Title 18, which is Section 1030, "Fraud and related activity in connection with computers." This statute gives the Secret Service direct jurisdiction over acts of computer intrusion. On the face of it, the Secret Service would now seem to command the field. Section 1030, however, is nowhere near so ductile as Section 1029. The first annoyance is Section 1030(d), which reads:

"(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General." (Author's italics.)

The Secretary of the Treasury is the titular head of the Secret Service, while the Attorney General is in charge of the FBI. In Section (d), Congress shrugged off responsibility for the computer crime turf-battle between the Service and the Bureau, and made them fight it out all by themselves. The result was a rather dire one for the Secret Service, for the FBI ended up with exclusive jurisdiction over computer break-ins having to do with national security, foreign espionage, federally insured banks, and U.S. military bases, while retaining joint jurisdiction over all the other computer intrusions. Essentially, when it comes to Section 1030, the FBI not only gets the real glamor stuff for itself, but can peer over the shoulder of the Secret Service and barge in to meddle whenever it suits them. The second problem has to do with the dicey term "Federal interest computer." Section 1030(a)(2) makes it illegal to "access a computer without authorization" if that computer belongs to a financial institution or an issuer of credit cards (fraud cases, in other words). Congress was quite willing to give the Secret Service jurisdiction over money-transferring computers, but Congress balked at letting them investigate any and all computer intrusions. Instead, the USSS had to settle for the money machines and the "Federal interest computers." A "Federal interest com-

puter" is a computer which the government itself owns, or is using. Large networks of interstate computers, linked over state lines, are also considered to be of "Federal interest." (This notion of "Federal interest" is legally rather foggy and has never been clearly defined in the courts. The Secret Service has never yet had its hand slapped for investigating computer break-ins that were not of "Federal interest," but conceivably someday this might happen.)

So the Secret Service's authority over "unauthorized access" to computers covers a lot of territory, but by no means the whole ball of cyberspatial wax. If you are, for instance, a local computer retailer, or the owner of a local bulletin board system, then a malicious local intruder can break in, crash your system, trash your files and scatter viruses, and the U.S. Secret Service cannot do a single thing about it.

At least, it can't do anything directly. But the Secret Service will do plenty to help the local people who can.

The FBI may have dealt itself an ace off the bottom of the deck when it comes to Section 1030; but that's not the whole story; that's not the street. What Congress thinks is one thing, and Congress has been known to change its mind. The real turfstruggle is out there in the streets where it's happening. If you're a local street-cop with a computer problem, the Secret Service wants you to know where you can find the real expertise. While the Bureau crowd are off having their favorite shoes polished - (wing-tips) - and making derisive fun of the Service's favorite shoes - ("pansy-ass tassels") - the tassel-toting Secret Service has a crew of ready-and-able hacker-trackers installed in the capital of every state in the Union. Need advice? They'll give you advice, or at least point you in the right direction. Need training? They can see to that, too.

If you're a local cop and you call in the FBI, the FBI (as is widely and slanderously rumored) will order you around like a coolie, take all the credit for your busts, and mop up every possible scrap of reflected glory. The Secret Service, on the other hand, doesn't brag a lot. They're the quiet types. Very quiet. Very cool. Efficient. High-tech. Mirrorshades, icy stares, radio earplugs, an Uzi machine-pistol tucked somewhere in that well-cut jacket. American samurai, sworn to give their lives to protect our President. "The granite agents." Trained in martial arts, absolutely fearless. Every single one of 'em has a top-secret security clearance. Something goes a little wrong, you're not gonna hear any whining and moaning and political buck-passing out of these guys.

The facade of the granite agent is not, of course, the reality. Secret Service agents are human beings. And the real glory in Service work is not in battling computer crime - not yet, anyway - but in protecting the President. The real glamour of Secret Service work is in the White House Detail. If you're at the President's side, then the kids and the wife see you on television; you rub shoulders with the most powerful people in the world. That's the real heart of Service work, the number one priority. More than one computer investigation has stopped dead in the water when Service agents vanished at the President's need.

There's romance in the work of the Service. The intimate access to circles of great power; the esprit de corps of a highly trained and disciplined elite; the high responsibility of defending the Chief Executive; the fulfillment of a patriotic duty. And as police work goes, the pay's not bad. But there's squalor in Service work, too. You may get spat upon by protesters howling abuse - and if they get violent, if they get too close, sometimes you have to knock one of them down - discreetly.

The real squalor in Service work is drudgery such as "the quarterlies," traipsing out four times a year, year in, year out, to interview the various pathetic wretches, many of them in prisons and asylums, who have seen fit to threaten the President's life. And then there's the grinding stress of searching all those faces in the endless bustling crowds, looking for hatred, looking for psychosis, looking for the tight, nervous face of an Arthur Bremer, a Squeaky Fromme, a Lee Harvey Oswald. It's watching all those grasping, waving hands for sudden movements, while your ears strain at your radio headphone for the long-rehearsed cry of "Gun!"

It’s poring, in grinding detail, over the biographies of every rotten loser who ever shot at a President. It’s the unsung work of the Protective Research Section, who study scrawled, anonymous death threats with all the meticulous tools of antiforgery techniques.

And it’s maintaining the hefty computerized files on anyone who ever threatened the President’s life. Civil libertarians have become increasingly concerned at the Government’s use of computer files to track American citizens - but the Secret Service file of potential Presidential assassins, which has upward of twenty thousand names, rarely causes a peep of protest. If you ever state that you intend to kill the President, the Secret Service will want to know and record who you are, where you are, what you are, and what you’re up to. If you’re a serious threat - if you’re officially considered “of protective interest” - then the Secret Service may well keep tabs on you for the rest of your natural life.

Protecting the President has first call on all the Service’s resources. But there’s a lot more to the Service’s traditions and history than standing guard outside the Oval Office. The Secret Service is the nation’s oldest general federal law enforcement agency. Compared to the Secret Service, the FBI are new-hires and the CIA are temps. The Secret Service was founded way back in 1865, at the suggestion of Hugh McCulloch, Abraham Lincoln’s Secretary of the Treasury. McCulloch wanted a specialized Treasury police to combat counterfeiting. Abraham Lincoln agreed that this seemed a good idea, and, with a terrible irony, Abraham Lincoln was shot that very night by John Wilkes Booth.

The Secret Service originally had nothing to do with protecting Presidents. They didn’t take this on as a regular assignment until after the Garfield assassination in 1881.

And they didn’t get any Congressional money for it until President McKinley was shot in 1901. The Service was originally designed for one purpose: destroying counterfeiters.

-Section 2-

There are interesting parallels between the Service’s nineteenth-century entry into counterfeiting, and America’s twentieth-century entry into computer crime.

In 1865, America’s paper currency was a terrible muddle. Security was drastically bad. Currency was printed on the spot by local banks in literally hundreds of different designs. No one really knew what the heck a dollar bill was supposed to look like. Bogus bills passed easily. If some joker told you that a one-dollar bill from the Railroad Bank of Lowell, Massachusetts had a woman leaning on a shield, with a locomotive, a cornucopia, a compass, various agricultural implements, a railroad bridge, and some factories, then you pretty much had to take his word for it. (And in fact he was telling the truth!)

Sixteen hundred local American banks designed and printed their own paper currency, and there were no general standards for security. Like a badly guarded node in a computer network, badly designed bills were easy to fake, and posed a security hazard for the entire monetary system.

No one knew the exact extent of the threat to the currency. There were panicked estimates that as much as a third of the entire national currency was faked. Counterfeiters - known as “boodlers” in the underground slang of the time - were mostly technically skilled printers who had gone to the bad. Many had once worked printing legitimate currency. Boodlers operated in rings and gangs. Technical experts engraved the bogus plates - commonly in basements in New York City. Smooth confidence men passed large wads of high-quality, high denomination fakes, including the really sophisticated stuff - government bonds, stock certificates, and railway shares. Cheaper, botched fakes were sold or sharewared to low-level gangs of boodler wannabes. (The really cheesy lowlife boodlers merely upgraded real bills by altering face values, changing ones to fives, tens to hundreds, and so on.) The techniques of boodling were little-known and regarded with a certain awe by the mid-nineteenth-century public. The ability to manipulate the system for rip-off seemed diabolically

clever. As the skill and daring of the boodlers increased, the situation became intolerable. The federal government stepped in, and began offering its own federal currency, which was printed in fancy green ink, but only on the back - the original "greenbacks." And at first, the improved security of the well-designed, well-printed federal greenbacks seemed to solve the problem; but then the counterfeiters caught on. Within a few years things were worse than ever: a centralized system where all security was bad!

The local police were helpless. The Government tried offering blood money to potential informants, but this met with little success. Banks, plagued by boodling, gave up hope of police help and hired private security men instead. Merchants and bankers queued up by the thousands to buy privately-printed manuals on currency security, slim little books like Laban Heath's Infallible Government Counterfeit Detector. The back of the book offered Laban Heath's patent microscope for five bucks. Then the Secret Service entered the picture. The first agents were a rough and ready crew. Their chief was one William P. Wood, a former guerilla in the Mexican War who'd won a reputation busting contractor fraudsters for the War Department during the Civil War. Wood, who was also Keeper of the Capital Prison, had a sideline as a counterfeiting expert, bagging boodlers for the federal bounty money.

Wood was named Chief of the new Secret Service in July 1865. There were only ten Secret Service agents in all: Wood himself, a handful who'd worked for him in the War Department, and a few former private investigators - counterfeiting experts - whom Wood had won over to public service. (The Secret Service of 1865 was much the size of the Chicago Computer Fraud Task Force or the Arizona Racketeering Unit of 1990.) These ten "Operatives" had an additional twenty or so "Assistant Operatives" and "Informants." Besides salary and per diem, each Secret Service employee received a whopping twenty-five dollars for each boodler he captured.

Wood himself publicly estimated that at least half of America's currency was counterfeit, a perhaps pardonable perception. Within a year the Secret Service had arrested over 200 counterfeiters. They busted about two hundred boodlers a year for four years straight.

Wood attributed his success to travelling fast and light, hitting the badguys hard, and avoiding bureaucratic baggage. "Because my raids were made without military escort and I did not ask the assistance of state officers, I surprised the professional counterfeiter."

Wood's social message to the once-impudent boodlers bore an eerie ring of Sundevil: "It was also my purpose to convince such characters that it would no longer be healthy for them to ply their vocation without being handled roughly, a fact they soon discovered."

William P. Wood, the Secret Service's guerilla pioneer, did not end well. He succumbed to the lure of aiming for the really big score. The notorious Brockway Gang of New York City, headed by William E. Brockway, the "King of the Counterfeiters," had forged a number of government bonds. They'd passed these brilliant fakes on the prestigious Wall Street investment firm of Jay Cooke and Company. The Cooke firm were frantic and offered a huge reward for the forgers' plates.

Laboring diligently, Wood confiscated the plates (though not Mr. Brockway) and claimed the reward. But the Cooke company treacherously reneged. Wood got involved in a down-and-dirty lawsuit with the Cooke capitalists. Wood's boss, Secretary of the Treasury McCulloch, felt that Wood's demands for money and glory were unseemly, and even when the reward money finally came through, McCulloch refused to pay Wood anything. Wood found himself mired in a seemingly endless round of federal suits and Congressional lobbying.

Wood never got his money. And he lost his job to boot. He resigned in 1869.

Wood's agents suffered, too. On May 12, 1869, the second Chief of the Secret Service took over, and almost immediately fired most of Wood's pioneer Secret Service agents: Operatives, Assistants and Informants alike. The practice of receiving $25 per crook was abolished. And the Secret Service began the long, uncertain process of thorough professionalization.

Wood ended badly. He must have felt stabbed in the back. In fact his entire organization was mangled.

On the other hand, William P. Wood was the first head of the Secret Service. William Wood was the pioneer. People still honor his name. Who remembers the name of the second head of the Secret Service?

As for William Brockway (also known as "Colonel Spencer"), he was finally arrested by the Secret Service in 1880. He did five years in prison, got out, and was still boodling at the age of seventy-four.

-Section 3-

Anyone with an interest in Operation Sundevil - or in American computer crime generally - could scarcely miss the presence of Gail Thackeray, Assistant Attorney General of the State of Arizona. computer crime training manuals often cited Thackeray's group and her work; she was the highest-ranking state official to specialize in computer-related offenses. Her name had been on the Sundevil press release (though modestly ranked well after the local federal prosecuting attorney and the head of the Phoenix Secret Service office). As public commentary, and controversy, began to mount about the Hacker Crackdown, this Arizonan state official began to take a higher and higher public profile. Though uttering almost nothing specific about the Sundevil operation itself, she coined some of the most striking soundbites of the growing propaganda war: "Agents are operating in good faith, and I don't think you can say that for the hacker community," was one. Another was the memorable "I am not a mad dog prosecutor" (Houston Chronicle, Sept 2, 1990.) In the meantime, the Secret Service maintained its usual extreme discretion; the Chicago Unit, smarting from the backlash of the Steve Jackson scandal, had gone completely to earth.

As I collated my growing pile of newspaper clippings, Gail Thackeray ranked as a comparative fount of public knowledge on police operations.

I decided that I had to get to know Gail Thackeray. I wrote to her at the Arizona Attorney General's Office.

Not only did she kindly reply to me, but, to my astonishment, she knew very well what "cyberpunk" science fiction was.

Shortly after this, Gail Thackeray lost her job. And I temporarily misplaced my own career as a science-fiction writer, to become a full-time computer crime journalist. In early March, 1991, I flew to Phoenix, Arizona, to interview Gail Thackeray for my book on the hacker crackdown.

-Section 4-

"Credit cards didn't use to cost anything to get," says Gail Thackeray. "Now they cost forty bucks - and that's all just to cover the costs from rip-off artists."

Electronic nuisance criminals are parasites. One by one they're not much harm, no big deal. But they never come just one by one. They come in swarms, heaps, legions, sometimes whole subcultures. And they bite. Every time we buy a credit card today, we lose a little financial vitality to a particular species of bloodsucker. What, in her expert opinion, are the worst forms of electronic crime, I ask, consulting my notes. Is it credit card fraud? Breaking into ATM bank machines? Phone-phreaking? Computer intrusions? Software viruses? Access-code theft? Records tampering? Software piracy? Pornographic bulletin boards? Satellite TV piracy? Theft of cable service? It's a long list. By the time I reach the end of it I feel rather depressed. "Oh no," says Gail Thackeray, leaning forward over the table, her whole body gone stiff with energetic indignation, "the biggest damage is telephone fraud. Fake sweepstakes, fake charities. Boiler-room con operations. You could pay off the national debt with what these guys steal… They target old people, they get hold of credit ratings and demographics, they rip off the old and the weak." The words come tumbling out of her.

It's low-tech stuff, your everyday boiler-room fraud. Grifters, conning people out of money over the phone, have been around for decades. This is where the word "phony" came from!

It's just that it's so much easier now, horribly facilitated by advances in technology and the byzantine structure of the modern phone system. The same professional fraudsters do it over and over, Thackeray tells me, they hide behind dense onion-shells of fake companies… fake holding corporations nine or ten layers deep, registered all over the map. They get a phone installed under a false name in an empty safe-house. And then they call-forward everything out of that phone to yet another phone, a phone that may even be in another state. And they don't even pay the charges on their phones; after a month or so, they just split. Set up somewhere else in another Podunkville with the same seedy crew of veteran phone-crooks. They buy or steal commercial credit card reports, slap them on the PC, have a program pick out people over sixty-five who pay a lot to charities. A whole subculture living off this, merciless folks on the con.

"The `light-bulbs for the blind' people," Thackeray muses, with a special loathing. "There's just no end to them."

We're sitting in a downtown diner in Phoenix, Arizona. It's a tough town, Phoenix. A state capital seeing some hard times. Even to a Texan like myself, Arizona state politics seem rather baroque. There was, and remains, endless trouble over the Martin Luther King holiday, the sort of stiff-necked, foot-shooting incident for which Arizona politics seem famous. There was Evan Mecham, the eccentric Republican millionaire governor who was impeached, after reducing state government to a ludicrous shambles. Then there was the national Keating scandal, involving Arizona savings and loans, in which both of Arizona's U.S. senators, DeConcini and McCain, played sadly prominent roles.

And the very latest is the bizarre AzScam case, in which state legislators were videotaped, eagerly taking cash from an informant of the Phoenix city police department, who was posing as a Vegas mobster.

"Oh," says Thackeray cheerfully. "These people are amateurs here, they thought they were finally getting to play with the big boys. They don't have the least idea how to take a bribe! It's not institutional corruption. It's not like back in Philly."

Gail Thackeray was a former prosecutor in Philadelphia. Now she's a former assistant attorney general of the State of Arizona. Since moving to Arizona in 1986, she had worked under the aegis of Steve Twist, her boss in the Attorney General's office. Steve Twist wrote Arizona's pioneering computer crime laws and naturally took an interest in seeing them enforced. It was a snug niche, and Thackeray's Organized Crime and Racketeering Unit won a national reputation for ambition and technical knowledgeability… Until the latest election in Arizona. Thackeray's boss ran for the top job, and lost. The victor, the new Attorney General, apparently went to some pains to eliminate the bureaucratic traces of his rival, including his pet group - Thackeray's group. Twelve people got their walking papers.

Now Thackeray's painstakingly assembled computer lab sits gathering dust somewhere in the glass-and-concrete Attorney General's HQ on 1275 Washington Street. Her computer crime books, her painstakingly garnered back issues of phreak and hacker zines, all bought at her own expense - are piled in boxes somewhere. The State of Arizona is simply not particularly interested in electronic racketeering at the moment.

At the moment of our interview, Gail Thackeray, officially unemployed, is working out of the county sheriff's office, living on her savings, and prosecuting several cases - working 60-hour weeks, just as always - for no pay at all. "I'm trying to train people," she mutters.

Half her life seems to be spent training people - merely pointing out, to the naive and incredulous (such as myself) that this stuff is actually going on out there. It's a small world, computer crime. A young world. Gail Thackeray, a trim blonde Baby Boomer who favors Grand Canyon white-water rafting to kill some slow time, is one of the world's most senior, most veteran "hacker-trackers." Her mentor was Donn Parker, the California think-tank theorist who got it all started 'way back in the mid70s, the "grandfather of the field," "the great bald eagle of computer crime."

And what she has learned, Gail Thackeray teaches. Endlessly. Tirelessly. To anybody. To Secret Service agents and state police, at the Glynco, Georgia federal training center. To local police, on "roadshows" with her slide pro-

jector and notebook. To corporate security personnel. To journalists. To parents.

Even crooks look to Gail Thackeray for advice. Phone-phreaks call her at the office. They know very well who she is. They pump her for information on what the cops are up to, how much they know. Sometimes whole crowds of phone phreaks, hanging out on illegal conference calls, will call Gail Thackeray up. They taunt her. And, as always, they boast. Phone-phreaks, real stone phone-phreaks, simply cannot shut up. They natter on for hours.

Left to themselves, they mostly talk about the intricacies of ripping-off phones; it's about as interesting as listening to hot-rodders talk about suspension and distributor-caps. They also gossip cruelly about each other. And when talking to Gail Thackeray, they incriminate themselves. "I have tapes," Thackeray says coolly.

Phone phreaks just talk like crazy. "Dial-Tone" out in Alabama has been known to spend half an hour simply reading stolen phone-codes aloud into voice-mail answering machines. Hundreds, thousands of numbers, recited in a monotone, without a break - an eerie phenomenon. When arrested, it's a rare phone phreak who doesn't inform at endless length on everybody he knows.

Hackers are no better. What other group of criminals, she asks rhetorically, publishes newsletters and holds conventions? She seems deeply nettled by the sheer brazenness of this behavior, though to an outsider, this activity might make one wonder whether hackers should be considered "criminals" at all. Skateboarders have magazines, and they trespass a lot. Hot rod people have magazines and they break speed limits and sometimes kill people…

I ask her whether it would be any loss to society if phone phreaking and computer hacking, as hobbies, simply dried up and blew away, so that nobody ever did it again. She seems surprised. "No," she says swiftly. "Maybe a little… in the old days… the MIT stuff… But there's a lot of wonderful, legal stuff you can do with computers now, you don't have to break into somebody else's just to learn. You don't have that excuse. You can learn all you like." Did you ever hack into a system? I ask.

The trainees do it at Glynco. Just to demonstrate system vulnerabilities. She's cool to the notion. Genuinely indifferent. "What kind of computer do you have?"

"A Compaq 286LE," she mutters.

"What kind do you wish you had?"

At this question, the unmistakable light of true hackerdom flares in Gail Thackeray's eyes. She becomes tense, animated, the words pour out: "An Amiga 2000 with an IBM card and Mac emulation! The most common hacker machines are Amigas and Commodores. And Apples." If she had the Amiga, she enthuses, she could run a whole galaxy of seized computer-evidence disks on one convenient multifunctional machine. A cheap one, too. Not like the old Attorney General lab, where they had an ancient CP/M machine, assorted Amiga flavors and Apple flavors, a couple IBMs, all the utility software… but no Commodores. The workstations down at the Attorney General's are Wang dedicated word-processors. Lame machines tied in to an office net - though at least they get online to the Lexis and Westlaw legal data services. I don't say anything. I recognize the syndrome, though. This computer-fever has been running through segments of our society for years now. It's a strange kind of lust: K-hunger, Meg-hunger; but it's a shared disease; it can kill parties dead, as conversation spirals into the deepest and most deviant recesses of software releases and expensive peripherals… The mark of the hacker beast. I have it too. The whole "electronic community," whatever the hell that is, has it. Gail Thackeray has it. Gail Thackeray is a hacker cop. My immediate reaction is a strong rush of indignant pity: why doesn't somebody buy this woman her Amiga?! It's not like she's asking for a Cray X-MP supercomputer mainframe; an Amiga's a sweet little cookie-box thing. We're losing zillions in organized fraud; prosecuting and defending a single hacker case in court can cost a hundred grand easy. How come nobody can come up with four lousy grand so this woman can do her job? For a hundred grand we could buy every computer cop in America an Amiga. There aren't that many of 'em.

Computers. The lust, the hunger, for computers. The loyalty they inspire, the intense sense of possessiveness. The culture they have bred. I myself am

sitting in downtown Phoenix, Arizona because it suddenly occurred to me that the police might - just might - come and take away my computer. The prospect of this, the mere implied threat, was unbearable. It literally changed my life. It was changing the lives of many others. Eventually it would change everybody's life.

Gail Thackeray was one of the top computer crime people in America. And I was just some novelist, and yet I had a better computer than hers. Practically everybody I knew had a better computer than Gail Thackeray and her feeble laptop 286. It was like sending the sheriff in to clean up Dodge City and arming her with a slingshot cut from an old rubber tire.

But then again, you don't need a howitzer to enforce the law. You can do a lot just with a badge. With a badge alone, you can basically wreak havoc, take a terrible vengeance on wrongdoers. Ninety percent of "computer crime investigation" is just "crime investigation:" names, places, dossiers, modus operandi, search warrants, victims, complainants, informants…

What will computer crime look like in ten years? Will it get better? Did "Sundevil" send 'em reeling back in confusion?

It'll be like it is now, only worse, she tells me with perfect conviction. Still there in the background, ticking along, changing with the times: the criminal underworld. It'll be like drugs are. Like our problems with alcohol. All the cops and laws in the world never solved our problems with alcohol. If there's something people want, a certain percentage of them are just going to take it. Fifteen percent of the populace will never steal. Fifteen percent will steal most anything not nailed down. The battle is for the hearts and minds of the remaining seventy percent.

And criminals catch on fast. If there's not "too steep a learning curve" - if it doesn't require a baffling amount of expertise and practice - then criminals are often some of the first through the gate of a new technology. Especially if it helps them to hide. They have tons of cash, criminals. The new communications tech - like pagers, cellular phones, faxes, Federal Express - were pioneered by rich corporate people, and by criminals. In the early years of pagers and beepers, dope dealers were so enthralled this technology that owing a beeper was practically prima facie evidence of cocaine dealing. CB radio exploded when the speed limit hit 55 and breaking the highway law became a national pastime. Dope dealers send cash by Federal Express, despite, or perhaps because of, the warnings in Fed Ex offices that tell you never to try this. Fed Ex uses X-rays and dogs on their mail, to stop drug shipments. That doesn't work very well.

Drug dealers went wild over cellular phones. There are simple methods of faking ID on cellular phones, making the location of the call mobile, free of charge, and effectively untraceable. Now victimized cellular companies routinely bring in vast toll-lists of calls to Colombia and Pakistan.

Judge Greene's fragmentation of the phone company is driving law enforcement nuts. Four thousand telecommunications companies. Fraud skyrocketing. Every temptation in the world available with a phone and a credit card number. Criminals untraceable. A galaxy of "new neat rotten things to do."

If there were one thing Thackeray would like to have, it would be an effective legal end-run through this new fragmentation minefield.

It would be a new form of electronic search warrant, an "electronic letter of marque" to be issued by a judge. It would create a new category of "electronic emergency." Like a wiretap, its use would be rare, but it would cut across state lines and force swift cooperation from all concerned. Cellular, phone, laser, computer network, PBXes, AT&T, Baby Bells, long-distance entrepreneurs, packet radio. Some document, some mighty court-order, that could slice through four thousand separate forms of corporate red-tape, and get her at once to the source of calls, the source of email threats and viruses, the sources of bomb threats, kidnapping threats. "From now on," she says, "the Lindberg baby will always die."

Something that would make the Net sit still, if only for a moment. Something that would get her up to speed. Seven league boots. That's what she really needs. "Those guys move in nanoseconds and I'm on the Pony Express." And then, too, there's the coming international angle. Electronic crime has never been easy to localize, to tie to a physical jurisdiction. And phone

phreaks and hackers loathe boundaries, they jump them whenever they can. The English. The Dutch. And the Germans, especially the ubiquitous Chaos Computer Club. The Australians. They've all learned phone-phreaking from America. It's a growth mischief industry. The multinational networks are global, but governments and the police simply aren't. Neither are the laws. Or the legal frameworks for citizen protection.

One language is global, though - English. Phone phreaks speak English; it's their native tongue even if they're Germans. English may have started in England but now it's the Net language; it might as well be called "CNNese."

Asians just aren't much into phone phreaking. They're the world masters at organized software piracy. The French aren't into phone-phreaking either. The French are into computerized industrial espionage.

In the old days of the MIT righteous hackerdom, crashing systems didn't hurt anybody. Not all that much, anyway. Not permanently. Now the players are more venal. Now the consequences are worse. Hacking will begin killing people soon. Already there are methods of stacking calls onto 911 systems, annoying the police, and possibly causing the death of some poor soul calling in with a genuine emergency. Hackers in Amtrak computers, or airtraffic control computers, will kill somebody someday. Maybe a lot of people. Gail Thackeray expects it.

And the viruses are getting nastier. The "Scud" virus is the latest one out. It wipes hard-disks.

According to Thackeray, the idea that phonephreaks are Robin Hoods is a fraud. They don't deserve this repute. Basically, they pick on the weak. AT&T now protects itself with the fearsome ANI (Automatic Number Identification) trace capability. When AT&T wised up and tightened security generally, the phreaks drifted into the Baby Bells. The Baby Bells lashed out in 1989 and 1990, so the phreaks switched to smaller long-distance entrepreneurs. Today, they are moving into locally owned PBXes and voice-mail systems, which are full of security holes, dreadfully easy to hack. These victims aren't the moneybags Sheriff of Nottingham or Bad King John, but small groups of innocent people who find it hard to protect themselves, and who really suffer from these depredations. Phone phreaks pick on the weak. They do it for power. If it were legal, they wouldn't do it. They don't want service, or knowledge, they want the thrill of powertripping. There's plenty of knowledge or service around, if you're willing to pay. Phone phreaks don't pay, they steal. It's because it is illegal that it feels like power, that it gratifies their vanity.

I leave Gail Thackeray with a handshake at the door of her office building - a vast International Style office building downtown. The Sheriff's office is renting part of it. I get the vague impression that quite a lot of the building is empty - real estate crash. In a Phoenix sports apparel store, in a downtown mall, I meet the "Sun Devil" himself. He is the cartoon mascot of Arizona State University, whose football stadium, "Sundevil," is near the local Secret Service HQ - hence the name Operation Sundevil. The Sun Devil himself is named "Sparky." Sparky the Sun Devil is maroon and bright yellow, the school colors. Sparky brandishes a three-tined yellow pitchfork. He has a small mustache, pointed ears, a barbed tail, and is dashing forward jabbing the air with the pitchfork, with an expression of devilish glee.

Phoenix was the home of Operation Sundevil. The Legion of Doom ran a hacker bulletin board called "The Phoenix Project." An Australian hacker named "Phoenix" once burrowed through the Internet to attack Cliff Stoll, then bragged and boasted about it to The New York Times. This net of coincidence is both odd and meaningless.

The headquarters of the Arizona Attorney General, Gail Thackeray's former workplace, is on 1275 Washington Avenue. Many of the downtown streets in Phoenix are named after prominent American presidents: Washington, Jefferson, Madison…

After dark, all the employees go home to their suburbs. Washington, Jefferson and Madison - what would be the Phoenix inner city, if there were an inner city in this sprawling automobile-bred town - become the haunts of transients and derelicts. The homeless. The sidewalks along Washington are lined with orange trees. Ripe fallen fruit lies scattered like croquet balls on the

sidewalks and gutters. No one seems to be eating them. I try a fresh one. It tastes unbearably bitter.

The Attorney General's office, built in 1981 during the Babbitt administration, is a long low two story building of white cement and wall-sized sheets of curtain-glass. Behind each glass wall is a lawyer's office, quite open and visible to anyone strolling by. Across the street is a dour government building labelled simply ECONOMIC SECURITY, something that has not been in great supply in the American Southwest lately.

The offices are about twelve feet square. They feature tall wooden cases full of red-spined lawbooks; Wang computer monitors; telephones; Post-it notes galore. Also framed law diplomas and a general excess of bad Western landscape art. Ansel Adams photos are a big favorite, perhaps to compensate for the dismal specter of the parking lot, two acres of striped black asphalt, which features gravel landscaping and some sickly-looking barrel cacti.

It has grown dark. Gail Thackeray has told me that the people who work late here, are afraid of muggings in the parking lot. It seems cruelly ironic that a woman tracing electronic racketeers across the interstate labyrinth of Cyberspace should fear an assault by a homeless derelict in the parking lot of her own workplace.

Perhaps this is less than coincidence. Perhaps these two seemingly disparate worlds are somehow generating one another. The poor and disenfranchised take to the streets, while the rich and computer-equipped, safe in their bedrooms, chatter over their modems. Quite often the derelicts kick the glass out and break in to the lawyers' offices, if they see something they need or want badly enough. I cross the parking lot to the street behind the Attorney General's office. A pair of young tramps are bedding down on flattened sheets of cardboard, under an alcove stretching over the sidewalk. One tramp wears a glitter-covered T-shirt reading "CALIFORNIA" in Coca-Cola cursive. His nose and cheeks look chafed and swollen; they glisten with what seems to be Vaseline. The other tramp has a ragged long-sleeved shirt and lank brown hair parted in the middle. They both wear blue jeans coated in grime. They are both drunk. "You guys crash here a lot?" I ask them.

They look at me warily. I am wearing black jeans, a black pinstriped suit jacket and a black silk tie. I have odd shoes and a funny haircut.

"It's our first time here," says the red-nosed tramp unconvincingly. There is a lot of cardboard stacked here. More than any two people could use.

"We usually stay at the Vinnie's down the street," says the brown-haired tramp, puffing a Marlboro with a meditative air, as he sprawls with his head on a blue nylon backpack. "The Saint Vincent's." "You know who works in that building over there?" I ask, pointing. The brown-haired tramp shrugs. "Some kind of attorneys, it says."

We urge one another to take it easy. I give them five bucks. A block down the street I meet a vigorous workman who is wheeling along some kind of industrial trolley; it has what appears to be a tank of propane on it.

We make eye contact. We nod politely. I walk past him. "Hey! Excuse me sir!" he says.

"Yes?" I say, stopping and turning.

"Have you seen," the guy says rapidly, "a black guy, about 6'7", scars on both his cheeks like this -" he gestures - "wears a black baseball cap on backwards, wandering around here anyplace?"

"Sounds like I don't much want to meet him," I say.

"He took my wallet," says my new acquaintance. "Took it this morning. Y'-know, some people would be scared of a guy like that. But I'm not scared. I'm from Chicago. I'm gonna hunt him down. We do things like that in Chicago."

"Yeah?"

"I went to the cops and now he's got an APB out on his ass," he says with satisfaction. "You run into him, you let me know." "Okay," I say. "What is your name, sir?"

"Stanley…"

"And how can I reach you?"

"Oh," Stanley says, in the same rapid voice, "you don't have to reach, uh, me. You can just call the cops. Go straight to the cops." He reaches into a

pocket and pulls out a greasy piece of pasteboard. “See, here’s my report on him.”

I look. The “report,” the size of an index card, is labelled PRO-ACT: Phoenix Residents Opposing Active Crime Threat… or is it Organized Against Crime Threat? In the darkening street it’s hard to read. Some kind of vigilante group? Neighborhood watch? I feel very puzzled.

“Are you a police officer, sir?”

He smiles, seems very pleased by the question.

“No,” he says.

“But you are a `Phoenix Resident?”’

“Would you believe a homeless person,” Stanley says.

“Really? But what’s with the…” For the first time I take a close look at Stanley’s trolley. It’s a rubber-wheeled thing of industrial metal, but the device I had mistaken for a tank of propane is in fact a water-cooler. Stanley also has an Army duffel-bag, stuffed tight as a sausage with clothing or perhaps a tent, and, at the base of his trolley, a cardboard box and a battered leather briefcase.

“I see,” I say, quite at a loss. For the first time I notice that Stanley has a wallet. He has not lost his wallet at all. It is in his back pocket and chained to his belt. It’s not a new wallet. It seems to have seen a lot of wear.

“Well, you know how it is, brother,” says Stanley. Now that I know that he is homeless - a possible threat - my entire perception of him has changed in an instant. His speech, which once seemed just bright and enthusiastic, now seems to have a dangerous tang of mania. “I have to do this!” he assures me. “Track this guy down… It’s a thing I do… you know… to keep myself together!” He smiles, nods, lifts his trolley by its decaying rubber handgrips.

“Gotta work together, y’know,” Stanley booms, his face alight with cheerfulness, “the police can’t do everything!”

The gentlemen I met in my stroll in downtown Phoenix are the only computer illiterates in this book. To regard them as irrelevant, however, would be a grave mistake.

As computerization spreads across society, the populace at large is subjected to wave after wave of future shock. But, as a necessary converse, the “computer community” itself is subjected to wave after wave of incoming computer illiterates. How will those currently enjoying America’s digital bounty regard, and treat, all this teeming refuse yearning to breathe free? Will the electronic frontier be another Land of Opportunity - or an armed and monitored enclave, where the disenfranchised snuggle on their cardboard at the locked doors of our houses of justice?

Some people just don’t get along with computers. They can’t read. They can’t type. They just don’t have it in their heads to master arcane instructions in wirebound manuals. Somewhere, the process of computerization of the populace will reach a limit. Some people - quite decent people maybe, who might have thrived in any other situation - will be left irretrievably outside the bounds. What’s to be done with these people, in the bright new shiny electroworld? How will they be regarded, by the mouse-whizzing masters of cyberspace? With contempt? Indifference? Fear?

In retrospect, it astonishes me to realize how quickly poor Stanley became a perceived threat. Surprise and fear are closely allied feelings. And the world of computing is full of surprises.

I met one character in the streets of Phoenix whose role in those book is supremely and directly relevant. That personage was Stanley’s giant thieving scarred phantom. This phantasm is everywhere in this book. He is the specter haunting cyberspace.

Sometimes he’s a maniac vandal ready to smash the phone system for no sane reason at all. Sometimes he’s a fascist fed, coldly programming his mighty mainframes to destroy our Bill of Rights. Sometimes he’s a telco bureaucrat, covertly conspiring to register all modems in the service of an Orwellian surveillance regime. Mostly, though, this fearsome phantom is a “hacker.” He’s strange, he doesn’t belong, he’s not authorized, he doesn’t smell right, he’s not keeping his proper place, he’s not one of us. The focus of fear is the hacker, for much the same reasons that Stanley’s fancied assailant is black.

Stanley's demon can't go away, because he doesn't exist. Despite single-minded and tremendous effort, he can't be arrested, sued, jailed, or fired. The only constructive way to do anything about him is to learn more about Stanley himself. This learning process may be repellent, it may be ugly, it may involve grave elements of paranoiac confusion, but it's necessary. Knowing Stanley requires something more than class-crossing condescension. It requires more than steely legal objectivity. It requires human compassion and sympathy. To know Stanley is to know his demon. If you know the other guy's demon, then maybe you'll come to know some of your own. You'll be able to separate reality from illusion. And then you won't do your cause, and yourself, more harm than good. Like poor damned Stanley from Chicago did.

Part Four: The Civil Libertarians.

- NuPrometheus + FBI = Grateful Dead
- Whole Earth + Computer Revolution = WELL
- Phiber Runs Underground and Acid Spikes the Well
- The Trial of Knight Lightning
- Shadowhawk Plummets to Earth
- Kyrie in the Confessional
- $79,499
- A Scholar Investigates
- Computers, Freedom, and Privacy

The story of the Hacker Crackdown, as we have followed it thus far, has been technological, subcultural, criminal and legal. The story of the Civil Libertarians, though it partakes of all those other aspects, is profoundly and thoroughly political.

In 1990, the obscure, long-simmering struggle over the ownership and nature of cyberspace became loudly and irretrievably public. People from some of the oddest corners of American society suddenly found themselves public figures. Some of these people found this situation much more than they had ever bargained for. They backpedalled, and tried to retreat back to the mandarin obscurity of their cozy subcultural niches. This was generally to prove a mistake.

But the civil libertarians seized the day in 1990. They found themselves organizing, propagandizing, podium-pounding, persuading, touring, negotiating, posing for publicity photos, submitting to interviews, squinting in the limelight as they tried a tentative, but growingly sophisticated, buck-and-wing upon the public stage.

It’s not hard to see why the civil libertarians should have this competitive advantage.

The hackers of the digital underground are an hermetic elite. They find it hard to make any remotely convincing case for their actions in front of the general public. Actually, hackers roundly despise the “ignorant” public, and have never trusted the judgement of “the system.” Hackers do propagandize, but only among themselves, mostly in giddy, badly spelled manifestos of class warfare, youth rebellion or naive techie utopianism. Hackers must strut and boast in order to establish and preserve their underground reputations. But if they speak out too loudly and publicly, they will break the fragile surface-tension of the underground, and they will be harrassed or arrested. Over the longer term, most hackers stumble, get busted, get betrayed, or simply give up. As a political force, the digital underground is hamstrung.

The telcos, for their part, are an ivory tower under protracted seige. They have plenty of money with which to push their calculated public image, but they waste much energy and goodwill attacking one another with slanderous and demeaning ad campaigns. The telcos have suffered at the hands of politicians, and, like hackers, they don’t trust the public’s judgement. And this distrust may be well-founded. Should the general public of the high-tech 1990s come to understand its own best interests in telecommunications, that might well pose a grave threat to the specialized technical power and authority that the telcos have relished for over a century. The telcos do have strong advantages: loyal employees, specialized expertise, influence in the halls of power, tactical allies in law enforcement, and unbelievably vast amounts of money. But politically speaking, they lack genuine grassroots support; they simply don’t seem to have many friends.

Cops know a lot of things other people don’t know. But cops willingly reveal only those aspects of their knowledge that they feel will meet their institutional purposes and further public order. Cops have respect, they have responsibilities, they have power in the streets and even power in the home,

but cops don't do particularly well in limelight. When pressed, they will step out in the public gaze to threaten bad guys, or to cajole prominent citizens, or perhaps to sternly lecture the naive and misguided. But then they go back within their time-honored fortress of the station-house, the courtroom and the rule-book.

The electronic civil libertarians, however, have proven to be born political animals. They seemed to grasp very early on the postmodern truism that communication is power. Publicity is power. Soundbites are power. The ability to shove one's issue onto the public agenda - and keep it there - is power. Fame is power. Simple personal fluency and eloquence can be power, if you can somehow catch the public's eye and ear.

The civil libertarians had no monopoly on "technical power" - though they all owned computers, most were not particularly advanced computer experts. They had a good deal of money, but nowhere near the earthshaking wealth and the galaxy of resources possessed by telcos or federal agencies. They had no ability to arrest people. They carried out no phreak and hacker covert dirty-tricks.

But they really knew how to network.

Unlike the other groups in this book, the civil libertarians have operated very much in the open, more or less right in the public hurly-burly. They have lectured audiences galore and talked to countless journalists, and have learned to refine their spiels. They've kept the cameras clicking, kept those faxes humming, swapped that email, run those photocopiers on overtime, licked envelopes and spent small fortunes on airfare and long-distance. In an information society, this open, overt, obvious activity has proven to be a profound advantage.

In 1990, the civil libertarians of cyberspace assembled out of nowhere in particular, at warp speed. This "group" (actually, a networking gaggle of interested parties which scarcely deserves even that loose term) has almost nothing in the way of formal organization. Those formal civil libertarian organizations which did take an interest in cyberspace issues, mainly the Computer Professionals for Social Responsibility and the American Civil Liberties Union, were carried along by events in 1990, and acted mostly as adjuncts, underwriters or launching-pads.

The civil libertarians nevertheless enjoyed the greatest success of any of the groups in the Crackdown of 1990. At this writing, their future looks rosy and the political initiative is firmly in their hands. This should be kept in mind as we study the highly unlikely lives and lifestyles of the people who actually made this happen.

-Section 1-

In June 1989, Apple Computer, Inc., of Cupertino, California, had a problem. Someone had illicitly copied a small piece of Apple's proprietary software, software which controlled an internal chip driving the Macintosh screen display. This Color QuickDraw source code was a closely guarded piece of Apple's intellectual property. Only trusted Apple insiders were supposed to possess it.

But the "NuPrometheus League" wanted things otherwise. This person (or persons) made several illicit copies of this source code, perhaps as many as two dozen. He (or she, or they) then put those illicit floppy disks into envelopes and mailed them to people all over America: people in the computer industry who were associated with, but not directly employed by, Apple Computer.

The NuPrometheus caper was a complex, highly ideological, and very hacker-like crime. Prometheus, it will be recalled, stole the fire of the Gods and gave this potent gift to the general ranks of downtrodden mankind. A similar god-in-the-manger attitude was implied for the corporate elite of Apple Computer, while the "Nu" Prometheus had himself cast in the role of rebel demi-god. The illicitly copied data was given away for free.

The new Prometheus, whoever he was, escaped the fate of the ancient Greek Prometheus, who was chained to a rock for centuries by the vengeful gods while an eagle tore and ate his liver. On the other hand, NuPrometheus chickened out

somewhat by comparison with his role model. The small chunk of Color QuickDraw code he had filched and replicated was more or less useless to Apple's industrial rivals (or, in fact, to anyone else). Instead of giving fire to mankind, it was more as if NuPrometheus had photocopied the schematics for part of a Bic lighter. The act was not a genuine work of industrial espionage. It was best interpreted as a symbolic, deliberate slap in the face for the Apple corporate hierarchy.

Apple's internal struggles were well-known in the industry. Apple's founders, Jobs and Wozniak, had both taken their leave long since. Their raucous core of senior employees had been a barnstorming crew of 1960s Californians, many of them markedly less than happy with the new button-down multimillion dollar regime at Apple. Many of the programmers and developers who had invented the Macintosh model in the early 1980s had also taken their leave of the company. It was they, not the current masters of Apple's corporate fate, who had invented the stolen Color QuickDraw code. The NuPrometheus stunt was well-calculated to wound company morale.

Apple called the FBI. The Bureau takes an interest in high-profile intellectual-property theft cases, industrial espionage and theft of trade secrets. These were likely the right people to call, and rumor has it that the entities responsible were in fact discovered by the FBI, and then quietly squelched by Apple management. NuPrometheus was never publicly charged with a crime, or prosecuted, or jailed. But there were no further illicit releases of Macintosh internal software. Eventually the painful issue of NuPrometheus was allowed to fade.

In the meantime, however, a large number of puzzled bystanders found themselves entertaining surprise guests from the FBI.

One of these people was John Perry Barlow. Barlow is a most unusual man, difficult to describe in conventional terms. He is perhaps best known as a songwriter for the Grateful Dead, for he composed lyrics for "Hell in a Bucket," "Picasso Moon," "Mexicali Blues," "I Need a Miracle," and many more; he has been writing for the band since 1970.

Before we tackle the vexing question as to why a rock lyricist should be interviewed by the FBI in a computer crime case, it might be well to say a word or two about the Grateful Dead. The Grateful Dead are perhaps the most successful and long-lasting of the numerous cultural emanations from the Haight-Ashbury district of San Francisco, in the glory days of Movement politics and lysergic transcendance. The Grateful Dead are a nexus, a veritable whirlwind, of applique decals, psychedelic vans, tie-dyed T-shirts, earth-color denim, frenzied dancing and open and unashamed drug use. The symbols, and the realities, of Californian freak power surround the Grateful Dead like knotted macrame.

The Grateful Dead and their thousands of Deadhead devotees are radical Bohemians. This much is widely understood. Exactly what this implies in the 1990s is rather more problematic.

The Grateful Dead are among the world's most popular and wealthy entertainers: number 20, according to Forbes magazine, right between M.C. Hammer and Sean Connery. In 1990, this jeans-clad group of purported raffish outcasts earned seventeen million dollars. They have been earning sums much along this line for quite some time now.

And while the Dead are not investment bankers or three-piece-suit tax specialists - they are, in point of fact, hippie musicians - this money has not been squandered in senseless Bohemian excess. The Dead have been quietly active for many years, funding various worthy activities in their extensive and widespread cultural community.

The Grateful Dead are not conventional players in the American power establishment. They nevertheless are something of a force to be reckoned with. They have a lot of money and a lot of friends in many places, both likely and unlikely.

The Dead may be known for back-to-the-earth environmentalist rhetoric, but this hardly makes them anti-technological Luddites. On the contrary, like most rock musicians, the Grateful Dead have spent their entire adult lives in the company of complex electronic equipment. They have funds to burn on any soph-

isticated tool and toy that might happen to catch their fancy. And their fancy is quite extensive.

The Deadhead community boasts any number of recording engineers, lighting experts, rock video mavens, electronic technicians of all descriptions. And the drift goes both ways. Steve Wozniak, Apple's co-founder, used to throw rock festivals. Silicon Valley rocks out.

These are the 1990s, not the 1960s. Today, for a surprising number of people all over America, the supposed dividing line between Bohemian and technician simply no longer exists. People of this sort may have a set of windchimes and a dog with a knotted kerchief 'round its neck, but they're also quite likely to own a multimegabyte Macintosh running MIDI synthesizer software and trippy fractal simulations. These days, even Timothy Leary himself, prophet of LSD, does virtual-reality computer-graphics demos in his lecture tours.

John Perry Barlow is not a member of the Grateful Dead. He is, however, a ranking Deadhead.

Barlow describes himself as a "techno-crank." A vague term like "social activist" might not be far from the mark, either. But Barlow might be better described as a "poet" - if one keeps in mind Percy Shelley's archaic definition of poets as "unacknowledged legislators of the world."

Barlow once made a stab at acknowledged legislator status. In 1987, he narrowly missed the Republican nomination for a seat in the Wyoming State Senate. Barlow is a Wyoming native, the third-generation scion of a well-to-do cattle-ranching family. He is in his early forties, married and the father of three daughters.

Barlow is not much troubled by other people's narrow notions of consistency. In the late 1980s, this Republican rock lyricist cattle rancher sold his ranch and became a computer telecommunications devotee.

The free-spirited Barlow made this transition with ease. He genuinely enjoyed computers. With a beep of his modem, he leapt from small-town Pinedale, Wyoming, into electronic contact with a large and lively crowd of bright, inventive, technological sophisticates from all over the world. Barlow found the social milieu of computing attractive: its fast-lane pace, its blue-sky rhetoric, its open-endedness. Barlow began dabbling in computer journalism, with marked success, as he was a quick study, and both shrewd and eloquent. He frequently travelled to San Francisco to network with Deadhead friends. There Barlow made extensive contacts throughout the Californian computer community, including friendships among the wilder spirits at Apple.

In May 1990, Barlow received a visit from a local Wyoming agent of the FBI. The NuPrometheus case had reached Wyoming.

Barlow was troubled to find himself under investigation in an area of his interests once quite free of federal attention. He had to struggle to explain the very nature of computer crime to a headscratching local FBI man who specialized in cattle-rustling. Barlow, chatting helpfully and demonstrating the wonders of his modem to the puzzled fed, was alarmed to find all "hackers" generally under FBI suspicion as an evil influence in the electronic community. The FBI, in pursuit of a hacker called "NuPrometheus," were tracing attendees of a suspect group called the Hackers Conference.

The Hackers Conference, which had been started in 1984, was a yearly Californian meeting of digital pioneers and enthusiasts. The hackers of the Hackers Conference had little if anything to do with the hackers of the digital underground. On the contrary, the hackers of this conference were mostly well-to-do Californian high-tech CEOs, consultants, journalists and entrepreneurs. (This group of hackers were the exact sort of "hackers" most likely to react with militant fury at any criminal degradation of the term "hacker.")

Barlow, though he was not arrested or accused of a crime, and though his computer had certainly not gone out the door, was very troubled by this anomaly. He carried the word to the Well.

Like the Hackers Conference, "the Well" was an emanation of the Point Foundation. Point Foundation, the inspiration of a wealthy Californian 60s radical named Stewart Brand, was to be a major launch-pad of the civil libertarian effort.

Point Foundation's cultural efforts, like those of their fellow Bay Area Californians the Grateful Dead, were multifaceted and multitudinous. Rigid ideological consistency had never been a strong suit of the Whole Earth Catalog. This Point publication had enjoyed a strong vogue during the late 60s and early 70s, when it offered hundreds of practical (and not so practical) tips on communitarian living, environmentalism, and getting back-to-the-land. The Whole Earth Catalog, and its sequels, sold two and half million copies and won a National Book Award.

With the slow collapse of American radical dissent, the Whole Earth Catalog had slipped to a more modest corner of the cultural radar; but in its magazine incarnation, CoEvolution Quarterly, the Point Foundation continued to offer a magpie potpourri of "access to tools and ideas."

CoEvolution Quarterly,which started in 1974, was never a widely popular magazine. Despite periodic outbreaks of millenarian fervor, CoEvolution Quarterly failed to revolutionize Western civilization and replace leaden centuries of history with bright new Californian paradigms. Instead, this propaganda arm of Point Foundation cakewalked a fine line between impressive brilliance and New Age flakiness. CoEvolution Quarterly carried no advertising, cost a lot, and came out on cheap newsprint with modest black-and-white graphics. It was poorly distributed, and spread mostly by subscription and word of mouth.

It could not seem to grow beyond 30,000 subscribers. And yet - it never seemed to shrink much, either. Year in, year out, decade in, decade out, some strange demographic minority accreted to support the magazine. The enthusiastic readership did not seem to have much in the way of coherent politics or ideals. It was sometimes hard to understand what held them together (if the often bitter debate in the letter-columns could be described as "togetherness").

But if the magazine did not flourish, it was resilient; it got by. Then, in 1984, the birth-year of the Macintosh computer, CoEvolution Quarterly suddenly hit the rapids. Point Foundation had discovered the computer revolution. Out came the Whole Earth Software Catalog of 1984, arousing headscratching doubts among the tie-dyed faithful, and rabid enthusiasm among the nascent "cyberpunk" milieu, present company included. Point Foundation started its yearly Hackers Conference, and began to take an extensive interest in the strange new possibilities of digital counterculture. CoEvolution Quarterly folded its teepee, replaced by Whole Earth Software Review and eventually by Whole Earth Review (the magazine's present incarnation, currently under the editorship of virtual-reality maven Howard Rheingold).

1985 saw the birth of the "WELL" - the "Whole Earth 'Lectronic Link." The Well was Point Foundation's bulletin board system.

As boards went, the Well was an anomaly from the beginning, and remained one. It was local to San Francisco. It was huge, with multiple phonelines and enormous files of commentary. Its complex UNIX-based software might be most charitably described as "user-opaque." It was run on a mainframe out of the rambling offices of a non-profit cultural foundation in Sausalito. And it was crammed with fans of the Grateful Dead.

Though the Well was peopled by chattering hipsters of the Bay Area counterculture, it was by no means a "digital underground" board. Teenagers were fairly scarce; most Well users (known as "Wellbeings") were thirty- and forty-something Baby Boomers. They tended to work in the information industry: hardware, software, telecommunications, media, entertainment. Librarians, academics, and journalists were especially common on the Well, attracted by Point Foundation's open-handed distribution of "tools and ideas."

There were no anarchy files on the Well, scarcely a dropped hint about access codes or credit card theft. No one used handles. Vicious "flame-wars" were held to a comparatively civilized rumble. Debates were sometimes sharp, but no Wellbeing ever claimed that a rival had disconnected his phone, trashed his house, or posted his credit card numbers.

The Well grew slowly as the 1980s advanced. It charged a modest sum for access and storage, and lost money for years - but not enough to hamper the Point Foundation, which was nonprofit anyway. By 1990, the Well had about five thousand users. These users wandered about a gigantic cyberspace smorgasbord

of "Conferences", each conference itself consisting of a welter of "topics," each topic containing dozens, sometimes hundreds of comments, in a tumbling, multiperson debate that could last for months or years on end.

Conferencies on the Well

- WELL "Screenzine" Digest (g zine)
- Best of the WELL - vintage material - (g best)
- Index listing of new topics in all conferences (g newtops)

Business - Education

- Apple Library Users Group(g alug)
- Agriculture (g agri)
- Brainstorming (g brain)
- Classifieds (g cla)
- Computer Journalism (g cj)
- Consultants (g consult)
- Consumers (g cons)
- Design (g design)
- Desktop Publishing (g desk)
- Disability (g disability)
- Education (g ed)
- Energy (g energy91)
- Entrepreneurs (g entre)
- Homeowners (g home)
- Indexing (g indexing)
- Investments (g invest)
- Kids91 (g kids)
- Legal (g legal)
- One Person Business (g one)
- Periodical/newsletter (g per)
- Telecomm Law (g tcl)
- The Future (g fut)
- Translators (g trans)
- Travel (g tra)
- Work (g work)
- Electronic Frontier Foundation (g eff)
- Computers, Freedom & Privacy (g cfp)
- Computer Professionals for Social Responsibility (g cpsr)

Social - Political - Humani-ties

- Aging (g gray)
- AIDS (g aids)
- Amnesty International (g amnesty)
- Archives (g arc)
- Berkeley (g berk)
- Buddhist (g wonderland)
- Christian (g cross)
- Couples (g couples)
- Current Events (g curr)
- Dreams (g dream)
- Drugs (g dru)
- East Coast (g east)
- Emotional Health**** (g private)
- Erotica (g eros)
- Environment (g env)
- Firearms (g firearms)
- First Amendment (g first)
- Fringes of Reason (g fringes)
- Gay (g gay)
- Gay (Private)# (g gaypriv)
- Geography (g geo)
- German (g german)
- Gulf War (g gulf)
- Hawaii (g aloha)
- Health (g heal)
- History (g hist)
- Holistic (g holi)
- Interview (g inter)
- Italian (g ital)
- Jewish (g jew)
- Liberty (g liberty)
- Mind (g mind)
- Miscellaneous (g misc)
- Men on the WELL** (g mow)
- Network Integration (g origin)
- Nonprofits (g non)
- North Bay (g north)
- Northwest (g nw)
- Pacific Rim (g pacrim)
- Parenting (g par)
- Peace (g pea)
- Peninsula (g pen)
- Poetry (g poetry)
- Philosophy (g phi)
- Politics (g pol)
- Psychology (g psy)
- Psychotherapy (g therapy)
- Recovery## (g recovery)
- San Francisco (g sanfran)
- Scams (g scam)
- Sexuality (g sex)
- Singles (g singles)
- Southern (g south)
- Spanish (g spanish)
- Spirituality (g spirit)
- Tibet (g tibet)
- Transportation (g transport)
- True Confessions (g tru)
- Unclear (g unclear)
- WELL Writer's Workshop***(g www)
- Whole Earth (g we)
- Women on the WELL*(g wow)
- Words (g words)
- Writers (g wri)

**** Private Conference - mail wooly for entry
*** Private Conference - mail sonia for entry
** Private Conference - mail flash for entry
* Private Conference - mail reva for entry
# Private Conference - mail hudu for entry
Private Conference - mail dhawk for entry

Arts - Recreation - Entertainment

- ArtCom Electronic Net (g acen)
- Audio-Videophilia (g aud)
- Bicycles (g bike)
- Bay Area Tonight**(g bat)
- Boating (g wet)
- Books (g books)
- CD's (g cd)
- Comics (g comics)
- Cooking (g cook)
- Flying (g flying)
- Fun (g fun)
- Games (g games)
- Gardening (g gard)
- Kids (g kids)
- Nightowls* (g owl)
- Jokes (g jokes)
- MIDI (g midi)

- Movies (g movies)
- Motorcycling (g ride)
- Motoring (g car)
- Music (g mus)
- On Stage (g onstage)
- Pets (g pets)
- Radio (g rad)
- Restaurant (g rest)
- Science Fiction (g sf)
- Sports (g spo)
- Star Trek (g trek)
- Television (g tv)
- Theater (g theater)
- Weird (g weird)
- Zines/Factsheet Five(g f5)

* Open from midnight to 6am
** Updated daily

Grateful Dead

- Grateful Dead (g gd)
- Deadplan* (g dp)
- Deadlit (g deadlit)
- Feedback (g feedback)
- GD Hour (g gdh)
- Tapes (g tapes)
- Tickets (g tix)
- Tours (g tours)

* Private conference - mail tnf for entry

Computers

- AI/Forth/Realtime (g realtime)
- Amiga (g amiga)
- Apple (g app)
- Computer Books (g cbook)
- Art & Graphics (g gra)
- Hacking (g hack)
- HyperCard (g hype)
- IBM PC (g ibm)
- LANs (g lan)
- Laptop (g lap)
- Macintosh (g mac)
- Mactech (g mactech)
- Microtimes (g microx)
- Muchomedia (g mucho)
- NeXt (g next)
- OS/2 (g os2)
- Printers (g print)
- Programmer's Net (g net)
- Siggraph (g siggraph)
- Software Design (g sdc)
- Software/Programming (g software)
- Software Support (g ssc)
- Unix (g unix)
- Windows (g windows)
- Word Processing (g word)

Technical - Communications

- Bioinfo (g bioinfo)
- Info (g boing)
- Media (g media)
- NAPLPS (g naplps)
- Netweaver (g netweaver)
- Networld (g networld)
- Packet Radio (g packet)
- Photography (g pho)
- Radio (g rad)
- Science (g science)
- Technical Writers (g tec)
- Telecommunications(g tele)
- Usenet (g usenet)
- Video (g vid)
- Virtual Reality (g vr)

The WELL Itself

- Deeper (g deeper)
- Entry (g ent)
- General (g gentech)
- Help (g help)
- Hosts (g hosts)
- Policy (g policy)
- System News (g news)
- Test (g test)

The list itself is dazzling, bringing to the untutored eye a dizzying impression of a bizarre milieu of mountain-climbing Hawaiian holistic photographers trading true-life confessions with bisexual word-processing Tibetans.

But this confusion is more apparent than real. Each of these conferences was a little cyberspace world in itself, comprising dozens and perhaps hundreds of sub-topics. Each conference was commonly frequented by a fairly small, fairly like-minded community of perhaps a few dozen people. It was humanly impossible to encompass the entire Well (especially since access to the Well's mainframe computer was billed by the hour). Most long-time users contented themselves with a few favorite topical neighborhoods, with the occasional foray elsewhere for a taste of exotica. But especially important news items, and hot topical debates, could catch the attention of the entire Well community.

Like any community, the Well had its celebrities, and John Perry Barlow, the silver-tongued and silver-modemed lyricist of the Grateful Dead, ranked prominently among them. It was here on the Well that Barlow posted his true-life tale of computer crime encounter with the FBI.

The story, as might be expected, created a great stir. The Well was already primed for hacker controversy. In December 1989, Harper's magazine had hosted a debate on the Well about the ethics of illicit computer intrusion. While over forty various computer-mavens took part, Barlow proved a star in the debate. So did "Acid Phreak" and "Phiber Optik," a pair of young New York hacker-phreaks whose skills at telco switching-station intrusion were matched only by their apparently limitless hunger for fame. The advent of these two boldly swaggering

outlaws in the precincts of the Well created a sensation akin to that of Black Panthers at a cocktail party for the radically chic.

Phiber Optik in particular was to seize the day in 1990. A devotee of the 2600 circle and stalwart of the New York hackers' group "Masters of Deception," Phiber Optik was a splendid exemplar of the computer intruder as committed dissident. The eighteen-year-old Optik, a high-school dropout and part-time computer repairman, was young, smart, and ruthlessly obsessive, a sharp-dressing, sharp-talking digital dude who was utterly and airily contemptuous of anyone's rules but his own. By late 1991, Phiber Optik had appeared in Harper's, Esquire, The New York Times, in countless public debates and conventions, even on a television show hosted by Geraldo Rivera.

Treated with gingerly respect by Barlow and other Well mavens, Phiber Optik swiftly became a Well celebrity. Strangely, despite his thorny attitude and utter single-mindedness, Phiber Optik seemed to arouse strong protective instincts in most of the people who met him. He was great copy for journalists, always fearlessly ready to swagger, and, better yet, to actually demonstrate some off-the-wall digital stunt. He was a born media darling.

Even cops seemed to recognize that there was something peculiarly unworldly and uncriminal about this particular troublemaker. He was so bold, so flagrant, so young, and so obviously doomed, that even those who strongly disapproved of his actions grew anxious for his welfare, and began to flutter about him as if he were an endangered seal pup.

In January 24, 1990 (nine days after the Martin Luther King Day Crash), Phiber Optik, Acid Phreak, and a third NYC scofflaw named Scorpion were raided by the Secret Service. Their computers went out the door, along with the usual blizzard of papers, notebooks, compact disks, answering machines, Sony Walkmans, etc. Both Acid Phreak and Phiber Optik were accused of having caused the Crash.

The mills of justice ground slowly. The case eventually fell into the hands of the New York State Police. Phiber had lost his machinery in the raid, but there were no charges filed against him for over a year. His predicament was extensively publicized on the Well, where it caused much resentment for police tactics. It's one thing to merely hear about a hacker raided or busted; it's another to see the police attacking someone you've come to know personally, and who has explained his motives at length. Through the Harper's debate on the Well, it had become clear to the Wellbeings that Phiber Optik was not in fact going to "hurt anything." In their own salad days, many Wellbeings had tasted tear-gas in pitched street-battles with police. They were inclined to indulgence for acts of civil disobedience.

Wellbeings were also startled to learn of the draconian thoroughness of a typical hacker search-and-seizure. It took no great stretch of imagination for them to envision themselves suffering much the same treatment.

As early as January 1990, sentiment on the Well had already begun to sour, and people had begun to grumble that "hackers" were getting a raw deal from the ham-handed powers-that-be. The resultant issue of Harper's magazine posed the question as to whether computer-intrusion was a "crime" at all. As Barlow put it later: "I've begun to wonder if we wouldn't also regard spelunkers as desperate criminals if AT&T owned all the caves."

In February 1991, more than a year after the raid on his home, Phiber Optik was finally arrested, and was charged with first-degree Computer Tampering and Computer Trespass, New York state offenses. He was also charged with a theft-of-service misdemeanor, involving a complex free-call scam to a 900 number. Phiber Optik pled guilty to the misdemeanor charge, and was sentenced to 35 hours of community service.

This passing harassment from the unfathomable world of straight people seemed to bother Optik himself little if at all. Deprived of his computer by the January search-and-seizure, he simply bought himself a portable computer so the cops could no longer monitor the phone where he lived with his Mom, and he went right on with his depredations, sometimes on live radio or in front of television cameras.

The crackdown raid may have done little to dissuade Phiber Optik, but its galling affect on the Wellbeings was profound. As 1990 rolled on, the slings and arrows mounted: the Knight Lightning raid, the Steve Jackson raid, the nation-

spanning Operation Sundevil. The rhetoric of law enforcement made it clear that there was, in fact, a concerted crackdown on hackers in progress.

The hackers of the Hackers Conference, the Wellbeings, and their ilk, did not really mind the occasional public misapprehension of "hacking"; if anything, this membrane of differentiation from straight society made the "computer community" feel different, smarter, better. They had never before been confronted, however, by a concerted vilification campaign.

Barlow's central role in the counter-struggle was one of the major anomalies of 1990. Journalists investigating the controversy often stumbled over the truth about Barlow, but they commonly dusted themselves off and hurried on as if nothing had happened. It was as if it were too much to believe that a 1960s freak from the Grateful Dead had taken on a federal law enforcement operation head-to-head and actually seemed to be winning!

Barlow had no easily detectable power-base for a political struggle of this kind. He had no formal legal or technical credentials. Barlow was, however, a computer networker of truly stellar brilliance. He had a poet's gift of concise, colorful phrasing. He also had a journalist's shrewdness, an off-the-wall, self-deprecating wit, and a phenomenal wealth of simple personal charm.

The kind of influence Barlow possessed is fairly common currency in literary, artistic, or musical circles. A gifted critic can wield great artistic influence simply through defining the temper of the times, by coining the catch-phrases and the terms of debate that become the common currency of the period. (And as it happened, Barlow was a part-time art critic, with a special fondness for the Western art of Frederic Remington.)

Barlow was the first commentator to adopt William Gibson's striking science-fictional term "cyberspace" as a synonym for the present-day nexus of computer and telecommunications networks. Barlow was insistent that cyberspace should be regarded as a qualitatively new world, a "frontier." According to Barlow, the world of electronic communications, now made visible through the computer screen, could no longer be usefully regarded as just a tangle of high-tech wiring. Instead, it had become a place, cyberspace, which demanded a new set of metaphors, a new set of rules and behaviors. The term, as Barlow employed it, struck a useful chord, and this concept of cyberspace was picked up by Time, Scientific American, computer police, hackers, and even Constitutional scholars. "Cyberspace" now seems likely to become a permanent fixture of the language.

Barlow was very striking in person: a tall, craggy-faced, bearded, deep-voiced Wyomingan in a dashing Western ensemble of jeans, jacket, cowboy boots, a knotted throat-kerchief and an ever-present Grateful Dead cloisonne lapel pin.

Armed with a modem, however, Barlow was truly in his element. Formal hierarchies were not Barlow's strong suit; he rarely missed a chance to belittle the "large organizations and their drones," with their uptight, institutional mindset. Barlow was very much of the free-spirit persuasion, deeply unimpressed by brass-hats and jacks-in-office. But when it came to the digital grapevine, Barlow was a cyberspace ad-hocrat par excellence.

There was not a mighty army of Barlows. There was only one Barlow, and he was a fairly anomolous individual. However, the situation only seemed to require a single Barlow. In fact, after 1990, many people must have concluded that a single Barlow was far more than they'd ever bargained for.

Barlow's querulous mini-essay about his encounter with the FBI struck a strong chord on the Well. A number of other free spirits on the fringes of Apple Computing had come under suspicion, and they liked it not one whit better than he did.

One of these was Mitchell Kapor, the co-inventor of the spreadsheet program "Lotus 1-2-3" and the founder of Lotus Development Corporation. Kapor had written-off the passing indignity of being fingerprinted down at his own local Boston FBI headquarters, but Barlow's post made the full national scope of the FBI's dragnet clear to Kapor. The issue now had Kapor's full attention. As the Secret Service swung into anti-hacker operation nationwide in 1990, Kapor watched every move with deep skepticism and growing alarm.

As it happened, Kapor had already met Barlow, who had interviewed Kapor for a California computer journal. Like most people who met Barlow, Kapor had been very taken with him. Now Kapor took it upon himself to drop in on Barlow for a heart-to-heart talk about the situation.

Kapor was a regular on the Well. Kapor had been a devotee of the Whole Earth Catalog since the beginning, and treasured a complete run of the magazine. And Kapor not only had a modem, but a private jet. In pursuit of the scattered high-tech investments of Kapor Enterprises Inc., his personal, multi-million dollar holding company, Kapor commonly crossed state lines with about as much thought as one might give to faxing a letter.

The Kapor-Barlow council of June 1990, in Pinedale, Wyoming, was the start of the Electronic Frontier Foundation. Barlow swiftly wrote a manifesto, "Crime and Puzzlement," which announced his, and Kapor's, intention to form a political organization to "raise and disburse funds for education, lobbying, and litigation in the areas relating to digital speech and the extension of the Constitution into Cyberspace."

Furthermore, proclaimed the manifesto, the foundation would "fund, conduct, and support legal efforts to demonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive, and unconstitutional."

"Crime and Puzzlement" was distributed far and wide through computer networking channels, and also printed in the Whole Earth Review. The sudden declaration of a coherent, politicized counter-strike from the ranks of hackerdom electrified the community. Steve Wozniak (perhaps a bit stung by the NuPrometheus scandal) swiftly offered to match any funds Kapor offered the Foundation.

John Gilmore, one of the pioneers of Sun Microsystems, immediately offered his own extensive financial and personal support. Gilmore, an ardent libertarian, was to prove an eloquent advocate of electronic privacy issues, especially freedom from governmental and corporate computer-assisted surveillance of private citizens.

A second meeting in San Francisco rounded up further allies: Stewart Brand of the Point Foundation, virtual-reality pioneers Jaron Lanier and Chuck Blanchard, network entrepreneur and venture capitalist Nat Goldhaber. At this dinner meeting, the activists settled on a formal title: the Electronic Frontier Foundation, Incorporated. Kapor became its president. A new EFF Conference was opened on the Point Foundation's Well, and the Well was declared "the home of the Electronic Frontier Foundation."

Press coverage was immediate and intense. Like their nineteenth-century spiritual ancestors, Alexander Graham Bell and Thomas Watson, the high-tech computer entrepreneurs of the 1970s and 1980s - people such as Wozniak, Jobs, Kapor, Gates, and H. Ross Perot, who had raised themselves by their bootstraps to dominate a glittering new industry - had always made very good copy.

But while the Wellbeings rejoiced, the press in general seemed nonplussed by the self-declared "civilizers of cyberspace." EFF's insistence that the war against "hackers" involved grave Constitutional civil liberties issues seemed somewhat farfetched, especially since none of EFF's organizers were lawyers or established politicians. The business press in particular found it easier to seize on the apparent core of the story - that high-tech entrepreneur Mitchell Kapor had established a "defense fund for hackers." Was EFF a genuinely important political development - or merely a clique of wealthy eccentrics, dabbling in matters better left to the proper authorities? The jury was still out.

But the stage was now set for open confrontation. And the first and the most critical battle was the hacker show-trial of "Knight Lightning."

-Section 2-

It has been my practice throughout this book to refer to hackers only by their "handles." There is little to gain by giving the real names of these people, many of whom are juveniles, many of whom have never been convicted of any crime, and many of whom had unsuspecting parents who have already suffered enough.

But the trial of Knight Lightning on July 24-27, 1990, made this particular "hacker" a nationally known public figure. It can do no particular harm to himself or his family if I repeat the long-established fact that his name is Craig Neidorf (pronounced NYE-dorf).

Neidorf's jury trial took place in the United States District Court, Northern District of Illinois, Eastern Division, with the Honorable Nicholas J. Bua presiding. The United States of America was the plaintiff, the defendant Mr. Neidorf. The defendant's attorney was Sheldon T. Zenner of the Chicago firm of Katten, Muchin and Zavis.

The prosecution was led by the stalwarts of the Chicago Computer Fraud and Abuse Task Force: William J. Cook, Colleen D. Coughlin, and David A. Glockner, all Assistant United States Attorneys. The Secret Service Case Agent was Timothy M. Foley.

It will be recalled that Neidorf was the co-editor of an underground hacker "magazine" called Phrack. Phrack was an entirely electronic publication, distributed through bulletin boards and over electronic networks. It was amateur publication given away for free. Neidorf had never made any money for his work in Phrack. Neither had his unindicted co-editor "Taran King" or any of the numerous Phrack contributors.

The Chicago Computer Fraud and Abuse Task Force, however, had decided to prosecute Neidorf as a fraudster. To formally admit that Phrack was a "magazine" and Neidorf a "publisher" was to open a prosecutorial Pandora's Box of First Amendment issues. To do this was to play into the hands of Zenner and his EFF advisers, which now included a phalanx of prominent New York civil rights lawyers as well as the formidable legal staff of Katten, Muchin and Zavis. Instead, the prosecution relied heavily on the issue of access device fraud: Section 1029 of Title 18, the section from which the Secret Service drew its most direct jurisdiction over computer crime.

Neidorf's alleged crimes centered around the E911 Document. He was accused of having entered into a fraudulent scheme with the Prophet, who, it will be recalled, was the Atlanta LoD member who had illicitly copied the E911 Document from the BellSouth AIMSX system.

The Prophet himself was also a co-defendant in the Neidorf case, part-and-parcel of the alleged "fraud scheme" to "steal" BellSouth's E911 Document (and to pass the Document across state lines, which helped establish the Neidorf trial as a federal case). The Prophet, in the spirit of full co-operation, had agreed to testify against Neidorf.

In fact, all three of the Atlanta crew stood ready to testify against Neidorf. Their own federal prosecutors in Atlanta had charged the Atlanta Three with: (a) conspiracy, (b) computer fraud, © wire fraud, (d) access device fraud, and (e) interstate transportation of stolen property (Title 18, Sections 371, 1030, 1343, 1029, and 2314).

Faced with this blizzard of trouble, Prophet and Leftist had ducked any public trial and had pled guilty to reduced charges - one conspiracy count apiece. Urvile had pled guilty to that odd bit of Section 1029 which makes it illegal to possess "fifteen or more" illegal access devices (in his case, computer passwords). And their sentences were scheduled for September 14, 1990 - well after the Neidorf trial. As witnesses, they could presumably be relied upon to behave.

Neidorf, however, was pleading innocent. Most everyone else caught up in the crackdown had "cooperated fully" and pled guilty in hope of reduced sentences. (Steve Jackson was a notable exception, of course, and had strongly protested his innocence from the very beginning. But Steve Jackson could not get a day in court - Steve Jackson had never been charged with any crime in the first place.)

Neidorf had been urged to plead guilty. But Neidorf was a political science major and was disinclined to go to jail for "fraud" when he had not made any money, had not broken into any computer, and had been publishing a magazine that he considered protected under the First Amendment.

Neidorf's trial was the only legal action of the entire Crackdown that actually involved bringing the issues at hand out for a public test in front of a jury of American citizens.

Neidorf, too, had cooperated with investigators. He had voluntarily handed over much of the evidence that had led to his own indictment. He had already admitted in writing that he knew that the E911 Document had been stolen before he had "published" it in Phrack - or, from the prosecution's point of view, illegally transported stolen property by wire in something purporting to be a "publication."

But even if the "publication" of the E911 Document was not held to be a crime, that wouldn't let Neidorf off the hook. Neidorf had still received the E911 Document when Prophet had transferred it to him from Rich Andrews' Jolnet node. On that occasion, it certainly hadn't been "published" - it was hacker booty, pure and simple, transported across state lines.

The Chicago Task Force led a Chicago grand jury to indict Neidorf on a set of charges that could have put him in jail for thirty years. When some of these charges were successfully challenged before Neidorf actually went to trial, the Chicago Task Force rearranged his indictment so that he faced a possible jail term of over sixty years! As a first offender, it was very unlikely that Neidorf would in fact receive a sentence so drastic; but the Chicago Task Force clearly intended to see Neidorf put in prison, and his conspiratorial "magazine" put permanently out of commission. This was a federal case, and Neidorf was charged with the fraudulent theft of property worth almost eighty thousand dollars.

William Cook was a strong believer in high-profile prosecutions with symbolic overtones. He often published articles on his work in the security trade press, arguing that "a clear message had to be sent to the public at large and the computer community in particular that unauthorized attacks on computers and the theft of computerized information would not be tolerated by the courts."

The issues were complex, the prosecution's tactics somewhat unorthodox, but the Chicago Task Force had proved sure-footed to date. "Shadowhawk" had been bagged on the wing in 1989 by the Task Force, and sentenced to nine months in prison, and a $10,000 fine. The Shadowhawk case involved charges under Section 1030, the "federal interest computer" section.

Shadowhawk had not in fact been a devotee of "federal interest" computers per se. On the contrary, Shadowhawk, who owned an AT&T home computer, seemed to cherish a special aggression toward AT&T. He had bragged on the underground boards "Phreak Klass 2600" and "Dr. Ripco" of his skills at raiding AT&T, and of his intention to crash AT&T's national phone system. Shadowhawk's brags were noticed by Henry Kluepfel of Bellcore Security, scourge of the outlaw boards, whose relations with the Chicago Task Force were long and intimate.

The Task Force successfully established that Section 1030 applied to the teenage Shadowhawk, despite the objections of his defense attorney. Shadowhawk had entered a computer "owned" by U.S. Missile Command and merely "managed" by AT&T. He had also entered an AT&T computer located at Robbins Air Force Base in Georgia. Attacking AT&T was of "federal interest" whether Shadowhawk had intended it or not.

The Task Force also convinced the court that a piece of AT&T software that Shadowhawk had illicitly copied from Bell Labs, the "Artificial Intelligence C5 Expert System," was worth a cool one million dollars. Shadowhawk's attorney had argued that Shadowhawk had not sold the program and had made no profit from the illicit copying. And in point of fact, the C5 Expert System was experimental software, and had no established market value because it had never been on the market in the first place. AT&T's own assessment of a "one million dollar" figure for its own intangible property was accepted without challenge by the court, however. And the court concurred with the government prosecutors that Shadowhawk showed clear "intent to defraud" whether he'd gotten any money or not. Shadowhawk went to jail.

The Task Force's other best-known triumph had been the conviction and jailing of "Kyrie." Kyrie, a true denizen of the digital criminal underground, was a 36-year-old Canadian woman, convicted and jailed for telecommunications fraud in Canada. After her release from prison, she had fled the wrath of Canada Bell and the Royal Canadian Mounted Police, and eventually settled, very unwisely, in Chicago.

"Kyrie," who also called herself "Long Distance Information," specialized in voice-mail abuse. She assembled large numbers of hot long-distance codes, then read them aloud into a series of corporate voice-mail systems. Kyrie and her friends were electronic squatters in corporate voice-mail systems, using them much as if they were pirate bulletin boards, then moving on when their vocal chatter clogged the system and the owners necessarily wised up. Kyrie's camp followers were a loose tribe of some hundred and fifty phone-phreaks, who followed her trail of piracy from machine to machine, ardently begging for her services and expertise.

Kyrie's disciples passed her stolen credit card numbers, in exchange for her stolen "long distance information." Some of Kyrie's clients paid her off in cash, by scamming credit card cash advances from Western Union.

Kyrie travelled incessantly, mostly through airline tickets and hotel rooms that she scammed through stolen credit cards. Tiring of this, she found refuge with a fellow female phone phreak in Chicago. Kyrie's hostess, like a surprising number of phone phreaks, was blind. She was also physically disabled. Kyrie allegedly made the best of her new situation by applying for, and receiving, state welfare funds under a false identity as a qualified caretaker for the handicapped.

Sadly, Kyrie's two children by a former marriage had also vanished underground with her; these pre-teen digital refugees had no legal American identity, and had never spent a day in school.

Kyrie was addicted to technical mastery and enthralled by her own cleverness and the ardent worship of her teenage followers. This foolishly led her to phone up Gail Thackeray in Arizona, to boast, brag, strut, and offer to play informant. Thackeray, however, had already learned far more than enough about Kyrie, whom she roundly despised as an adult criminal corrupting minors, a "female Fagin." Thackeray passed her tapes of Kyrie's boasts to the Secret Service.

Kyrie was raided and arrested in Chicago in May 1989. She confessed at great length and pled guilty.

In August 1990, Cook and his Task Force colleague Colleen Coughlin sent Kyrie to jail for 27 months, for computer and telecommunications fraud. This was a markedly severe sentence by the usual wrist-slapping standards of "hacker" busts. Seven of Kyrie's foremost teenage disciples were also indicted and convicted. The Kyrie "high-tech street gang," as Cook described it, had been crushed. Cook and his colleagues had been the first ever to put someone in prison for voice-mail abuse. Their pioneering efforts had won them attention and kudos.

In his article on Kyrie, Cook drove the message home to the readers of Security Management magazine, a trade journal for corporate security professionals. The case, Cook said, and Kyrie's stiff sentence, "reflect a new reality for hackers and computer crime victims in the '90s… Individuals and corporations who report computer and telecommunications crimes can now expect that their cooperation with federal law enforcement will result in meaningful punishment. Companies and the public at large must report computer-enhanced crimes if they want prosecutors and the course to protect their rights to the tangible and intangible property developed and stored on computers."

Cook had made it his business to construct this "new reality for hackers." He'd also made it his business to police corporate property rights to the intangible.

Had the Electronic Frontier Foundation been a "hacker defense fund" as that term was generally understood, they presumably would have stood up for Kyrie. Her 1990 sentence did indeed send a "message" that federal heat was coming down on "hackers." But Kyrie found no defenders at EFF, or anywhere else, for that matter. EFF was not a bail-out fund for electronic crooks.

The Neidorf case paralleled the Shadowhawk case in certain ways. The victim once again was allowed to set the value of the "stolen" property. Once again Kluepfel was both investigator and technical advisor. Once again no money had changed hands, but the "intent to defraud" was central.

The prosecution's case showed signs of weakness early on. The Task Force had originally hoped to prove Neidorf the center of a nationwide Legion of Doom criminal conspiracy. The Phrack editors threw physical get-togethers every summer, which attracted hackers from across the country; generally two dozen or so of the magazine's favorite contributors and readers. (Such conventions were common in the hacker community; 2600 Magazine, for instance, held public meetings of hackers in New York, every month.) LoD heavy-dudes were always a strong presence at these Phrack-sponsored "Summercons."

In July 1988, an Arizona hacker named "Dictator" attended Summercon in Neidorf's home town of St. Louis. Dictator was one of Gail Thackeray's underground informants; Dictator's underground board in Phoenix was a sting operation for the Secret Service. Dictator brought an undercover crew of Secret Service agents to Summercon. The agents bored spyholes through the wall of Dictator's hotel room

in St Louis, and videotaped the frolicking hackers through a one-way mirror. As it happened, however, nothing illegal had occurred on videotape, other than the guzzling of beer by a couple of minors. Summercons were social events, not sinister cabals. The tapes showed fifteen hours of raucous laughter, pizza-gobbling, in-jokes and back-slapping.

Neidorf's lawyer, Sheldon Zenner, saw the Secret Service tapes before the trial. Zenner was shocked by the complete harmlessness of this meeting, which Cook had earlier characterized as a sinister interstate conspiracy to commit fraud. Zenner wanted to show the Summercon tapes to the jury. It took protracted maneuverings by the Task Force to keep the tapes from the jury as "irrelevant."

The E911 Document was also proving a weak reed. It had originally been valued at $79,449. Unlike Shadowhawk's arcane Artificial Intelligence booty, the E911 Document was not software - it was written in English. Computer-knowledgeable people found this value - for a twelve-page bureaucratic document - frankly incredible. In his "Crime and Puzzlement" manifesto for EFF, Barlow commented: "We will probably never know how this figure was reached or by whom, though I like to imagine an appraisal team consisting of Franz Kafka, Joseph Heller, and Thomas Pynchon."

As it happened, Barlow was unduly pessimistic. The EFF did, in fact, eventually discover exactly how this figure was reached, and by whom - but only in 1991, long after the Neidorf trial was over.

Kim Megahee, a Southern Bell security manager, had arrived at the document's value by simply adding up the "costs associated with the production" of the E911 Document. Those "costs" were as follows:

1. A technical writer had been hired to research and write the E911 Document. 200 hours of work, at $35 an hour, cost : $7,000. A Project Manager had overseen the technical writer. 200 hours, at $31 an hour, made: $6,200.
2. A week of typing had cost $721 dollars. A week of formatting had cost $721. A week of graphics formatting had cost $742.
3. Two days of editing cost $367.
4. A box of order labels cost five dollars.
5. Preparing a purchase order for the Document, including typing and the obtaining of an authorizing signature from within the BellSouth bureaucracy, cost $129.
6. Printing cost $313. Mailing the Document to fifty people took fifty hours by a clerk, and cost $858.
7. Placing the Document in an index took two clerks an hour each, totalling $43.

Bureaucratic overhead alone, therefore, was alleged to have cost a whopping $17,099. According to Mr. Megahee, the typing of a twelve-page document had taken a full week. Writing it had taken five weeks, including an overseer who apparently did nothing else but watch the author for five weeks. Editing twelve pages had taken two days. Printing and mailing an electronic document (which was already available on the Southern Bell Data Network to any telco employee who needed it), had cost over a thousand dollars.

But this was just the beginning. There were also the hardware expenses. Eight hundred fifty dollars for a VT220 computer monitor. Thirty-one thousand dollars for a sophisticated VAXstation II computer. Six thousand dollars for a computer printer. Twenty-two thousand dollars for a copy of "Interleaf" software. Two thousand five hundred dollars for VMS software. All this to create the twelve-page Document.

Plus ten percent of the cost of the software and the hardware, for maintenance. (Actually, the ten percent maintenance costs, though mentioned, had been left off the final $79,449 total, apparently through a merciful oversight).

Mr. Megahee's letter had been mailed directly to William Cook himself, at the office of the Chicago federal attorneys. The United States Government accepted these telco figures without question.

As incredulity mounted, the value of the E911 Document was officially revised downward. This time, Robert Kibler of BellSouth Security estimated the value of the twelve pages as a mere $24,639.05 - based, purportedly, on "R&D costs." But this specific estimate, right down to the nickel, did not move the skeptics at all; in fact it provoked open scorn and a torrent of sarcasm.

The financial issues concerning theft of proprietary information have always been peculiar. It could be argued that BellSouth had not "lost" its E911 Docu-

ment at all in the first place, and therefore had not suffered any monetary damage from this "theft." And Sheldon Zenner did in fact argue this at Neidorf's trial - that Prophet's raid had not been "theft," but was better understood as illicit copying.

The money, however, was not central to anyone's true purposes in this trial. It was not Cook's strategy to convince the jury that the E911 Document was a major act of theft and should be punished for that reason alone. His strategy was to argue that the E911 Document was dangerous. It was his intention to establish that the E911 Document was "a road-map" to the Enhanced 911 System. Neidorf had deliberately and recklessly distributed a dangerous weapon. Neidorf and the Prophet did not care (or perhaps even gloated at the sinister idea) that the E911 Document could be used by hackers to disrupt 911 service, "a life line for every person certainly in the Southern Bell region of the United States, and indeed, in many communities throughout the United States," in Cook's own words. Neidorf had put people's lives in danger.

In pre-trial maneuverings, Cook had established that the E911 Document was too hot to appear in the public proceedings of the Neidorf trial. The jury itself would not be allowed to ever see this Document, lest it slip into the official court records, and thus into the hands of the general public, and, thus, somehow, to malicious hackers who might lethally abuse it.

Hiding the E911 Document from the jury may have been a clever legal maneuver, but it had a severe flaw. There were, in point of fact, hundreds, perhaps thousands, of people, already in possession of the E911 Document, just as Phrack had published it. Its true nature was already obvious to a wide section of the interested public (all of whom, by the way, were, at least theoretically, party to a gigantic wire-fraud conspiracy). Most everyone in the electronic community who had a modem and any interest in the Neidorf case already had a copy of the Document. It had already been available in Phrack for over a year.

People, even quite normal people without any particular prurient interest in forbidden knowledge, did not shut their eyes in terror at the thought of beholding a "dangerous" document from a telephone company. On the contrary, they tended to trust their own judgement and simply read the Document for themselves. And they were not impressed.

One such person was John Nagle. Nagle was a forty-one-year-old professional programmer with a masters' degree in computer science from Stanford. He had worked for Ford Aerospace, where he had invented a computer-networking technique known as the "Nagle Algorithm," and for the prominent Californian computer-graphics firm "Autodesk," where he was a major stockholder.

Nagle was also a prominent figure on the Well, much respected for his technical knowledgeability.

Nagle had followed the civil-liberties debate closely, for he was an ardent telecommunicator. He was no particular friend of computer intruders, but he believed electronic publishing had a great deal to offer society at large, and attempts to restrain its growth, or to censor free electronic expression, strongly roused his ire.

The Neidorf case, and the E911 Document, were both being discussed in detail on the Internet, in an electronic publication called Telecom Digest. Nagle, a longtime Internet maven, was a regular reader of Telecom Digest. Nagle had never seen a copy of Phrack, but the implications of the case disturbed him.

While in a Stanford bookstore hunting books on robotics, Nagle happened across a book called The Intelligent Network. Thumbing through it at random, Nagle came across an entire chapter meticulously detailing the workings of E911 police emergency systems. This extensive text was being sold openly, and yet in Illinois a young man was in danger of going to prison for publishing a thin six-page document about 911 service.

Nagle made an ironic comment to this effect in Telecom Digest. From there, Nagle was put in touch with Mitch Kapor, and then with Neidorf's lawyers.

Sheldon Zenner was delighted to find a computer telecommunications expert willing to speak up for Neidorf, one who was not a wacky teenage "hacker." Nagle was fluent, mature, and respectable; he'd once had a federal security clearance.

Nagle was asked to fly to Illinois to join the defense team.

Having joined the defense as an expert witness, Nagle read the entire E911 Document for himself. He made his own judgement about its potential for menace.

The time has now come for you yourself, the reader, to have a look at the E911 Document. This six-page piece of work was the pretext for a federal prosecution that could have sent an electronic publisher to prison for thirty, or even sixty, years. It was the pretext for the search and seizure of Steve Jackson Games, a legitimate publisher of printed books. It was also the formal pretext for the search and seizure of the Mentor's bulletin board, "Phoenix Project," and for the raid on the home of Erik Bloodaxe. It also had much to do with the seizure of Richard Andrews' Jolnet node and the shutdown of Charles Boykin's AT&T node. The E911 Document was the single most important piece of evidence in the Hacker Crackdown. There can be no real and legitimate substitute for the Document itself.

Phrack Inc.

Volume Two, Issue 24, File 5 of 13.

Control Office Administration Of Enhanced 911 Services For Special Services and Account Centers.

by the Eavesdropper

March, 1988

Description of Service

The control office for Emergency 911 service is assigned in accordance with the existing standard guidelines to one of the following centers:

- Special Services Center (SSC)
- Major Accounts Center (MAC)
- Serving Test Center (STC)
- Toll Control Center (TCC)

The SSC/MAC designation is used in this document interchangeably for any of these four centers. The Special Services Centers (SSCs) or Major Account Centers (MACs) have been designated as the trouble reporting contact for all E911 customer (PSAP) reported troubles. Subscribers who have trouble on an E911 call will continue to contact local repair service (CRSAB) who will refer the trouble to the SSC/MAC, when appropriate.

Due to the critical nature of E911 service, the control and timely repair of troubles is demanded. As the primary E911 customer contact, the SSC/MAC is in the unique position to monitor the status of the trouble and insure its resolution.

System Overview

The number 911 is intended as a nationwide universal telephone number which provides the public with direct access to a Public Safety Answering Point (PSAP). A PSAP is also referred to as an Emergency Service Bureau (ESB). A PSAP is an agency or facility which is authorized by a municipality to receive and respond to police, fire and/or ambulance services. One or more attendants are located at the PSAP facilities to receive and handle calls of an emergency nature in accordance with the local municipal requirements.

An important advantage of E911 emergency service is improved (reduced) response times for emergency services. Also close coordination among agencies providing various emergency services is a valuable capability provided by E911 service.

1A ESS is used as the tandem office for the E911 network to route all 911 calls to the correct (primary) PSAP designated to serve the calling station. The E911 feature was developed primarily to provide routing to the correct PSAP for all 911 calls. Selective routing allows a 911 call originated from a particular station located in a particular district, zone, or town, to be routed to the primary PSAP designated to serve that customer station regardless of wire center boundaries. Thus, selective routing eliminates the problem of wire center boundaries not coinciding with district or other political boundaries.

The services available with the E911 feature include:

- Forced Disconnect Default Routing
- Alternative Routing Night Service
- Selective Routing Automatic Number
- Identification (ANI)
- Selective Transfer Automatic Location
- Identification (ALI)

Preservice/Installation Guidelines

When a contract for an E911 system has been signed, it is the responsibility of Network Marketing to establish an implementation/cutover committee which should include a representative from the SSC/MAC. Duties of the E911 Implementation Team include coordination of all phases of the E911 system deployment and the formation of an on-going E911 maintenance subcommittee.

Marketing is responsible for providing the following customer specific information to the SSC/MAC prior to the start of call through testing:

- All PSAP's (name, address, local contact)
- All PSAP circuit ID's
- 1004 911 service request including PSAP details on each PSAP (1004 Section K, L, M)
- Network configuration
- Any vendor information (name, telephone number, equipment)

The SSC/MAC needs to know if the equipment and sets at the PSAP are maintained by the BOCs, an independent company, or an outside vendor, or any combination. This information is then entered on the PSAP profile sheets and reviewed quarterly for changes, additions and deletions.

Marketing will secure the Major Account Number (MAN) and provide this number to Corporate Communications so that the initial issue of the service orders carry the MAN and can be tracked by the SSC/MAC via CORDNET. PSAP circuits are official services by definition.

All service orders required for the installation of the E911 system should include the MAN assigned to the city/county which has purchased the system.

In accordance with the basic SSC/MAC strategy for provisioning, the SSC/MAC will be Overall Control Office (OCO) for all Node to PSAP circuits (official services) and any other ser-

vices for this customer. Training must be scheduled for all SSC/MAC involved personnel during the pre-service stage of the project.
The E911 Implementation Team will form the on-going maintenance subcommittee prior to the initial implementation of the E911 system. This sub-committee will establish post implementation quality assurance procedures to ensure that the E911 system continues to provide quality service to the customer. Customer/Company training, trouble reporting interfaces for the customer, telephone company and any involved independent telephone companies needs to be addressed and implemented prior to E911 cutover. These functions can be best addressed by the formation of a sub-committee of the E911 Implementation Team to set up guidelines for and to secure service commitments of interfacing organizations. A SSC/MAC supervisor should chair this subcommittee and include the following organizations:

1. Switching Control Center - E911 translations - Trunking - End office and Tandem office hardware/software
2. Recent Change Memory Administration Center - Daily RC update activity for TN/ESN translations - Processes validity errors and rejects
3. Line and Number Administration - Verification of TN/ESN translations
4. Special Service Center/Major Account Center - Single point of contact for all PSAP and Node to host troubles - Logs, tracks & statusing of all trouble reports - Trouble referral, follow up, and escalation - Customer notification of status and restoration - Analyzation of ``chronic" troubles - Testing, installation and maintenance of E911 circuits
5. Installation and Maintenance (SSIM/I&M.) - Repair and maintenance of PSAP equipment and Telco owned sets
6. Minicomputer Maintenance Operations Center - E911 circuit maintenance (where applicable)
7. Area Maintenance Engineer - Technical assistance on voice (CO-PSAP. network) related E911 troubles

Maintenance Guidelines

The CCNC will test the Node circuit from the 202T at the Host site to the 202T at the Node site. Since Host to Node (CCNC to MMOC) circuits are official company services, the CCNC will refer all Node circuit troubles to the SSC/MAC. The SSC/MAC is responsible for the testing and follow up to restoration of these circuit troubles.
Although Node to PSAP circuit are official services, the MMOC will refer PSAP circuit troubles to the appropriate SSC/MAC. The SSC/MAC is responsible for testing and follow up to restoration of PSAP circuit troubles.
The SSC/MAC will also receive reports from CRSAB/IMC(s) on subscriber 911 troubles when they are not line troubles. The SSC/MAC is responsible for testing and restoration of these troubles.

Maintenance responsibilities are as follows:

SCC* Voice Network (ANI to PSAP)
*SCC responsible for tandem switch
SSIM/I&M PSAP Equipment (Modems, CIU's, sets)
VendorPSAP Equipment (when CPE)
SSC/MAC PSAP to Node circuits, and tandem to PSAP voice circuits (EMNT)
MMOC Node site (Modems, cables, etc)
Note: All above work groups are required to resolve troubles by interfacing with appropriate work groups for resolution.

The Switching Control Center (SCC) is responsible for E911/1AESS translations in tandem central offices. These translations route E911 calls, selective transfer, default routing, speed calling, etc., for each PSAP. The SCC is also responsible for troubleshooting on the voice network (call originating to end office tandem equipment).
For example, ANI failures in the originating offices would be a responsibility of the SCC.
Recent Change Memory Administration Center (RCMAC) performs the daily tandem translation updates (recent change) for routing of individual telephone numbers.
Recent changes are generated from service order activity (new service, address changes, etc.) and compiled into a daily file by the E911 Center (ALI/DMS E911 Computer).
SSIM/I&M is responsible for the installation and repair of PSAP equipment. PSAP equipment includes ANI Controller, ALI Controller, data sets, cables, sets, and other peripheral equipment that is not vendor owned. SSIM/I&M is responsible for establishing maintenance test kits, complete with spare parts for PSAP maintenance. This includes test gear, data sets, and ANI/ALI Controller parts.
Special Services Center (SSC) or Major Account Center (MAC) serves as the trouble reporting contact for all (PSAP) troubles reported by customer. The SSC/MAC refers troubles to proper organizations for handling and tracks status of troubles, escalating when necessary. The SSC/MAC will close out troubles with customer. The SSC/MAC will analyze all troubles and tracks ``chronic" PSAP troubles. Corporate Communications Network Center (CCNC) will test and refer troubles on all node to host circuits. All E911 circuits are classified as official company property.
The Minicomputer Maintenance Operations Center (MMOC) maintains the E911 (ALI/DMS) computer hardware at the Host site. This MMOC is also responsible for monitoring the system and reporting certain PSAP and system problems to the local MMOC's, SCC's or SSC/MAC's. The MMOC personnel also operate software programs that maintain the TN data base under the direction of the E911 Center. The maintenance of the NODE computer (the interface between the PSAP and the ALI/DMS computer) is a function of the MMOC at the NODE site. The MMOC's at the NODE sites may also be involved in the testing of NODE to Host circuits. The MMOC will also assist on Host to PSAP and data network related troubles not resolved through standard trouble clearing procedures.
Installation And Maintenance Center (IMC) is responsible for referral of E911 subscriber troubles that are not subscriber line problems.
E911 Center - Performs the role of System Administration and is responsible for overall operation of the E911 computer software. The E911 Center does A-Z trouble analysis and provides statistical information on the performance of the system.
This analysis includes processing PSAP inquiries (trouble reports) and referral of network troubles. The E911 Center also performs daily processing of tandem recent change and provides information to the RCMAC for tandem input. The E911 Center is responsible for daily processing of the ALI/DMS computer data base and provides error files, etc. to the Customer Services department for investigation and correction. The E911 Center participates in all system implementations and on-going maintenance effort and assists in the development of procedures, training and education of information to all groups.

Any group receiving a 911 trouble from the SSC/MAC should close out the trouble with the SSC/MAC or provide a status if the trouble has been referred to another group. This will allow the SSC/MAC to provide a status back to the customer or escalate as appropriate.
Any group receiving a trouble from the Host site (MMOC or CCNC) should close the trouble back to that group.
The MMOC should notify the appropriate SSC/MAC when the Host, Node, or all Node circuits are down so that the SSC/MAC can reply to customer reports that may be called in by the PSAPs. This will eliminate duplicate reporting of troubles. On complete outages the MMOC will follow escalation procedures for a Node after two (2) hours and for a PSAP after four (4) hours. Additionally the MMOC will notify the appropriate SSC/MAC when the Host, Node, or all Node circuits are down.
The PSAP will call the SSC/MAC to report E911 troubles. The person reporting the E911 trouble may not have a circuit I.D. and will therefore report the PSAP name and address. Many PSAP troubles are not circuit specific. In those instances where the caller cannot provide a circuit I.D., the SSC/MAC will be required to determine the circuit I.D. using the PSAP profile. Under no circumstances will the SSC/MAC Center refuse to take the trouble. The E911 trouble should be handled as quickly as possible, with the SSC/MAC providing as much assistance as possible while taking the trouble report from the caller.
The SSC/MAC will screen/test the trouble to determine the appropriate handoff organization based on the following criteria:
PSAP equipment problem: SSIM/I&M Circuit problem: SSC/MAC Voice network problem: SCC (report trunk group number) Problem affecting multiple PSAPs (No ALI report from all PSAPs): Contact the MMOC to check for NODE or Host computer problems before further testing.
The SSC/MAC will track the status of reported troubles and escalate as appropriate. The SSC/MAC will close out customer/company reports with the initiating contact. Groups with specific maintenance responsibilities, defined above, will investigate ``chronic'' troubles upon request from the SSC/MAC and the ongoing maintenance subcommittee.
All ``out of service'' E911 troubles are priority one type reports. One link down to a PSAP is considered a priority one trouble and should be handled as if the PSAP was isolated.
The PSAP will report troubles with the ANI controller, ALI controller or set equipment to the SSC/MAC.
NO ANI: Where the PSAP reports NO ANI (digital display screen is blank) ask if this condition exists on all screens and on all calls. It is important to differentiate between blank screens and screens displaying 911-00XX, or all zeroes.
When the PSAP reports all screens on all calls, ask if there is any voice contact with callers. If there is no voice contact the trouble should be referred to the SCC immediately since 911 calls are not getting through which may require alternate routing of calls to another PSAP.
When the PSAP reports this condition on all screens but not all calls and has voice contact with callers, the report should be referred to SSIM/I&M for dispatch. The SSC/MAC should verify with the SCC that ANI is pulsing before dispatching SSIM.
When the PSAP reports this condition on one screen for all calls (others work fine) the trouble should be referred to SSIM/I&M for dispatch, because the trouble is isolated to one piece of equipment at the customer premise.
An ANI failure (i.e. all zeroes) indicates that the ANI has not been received by the PSAP from the tandem office or was lost by the PSAP ANI controller. The PSAP may receive ``02'' alarms which can be caused by the ANI controller logging more than three all zero failures on the same trunk. The PSAP has been instructed to report this condition to the SSC/MAC since it could indicate an equipment trouble at the PSAP which might be affecting all subscribers calling into the PSAP. When all zeroes are being received on all calls or "02" alarms continue, a tester should analyze the condition to determine the appropriate action to be taken. The tester must perform cooperative testing with the SCC when there appears to be a problem on the Tandem-PSAP trunks before requesting dispatch.
When an occasional all zero condition is reported, the SSC/MAC should dispatch SSIM/I&M to routine equipment on a ``chronic'' trouble-sweep.
The PSAPs are instructed to report incidental ANI failures to the BOC on a PSAP inquiry trouble ticket (paper) that is sent to the Customer Services E911 group and forwarded to E911 center when required. This usually involves only a particular telephone number and is not a condition that would require a report to the SSC/MAC. Multiple ANI failures which our from the same end office (XX denotes end office), indicate a hard trouble condition may exist in the end office or end office tandem trunks. The PSAP will report this type of condition to the SSC/MAC and the SSC/MAC should refer the report to the SCC responsible for the tandem office. NOTE: XX is the ESCO (Emergency Service Number) associated with the incoming 911 trunks into the tandem. It is important that the C/MAC tell the SCC what is displayed at the PSAP (i.e. 911-0011) which indicates to the SCC which end office is in trouble.
Note: It is essential that the PSAP fill out inquiry form on every ANI failure.
The PSAP will report a trouble any time an address is not received on an address display (screen blank) E911 call. (If a record is not in the 911 data base or an ANI failure is encountered, the screen will provide a display noticing such condition). The SSC/MAC should verify with the PSAP whether the NO ALI condition is on one screen or all screens.
When the condition is on one screen (other screens receive ALI information) the SSC/MAC will request SSIM/I&M to dispatch.
If no screens are receiving ALI information, there is usually a circuit trouble between the PSAP and the Host computer. The SSC/MAC should test the trouble and refer for restoral.
Note: If the SSC/MAC receives calls from multiple PSAP's, all of which are receiving NO ALI, there is a problem with the Node or Node to Host circuits or the Host computer itself. Before referring the trouble the SSC/MAC should call the MMOC to inquire if the Node or Host is in trouble.
Alarm conditions on the ANI controller digital display at the PSAP are to be reported by the PSAP's. These alarms can indicate various trouble conditions so the SSC/MAC should ask the PSAP if any portion of the E911 system is not functioning properly.
The SSC/MAC should verify with the PSAP attendant that the equipment's primary function is answering E911 calls. If it is, the SSC/MAC should request a dispatch SSIM/I&M. If the equipment is not primarily used for E911, then

the SSC/MAC should advise PSAP to contact their CPE vendor.
Note: These troubles can be quite confusing when the PSAP has vendor equipment mixed in with equipment that the BOC maintains. The Marketing representative should provide the SSC/MAC information concerning any unusual or exception items where the PSAP should contact their vendor. This information should be included in the PSAP profile sheets.
ANI or ALI controller down: When the host computer sees the PSAP equipment down and it does not come back up, the MMOC will report the trouble to the SSC/MAC; the equipment is down at the PSAP, a dispatch will be required.
PSAP link (circuit) down: The MMOC will provide the SSC/MAC with the circuit ID that the Host computer indicates in trouble. Although each PSAP has two circuits, when either circuit is down the condition must be treated as an emergency since failure of the second circuit will cause the PSAP to be isolated.
Any problems that the MMOC identifies from the Node location to the Host computer will be handled directly with the appropriate MMOC(s)/CCNC.
Note: The customer will call only when a problem is apparent to the PSAP. When only one circuit is down to the PSAP, the customer may not be aware there is a trouble, even though there is one link down, notification should appear on the PSAP screen. Troubles called into the SSC/MAC from the MMOC or other company employee should not be closed out by calling the PSAP since it may result in the customer responding that they do not have a trouble. These reports can only be closed out by receiving information that the trouble was fixed and by checking with the company employee that reported the trouble. The MMOC personnel will be able to verify that the trouble has cleared by reviewing a printout from the host.
When the CRSAB receives a subscriber complaint (i.e., cannot dial 911) the RSA should obtain as much information as possible while the customer is on the line.
For example, what happened when the subscriber dialed 911? The report is automatically directed to the IMC for subscriber line testing. When no line trouble is found, the IMC will refer the trouble condition to the SSC/MAC. The SSC/MAC will contact Customer Services E911 Group and verify that the subscriber should be able to call 911 and obtain the ESN. The SSC/MAC will verify the ESN via 2SCCS. When both verifications match, the SSC/MAC will refer the report to the SCC responsible for the 911 tandem office for investigation and resolution. The MAC is responsible for tracking the trouble and informing the IMC when it is resolved.

For more information, please refer to E911 Glossary of Terms.

End of Phrack File

The reader is forgiven if he or she was entirely unable to read this document. John Perry Barlow had a great deal of fun at its expense, in "Crime and Puzzlement:" "Bureaucratese of surpassing opacity… To read the whole thing straight through without entering coma requires either a machine or a human who has too much practice thinking like one. Anyone who can understand it fully and fluidly had altered his consciousness beyone the ability to ever again read Blake, Whitman, or Tolstoy… the document contains little of interest to anyone who is not a student of advanced organizational sclerosis."

With the Document itself to hand, however, exactly as it was published (in its six-page edited form) in Phrack, the reader may be able to verify a few statements of fact about its nature. First, there is no software, no computer code, in the Document. It is not computer-programming language like FORTRAN or C++, it is English; all the sentences have nouns and verbs and punctuation. It does not explain how to break into the E911 system. It does not suggest ways to destroy or damage the E911 system.

There are no access codes in the Document. There are no computer passwords. It does not explain how to steal long distance service. It does not explain how to break in to telco switching stations. There is nothing in it about using a personal computer or a modem for any purpose at all, good or bad.

Close study will reveal that this document is not about machinery. The E911 Document is about administration. It describes how one creates and administers certain units of telco bureaucracy: Special Service Centers and Major Account Centers (SSC/MAC). It describes how these centers should distribute responsibility for the E911 service, to other units of telco bureaucracy, in a chain of command, a formal hierarchy. It describes who answers customer complaints, who screens calls, who reports equipment failures, who answers those reports, who handles maintenance, who chairs subcommittees, who gives orders, who follows orders, who tells whom what to do. The Document is not a "roadmap" to computers. The Document is a roadmap to people.

As an aid to breaking into computer systems, the Document is useless. As an aid to harassing and deceiving telco people, however, the Document might prove handy (especially with its Glossary, which I have not included). An intense and protracted study of this Document and its Glossary, combined with many other such documents, might teach one to speak like a telco employee. And telco people live by speech - they live by phone communication. If you can mimic their language over the phone, you can "social-engineer" them. If you can con telco

people, you can wreak havoc among them. You can force them to no longer trust one another; you can break the telephonic ties that bind their community; you can make them paranoid. And people will fight harder to defend their community than they will fight to defend their individual selves.

This was the genuine, gut-level threat posed by Phrack magazine. The real struggle was over the control of telco language, the control of telco knowledge. It was a struggle to defend the social "membrane of differentiation" that forms the walls of the telco community's ivory tower - the special jargon that allows telco professionals to recognize one another, and to exclude charlatans, thieves, and upstarts. And the prosecution brought out this fact. They repeatedly made reference to the threat posed to telco professionals by hackers using "social engineering."

However, Craig Neidorf was not on trial for learning to speak like a professional telecommunications expert. Craig Neidorf was on trial for access device fraud and transportation of stolen property. He was on trial for stealing a document that was purportedly highly sensitive and purportedly worth tens of thousands of dollars.

Afterword: The Hacker Crackdown Three Years Later.

Three years in cyberspace is like thirty years anyplace real. It feels as if a generation has passed since I wrote this book. In terms of the generations of computing machinery involved, that's pretty much the case.

The basic shape of cyberspace has changed drastically since 1990. A new U.S. Administration is in power whose personnel are, if anything, only too aware of the nature and potential of electronic networks. It's now clear to all players concerned that the status quo is dead-and-gone in American media and telecommunications, and almost any territory on the electronic frontier is up for grabs. Interactive multimedia, cable-phone alliances, the Information Superhighway, fiber-to-the-curb, laptops and palmtops, the explosive growth of cellular and the Internet - the earth trembles visibly.

The year 1990 was not a pleasant one for AT&T. By 1993, however, AT&T had successfully devoured the computer company NCR in an unfriendly takeover, finally giving the pole-climbers a major piece of the digital action. AT&T managed to rid itself of ownership of the troublesome UNIX operating system, selling it to Novell, a netware company, which was itself preparing for a savage market dust-up with operating-system titan Microsoft. Furthermore, AT&T acquired McCaw Cellular in a gigantic merger, giving AT&T a potential wireless whip-hand over its former progeny, the RBOCs. The RBOCs themselves were now AT&T's clearest potential rivals, as the Chinese firewalls between regulated monopoly and frenzied digital entrepreneurism began to melt and collapse headlong.

AT&T, mocked by industry analysts in 1990, was reaping awestruck praise by commentators in 1993. AT&T had managed to avoid any more major software crashes in its switching stations. AT&T's newfound reputation as "the nimble giant" was all the sweeter, since AT&T's traditional rival giant in the world of multinational computing, IBM, was almost prostrate by 1993. IBM's vision of the commercial computer-network of the future, "Prodigy," had managed to spend $900 million without a whole heck of a lot to show for it, while AT&T, by contrast, was boldly speculating on the possibilities of personal communicators and hedging its bets with investments in handwritten interfaces. In 1990 AT&T had looked bad; but in 1993 AT&T looked like the future.

At least, AT&T's advertising looked like the future. Similar public attention was riveted on the massive $22 billion megamerger between RBOC Bell Atlantic and cable-TV giant Tele-Communications Inc. Nynex was buying into cable company Viacom International. BellSouth was buying stock in Prime Management, Southwestern Bell acquiring a cable company in Washington DC, and so forth. By stark contrast, the Internet, a noncommercial entity which officially did not even exist, had no advertising budget at all. And yet, almost below the level of governmental and corporate awareness, the Internet was stealthily devouring everything in its path, growing at a rate that defied comprehension. Kids who might have been eager computer-intruders a mere five years earlier were now surfing the Internet, where their natural urge to explore led them into cyberspace landscapes of such mindboggling vastness that the very idea of hacking passwords seemed rather a waste of time.

By 1993, there had not been a solid, knock 'em down, panic-striking, teenage-hacker computer-intrusion scandal in many long months. There had, of course, been some striking and well-publicized acts of illicit computer access, but they had been committed by adult white-collar industry insiders in clear pursuit of personal or commercial advantage. The kids, by contrast, all seemed to be on IRC, Internet Relay Chat.

Or, perhaps, frolicking out in the endless glass-roots network of personal bulletin board systems. In 1993, there were an estimated 60,000 boards in America; the population of boards had fully doubled since Operation Sundevil in 1990. The hobby was transmuting fitfully into a genuine industry. The board community were no longer obscure hobbyists; many were still hobbyists and proud of it, but board sysops and advanced board users had become a far more cohesive and politically aware community, no longer allowing themselves to be obscure.

The specter of cyberspace in the late 1980s, of outwitted authorities trembling in fear before teenage hacker whiz-kids, seemed downright antiquated by 1993. Law enforcement emphasis had changed, and the favorite electronic villain of 1993 was not the vandal child, but the victimizer of children, the digital child pornographer. "Operation Longarm," a child-pornography computer raid carried out by the previously little-known cyberspace rangers of the U.S. Customs Service, was almost the size of Operation Sundevil, but received very little notice by comparison.

The huge and well-organized "Operation Disconnect," an FBI strike against telephone rip-off con-artists, was actually larger than Sundevil. "Operation Disconnect" had its brief moment in the sun of publicity, and then vanished utterly. It was unfortunate that a law enforcement affair as apparently well-conducted as Operation Disconnect, which pursued telecom adult career criminals a hundred times more morally repugnant than teenage hackers, should have received so little attention and fanfare, especially compared to the abortive Sundevil and the basically disastrous efforts of the Chicago Computer Fraud and Abuse Task Force. But the life of an electronic policeman is seldom easy.

If any law enforcement event truly deserved full-scale press coverage (while somehow managing to escape it), it was the amazing saga of New York State Police Senior Investigator Don Delaney Versus the Orchard Street Finger-Hackers. This story probably represents the real future of professional telecommunications crime in America. The finger-hackers sold, and still sell, stolen long-distance phone service to a captive clientele of illegal aliens in New York City. This clientele is desperate to call home, yet as a group, illegal aliens have few legal means of obtaining standard phone service, since their very presence in the United States is against the law. The finger-hackers of Orchard Street were very unusual "hackers," with an astonishing lack of any kind of genuine technological knowledge. And yet these New York call-sell thieves showed a street-level ingenuity appalling in its single-minded sense of larceny.

There was no dissident-hacker rhetoric about freedom-of-information among the finger-hackers. Most of them came out of the cocaine-dealing fraternity, and they retailed stolen calls with the same street-crime techniques of lookouts and bagholders that a crack gang would employ. This was down-and-dirty, urban, ethnic, organized crime, carried out by crime families every day, for cash on the barrelhead, in the harsh world of the streets. The finger-hackers dominated certain payphones in certain strikingly unsavory neighborhoods. They provided a service no one else would give to a clientele with little to lose.

With such a vast supply of electronic crime at hand, Don Delaney rocketed from a background in homicide to teaching telecom crime at FLETC in less than three years. Few can rival Delaney's hands-on, street-level experience in phone fraud. Anyone in 1993 who still believes telecommunications crime to be something rare and arcane should have a few words with Mr Delaney. Don Delaney has also written two fine essays, on telecom fraud and computer crime, in Joseph Grau's Criminal and Civil Investigations Handbook (McGraw Hill 1993).

Phrack was still publishing in 1993, now under the able editorship of Erik Bloodaxe. Bloodaxe made a determined attempt to get law enforcement and corporate security to pay real money for their electronic copies of Phrack, but, as usual, these stalwart defenders of intellectual property preferred to pirate the magazine. Bloodaxe has still not gotten back any of his property from the seizure raids of March 1, 1990. Neither has the Mentor, who is still the managing editor of Steve Jackson Games.

Nor has Robert Izenberg, who has suspended his court struggle to get his machinery back. Mr Izenberg has calculated that his $20,000 of equipment seized in 1990 is, in 1993, worth $4,000 at most. The missing software, also gone out his door, was long ago replaced. He might, he says, sue for the sake of principle, but he feels that the people who seized his machinery have already been discredited, and won't be doing any more seizures. And even if his machinery were returned - and in good repair, which is doubtful - it will be essentially worthless by 1995. Robert Izenberg no longer works for IBM, but has a job programming for a major telecommunications company in Austin.

Steve Jackson won his case against the Secret Service on March 12, 1993, just over three years after the federal raid on his enterprise. Thanks to the delaying tactics available through the legal doctrine of "qualified immunity," Jack-

son was tactically forced to drop his suit against the individuals William Cook, Tim Foley, Barbara Golden and Henry Kluepfel. (Cook, Foley, Golden and Kluepfel did, however, testify during the trial.)

The Secret Service fought vigorously in the case, battling Jackson's lawyers right down the line, on the (mostly previously untried) legal turf of the Electronic Communications Privacy Act and the Privacy Protection Act of 1980. The Secret Service denied they were legally or morally responsible for seizing the work of a publisher. They claimed that (1) Jackson's gaming "books" weren't real books anyhow, and (2) the Secret Service didn't realize SJG Inc was a "publisher" when they raided his offices, and (3) the books only vanished by accident because they merely happened to be inside the computers the agents were appropriating.

The Secret Service also denied any wrongdoing in reading and erasing all the supposedly "private" e-mail inside Jackson's seized board, Illuminati. The USSS attorneys claimed the seizure did not violate the Electronic Communications Privacy Act, because they weren't actually "intercepting" electronic mail that was moving on a wire, but only electronic mail that was quietly sitting on a disk inside Jackson's computer. They also claimed that USSS agents hadn't read any of the private mail on Illuminati; and anyway, even supposing that they had, they were allowed to do that by the subpoena.

The Jackson case became even more peculiar when the Secret Service attorneys went so far as to allege that the federal raid against the gaming company had actually improved Jackson's business thanks to the ensuing nationwide publicity.

It was a long and rather involved trial. The judge seemed most perturbed, not by the arcane matters of electronic law, but by the fact that the Secret Service could have avoided almost all the consequent trouble simply by giving Jackson his computers back in short order. The Secret Service easily could have looked at everything in Jackson's computers, recorded everything, and given the machinery back, and there would have been no major scandal or federal court suit. On the contrary, everybody simply would have had a good laugh. Unfortunately, it appeared that this idea had never entered the heads of the Chicago-based investigators. They seemed to have concluded unilaterally, and without due course of law, that the world would be better off if Steve Jackson didn't have computers. Golden and Foley claimed that they had both never even heard of the Privacy Protection Act. Cook had heard of the Act, but he'd decided on his own that the Privacy Protection Act had nothing to do with Steve Jackson.

The Jackson case was also a very politicized trial, both sides deliberately angling for a long-term legal precedent that would stake-out big claims for their interests in cyberspace. Jackson and his EFF advisors tried hard to establish that the least e-mail remark of the lonely electronic pamphleteer deserves the same somber civil-rights protection as that afforded The New York Times. By stark contrast, the Secret Service's attorneys argued boldly that the contents of an electronic bulletin board have no more expectation of privacy than a heap of postcards. In the final analysis, very little was firmly nailed down. Formally, the legal rulings in the Jackson case apply only in the federal Western District of Texas. It was, however, established that these were real civil-liberties issues that powerful people were prepared to go to the courthouse over; the seizure of bulletin board systems, though it still goes on, can be a perilous act for the seizer. The Secret Service owes Steve Jackson $50,000 in damages, and a thousand dollars each to three of Jackson's angry and offended board users. And Steve Jackson, rather than owning the single-line bulletin board system "Illuminati" seized in 1990, now rejoices in possession of a huge privately-owned Internet node, "io.com," with dozens of phone-lines on its own T-1 trunk.

Jackson has made the entire blow-by-blow narrative of his case available electronically, for interested parties. And yet, the Jackson case may still not be over; a Secret Service appeal seems likely and the EFF is also gravely dissatisfied with the ruling on electronic interception.

The WELL, home of the American electronic civil libertarian movement, added two thousand more users and dropped its aging Sequent computer in favor of a snappy new Sun Sparcstation. Search-and-seizure dicussions on the WELL are now taking a decided back-seat to the current hot topic in digital civil liberties, unbreakable public-key encryption for private citizens.

The Electronic Frontier Foundation left its modest home in Boston to move inside the Washington Beltway of the Clinton Administration. Its new executive director, ECPA pioneer and longtime ACLU activist Jerry Berman, gained a reputation of a man adept as dining with tigers, as the EFF devoted its attention to networking at the highest levels of the computer and telecommunications industry. EFF's pro-encryption lobby and anti-wiretapping initiative were especially impressive, successfully assembling a herd of highly variegated industry camels under the same EFF tent, in open and powerful opposition to the electronic ambitions of the FBI and the NSA.

EFF had transmuted at light-speed from an insurrection to an institution. EFF Co-Founder Mitch Kapor once again sidestepped the bureaucratic consequences of his own success, by remaining in Boston and adapting the role of EFF guru and gray eminence. John Perry Barlow, for his part, left Wyoming, quit the Republican Party, and moved to New York City, accompanied by his swarm of cellular phones. Mike Godwin left Boston for Washington as EFF's official legal adviser to the electronically afflicted.

After the Neidorf trial, Dorothy Denning further proved her firm scholastic independence-of-mind by speaking up boldly on the usefulness and social value of federal wiretapping. Many civil libertarians, who regarded the practice of wiretapping with deep occult horror, were crestfallen to the point of comedy when nationally known "hacker sympathizer" Dorothy Denning sternly defended police and public interests in official eavesdropping. However, no amount of public uproar seemed to swerve the "quaint" Dr. Denning in the slightest. She not only made up her own mind, she made it up in public and then stuck to her guns.

In 1993, the stalwarts of the Masters of Deception, Phiber Optik, Acid Phreak and Scorpion, finally fell afoul of the machineries of legal prosecution. Acid Phreak and Scorpion were sent to prison for six months, six months of home detention, 750 hours of community service, and, oddly, a $50 fine for conspiracy to commit computer crime. Phiber Optik, the computer intruder with perhaps the highest public profile in the entire world, took the longest to plead guilty, but, facing the possibility of ten years in jail, he finally did so. He was sentenced to a year and a day in prison.

As for the Atlanta wing of the Legion of Doom, Prophet, Leftist and Urvile… Urvile now works for a software company in Atlanta. He is still on probation and still repaying his enormous fine. In fifteen months, he will once again be allowed to own a personal computer. He is still a convicted federal felon, but has not had any legal difficulties since leaving prison. He has lost contact with Prophet and Leftist. Unfortunately, so have I, though not through lack of honest effort.

Knight Lightning, now 24, is a technical writer for the federal government in Washington DC. He has still not been accepted into law school, but having spent more than his share of time in the company of attorneys, he's come to think that maybe an MBA would be more to the point. He still owes his attorneys $30,000, but the sum is dwindling steadily since he is manfully working two jobs. Knight Lightning customarily wears a suit and tie and carries a valise. He has a federal security clearance.

Unindicted Phrack co-editor Taran King is also a technical writer in Washington DC, and recently got married.

Terminus did his time, got out of prison, and currently lives in Silicon Valley where he is running a full-scale Internet node, "netsys.com." He programs professionally for a company specializing in satellite links for the Internet.

Carlton Fitzpatrick still teaches at the Federal Law Enforcement Training Center, but FLETC found that the issues involved in sponsoring and running a bulletin board system are rather more complex than they at first appear to be.

Gail Thackeray briefly considered going into private security, but then changed tack, and joined the Maricopa County District Attorney's Office (with a salary). She is still vigorously prosecuting electronic racketeering in Phoenix, Arizona.

The fourth consecutive Computers, Freedom and Privacy Conference will take place in March 1994 in Chicago.

As for Bruce Sterling… well `*8-)'. I thankfully abandoned my brief career as a true-crime journalist and wrote a new science fiction novel, Heavy Weather, and assembled a new collection of short stories, Globalhead. I also write non-

fiction regularly, for the popular-science column in The Magazine of Fantasy and Science Fiction.

I like life better on the far side of the boundary between fantasy and reality; but I've come to recognize that reality has an unfortunate way of annexing fantasy for its own purposes. That's why I'm on the Police Liaison Committee for EFF-Austin, a local electronic civil liberties group (eff-austin@tic.com). I don't think I will ever get over my experience of the Hacker Crackdown, and I expect to be involved in electronic civil liberties activism for the rest of my life.

It wouldn't be hard to find material for another book on computer crime and civil liberties issues. I truly believe that I could write another book much like this one, every year. Cyberspace is very big. There's a lot going on out there, far more than can be adequately covered by the tiny, though growing, cadre of network-literate reporters. I do wish I could do more work on this topic, because the various people of cyberspace are an element of our society that definitely requires sustained study and attention.

But there's only one of me, and I have a lot on my mind, and, like most science fiction writers, I have a lot more imagination than discipline. Having done my stint as an electronic-frontier reporter, my hat is off to those stalwart few who do it every day. I may return to this topic some day, but I have no real plans to do so. However, I didn't have any real plans to write "Hacker Crackdown," either. Things happen, nowadays. There are landslides in cyberspace. I'll just have to try and stay alert and on my feet.

The electronic landscape changes with astounding speed. We are living through the fastest technological transformation in human history. I was glad to have a chance to document cyberspace during one moment in its long mutation; a kind of strobe-flash of the maelstrom. This book is already out-of-date, though, and it will be quite obsolete in another five years. It seems a pity.

However, in about fifty years, I think this book might seem quite interesting. And in a hundred years, this book should seem mind-bogglingly archaic and bizarre, and will probably seem far weirder to an audience in 2092 than it ever seemed to the contemporary readership.

Keeping up in cyberspace requires a great deal of sustained attention. Personally, I keep tabs with the milieu by reading the invaluable electronic magazine Computer underground Digest (tk0jut2@mvs.cso.niu.edu with the subject header: SUB CuD and a message that says: SUB CuD your name your.full.internet@address). I also read Jack Rickard's bracingly iconoclastic Boardwatch Magazine for print news of the BBS and online community. And, needless to say, I read Wired, the first magazine of the 1990s that actually looks and acts like it really belongs in this decade. There are other ways to learn, of course, but these three outlets will guide your efforts very well.

When I myself want to publish something electronically, which I'm doing with increasing frequency, I generally put it on the gopher at Texas Internet Consulting, who are my, well, Texan Internet consultants (tic.com). This book can be found there. I think it is a worthwhile act to let this work go free.

From thence, one's bread floats out onto the dark waters of cyberspace, only to return someday, tenfold. And of course, thoroughly soggy, and riddled with an entire amazing ecosystem of bizarre and gnawingly hungry cybermarine life-forms. For this author at least, that's all that really counts.

Thanks for your attention `*8-)'

Bruce Sterling (bruces@well.sf.ca.us)
New Years' Day 1994, Austin Texas

Chronology of the Hacker Crackdown.

1865		U.S. Secret Service (USSS) founded.
1876		Alexander Graham Bell invents telephone.
1878		First teenage males flung off phone system by enraged authorities.
1939		"Futurian" science-fiction group raided by Secret Service.
1971		Yippie phone phreaks start YIPL/TAP magazine.
1972		Ramparts magazine seized in blue-box rip-off scandal.
1978		Ward Christenson and Randy Suess create first personal computer bulletin board system.
1982		William Gibson coins term "cyberspace."
1982		"414 Gang" raided. 1983-1983 AT&T dismantled in divestiture. 1984 Congress passes Compre-hensive Crime Control Act giving USSS jurisdiction over credit card fraud and computer fraud.
1984		"Legion of Doom" formed.
1984		2600: The Hacker Quarterly founded.
1984		Whole Earth Software Catalog published.
1985		First police "sting" bulletin board systems established.
1985		Whole Earth 'Lectronic Link computer confe-rence (WELL) goes on-line.
1986		Computer Fraud and Abuse Act passed.
1986		Electronic Communications Privacy Act passed.
1987		Chicago prosecutors form Computer Fraud and Abuse Task Force.
1988	July	Secret Service covertly videotapes "SummerCon" hacker convention.
	September	"Prophet" cracks BellSouth AIMSX computer network and downloads E911 Document to his own computer and to Jolnet.
	September	AT&T Corporate Information Security informed of Prophet's action.
	October	Bellcore Security informed of Prophet's action.
1989	January	Prophet uploads E911 Document to Knight Lightning.
	February 25	Knight Lightning publishes E911 Document in Phrack electronic newsletter.
	May	Chicago Task Force raids and arrests "Kyrie."
	June	"NuPrometheus League" distributes Apple Computer proprietary software.
	June 13	Florida probation office crossed with phone-sex line in switching-station stunt.
	July	"Fry Guy" raided by USSS and Chicago Computer Fraud and Abuse Task Force.
	July	Secret Service raids "Prophet", "Leftist", and "Urvile" in Georgia.
1990	January 15	Martin Luther King Day Crash strikes AT&T long-distance network nationwide.
	January 18, 19	Chicago Task Force raids Knight Lightning in St. Louis.
	January 24	USSS and New York State Police raid "Phiber Optik", "Acid Phreak", and "Scorpion" in New York City.
	February 1	USSS raids "Terminus" in Maryland.
	February 3	Chicago Task Force raids Richard Andrews' home.
	February 6	Chicago Task Force raids Richard Andrews' business.
	February 6	USSS arrests Terminus, Prophet, Leftist, and Urvile.
	February 9	Chicago Task Force arrests Knight Lightning.
	February	AT&T Security shuts down public-access "attctc" computer in

	20	Dallas.
	February 21	Chicago Task Force raids Robert Izenberg in Austin.
	March 1	Chicago Task Force raids Steve Jackson Games, Inc., “Mentor,” and “Erik Bloodaxe” in Austin.
	May 7, 8, 9	USSS and Arizona Organized Crime and Racketeering Bureau conduct “Operation Sundevil” raids in Cincinnatti, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose, and San Francisco.
	May	FBI interviews John Perry Barlow re NuPrometheus case.
	June	Mitch Kapor and Barlow found Electronic Frontier Foundation; Barlow publishes Crime and Puzzlement manifesto.
	July 24-27	Trial of Knight Lightning.
1991	February	CPSR Roundtable in Washington, D.C.
	March 25-28	Computers, Freedom and Privacy conference in San Francisco.
	May 1	Electronic Frontier Foundation, Steve Jackson, and others file suit against members of Chicago Task Force.
	July 12	Switching station phone software crash affects Washington, Los Angeles, Pittsburgh, San Francisco.
	September 17	AT&T phone crash affects New York City and three airports.

Internet

From *The Magazine Of Fantasy And Science Fiction*, February 1993.
F&SF, Box 56, Cornwall CT 06753 $26/yr USA $31/yr other

F&SF Science Column #5

Some thirty years ago, the RAND Corporation, America's foremost Cold War think-tank, faced a strange strategic problem. How could the US authorities successfully communicate after a nuclear war?

Postnuclear America would need a command-and-control network, linked from city to city, state to state, base to base. But no matter how thoroughly that network was armored or protected, its switches and wiring would always be vulnerable to the impact of atomic bombs. A nuclear attack would reduce any conceivable network to tatters.

And how would the network itself be commanded and controlled? Any central authority, any network central citadel, would be an obvious and immediate target for an enemy missile. The center of the network would be the very first place to go. RAND mulled over this grim puzzle in deep military secrecy, and arrived at a daring solution. The RAND proposal (the brainchild of RAND staffer Paul Baran) was made public in 1964. In the first place, the network would "have no central authority." Furthermore, it would be "designed from the beginning to operate while in tatters."

The principles were simple. The network itself would be assumed to be unreliable at all times. It would be designed from the get-go to transcend its own unreliability. All the nodes in the network would be equal in status to all other nodes, each node with its own authority to originate, pass, and receive messages. The messages themselves would be divided into packets, each packet separately addressed. Each packet would begin at some specified source node, and end at some other specified destination node. Each packet would wind its way through the network on an individual basis.

The particular route that the packet took would be unimportant. Only final results would count. Basically, the packet would be tossed like a hot potato from node to node to node, more or less in the direction of its destination, until it ended up in the proper place. If big pieces of the network had been blown away, that simply wouldn't matter; the packets would still stay airborne, lateralled wildly across the field by whatever nodes happened to survive. This rather haphazard delivery system might be "inefficient" in the usual sense (especially compared to, say, the telephone system) -- but it would be extremely rugged.

During the 60s, this intriguing concept of a decentralized, blastproof, packet-switching network was kicked around by RAND, MIT and UCLA. The National Physical Laboratory in Great Britain set up the first test network on these principles in 1968.

Shortly afterward, the Pentagon's Advanced Research Projects Agency decided to fund a larger, more ambitious project in the USA. The nodes of the network were to be high-speed supercomputers (or what passed for supercomputers at the time). These were rare and valuable machines which were in real need of good solid networking, for the sake of national research-and-development projects.

In fall 1969, the first such node was installed in UCLA. By December 1969, there were four nodes on the infant network, which was named ARPANET, after its Pentagon sponsor. The four computers could transfer data on dedicated high-speed transmission lines. They could even be programmed remotely from the other nodes. Thanks to ARPANET, scientists and researchers could share one another's computer facilities by long-distance. This was a very handy service, for computer-time was precious in the early '70s. In 1971 there were fifteen nodes in ARPANET; by 1972, thirty-seven nodes. And it was good.

By the second year of operation, however, an odd fact became clear. ARPANET's users had warped the computer-sharing network into a dedicated, high-speed, federally subsidized electronic post-office. The main traffic on ARPANET was not long-distance computing. Instead, it was news and personal messages. Researchers were using ARPANET to collaborate on projects, to trade notes on work, and eventually, to downright gossip and schmooze. People had their own personal user ac-

counts on the ARPANET computers, and their own personal addresses for electronic mail. Not only were they using ARPANET for person-to-person communication, but they were very enthusiastic about this particular service -- far more enthusiastic than they were about long-distance computation.

It wasn't long before the invention of the mailing-list, an ARPANET broadcasting technique in which an identical message could be sent automatically to large numbers of network subscribers. Interestingly, one of the first really big mailing-lists was "SF-LOVERS," for science fiction fans. Discussing science fiction on the network was not work-related and was frowned upon by many ARPANET computer administrators, but this didn't stop it from happening.

Throughout the '70s, ARPA's network grew. Its decentralized structure made expansion easy. Unlike standard corporate computer networks, the ARPA network could accommodate many different kinds of machine. As long as individual machines could speak the packet-switching lingua franca of the new, anarchic network, their brand-names, and their content, and even their ownership, were irrelevant.

The ARPA's original standard for communication was known as NCP, "Network Control Protocol," but as time passed and the technique advanced, NCP was superceded by a higher-level, more sophisticated standard known as TCP/IP. TCP, or "Transmission Control Protocol," converts messages into streams of packets at the source, then reassembles them back into messages at the destination. IP, or "Internet Protocol," handles the addressing, seeing to it that packets are routed across multiple nodes and even across multiple networks with multiple standards -- not only ARPA's pioneering NCP standard, but others like Ethernet, FDDI, and X.25.

As early as 1977, TCP/IP was being used by other networks to link to ARPANET. ARPANET itself remained fairly tightly controlled, at least until 1983, when its military segment broke off and became MILNET. But TCP/IP linked them all. And ARPANET itself, though it was growing, became a smaller and smaller neighborhood amid the vastly growing galaxy of other linked machines.

As the '70s and '80s advanced, many very different social groups found themselves in possession of powerful computers. It was fairly easy to link these computers to the growing network-of-networks. As the use of TCP/IP became more common, entire other networks fell into the digital embrace of the Internet, and messily adhered. Since the software called TCP/IP was public-domain, and the basic technology was decentralized and rather anarchic by its very nature, it was difficult to stop people from barging in and linking up somewhere-or-other. In point of fact, nobody "wanted" to stop them from joining this branching complex of networks, which came to be known as the "Internet."

Connecting to the Internet cost the taxpayer little or nothing, since each node was independent, and had to handle its own financing and its own technical requirements. The more, the merrier. Like the phone network, the computer network became steadily more valuable as it embraced larger and larger territories of people and resources.

A fax machine is only valuable if "everybody else" has a fax machine. Until they do, a fax machine is just a curiosity. ARPANET, too, was a curiosity for a while. Then computer-networking became an utter necessity.

In 1984 the National Science Foundation got into the act, through its Office of Advanced Scientific Computing. The new NSFNET set a blistering pace for technical advancement, linking newer, faster, shinier supercomputers, through thicker, faster links, upgraded and expanded, again and again, in 1986, 1988, 1990. And other government agencies leapt in: NASA, the National Institutes of Health, the Department of Energy, each of them maintaining a digital satrapy in the Internet confederation.

The nodes in this growing network-of-networks were divvied up into basic varieties. Foreign computers, and a few American ones, chose to be denoted by their geographical locations. The others were grouped by the six basic Internet "domains": gov, mil, edu, com, org and net. (Graceless abbreviations such as this are a standard feature of the TCP/IP protocols.) Gov, Mil, and Edu denoted governmental, military and educational institutions, which were, of course, the pioneers, since ARPANET had begun as a high-tech research exercise in national security. Com, however, stood for "commercial" institutions, which were soon

bursting into the network like rodeo bulls, surrounded by a dust-cloud of eager nonprofit "orgs." (The "net" computers served as gateways between networks.)

ARPANET itself formally expired in 1989, a happy victim of its own overwhelming success. Its users scarcely noticed, for ARPANET's functions not only continued but steadily improved. The use of TCP/IP standards for computer networking is now global. In 1971, a mere twenty-one years ago, there were only four nodes in the ARPANET network. Today there are tens of thousands of nodes in the Internet, scattered over forty-two countries, with more coming on-line every day. Three million, possibly four million people use this gigantic mother-of-all-computer-networks.

The Internet is especially popular among scientists, and is probably the most important scientific instrument of the late twentieth century. The powerful, sophisticated access that it provides to specialized data and personal communication has sped up the pace of scientific research enormously.

The Internet's pace of growth in the early 1990s is spectacular, almost ferocious. It is spreading faster than cellular phones, faster than fax machines. Last year the Internet was growing at a rate of twenty percent a "month." The number of "host" machines with direct connection to TCP/IP has been doubling every year since 1988. The Internet is moving out of its original base in military and research institutions, into elementary and high schools, as well as into public libraries and the commercial sector.

Why do people want to be "on the Internet?" One of the main reasons is simple freedom. The Internet is a rare example of a true, modern, functional anarchy. There is no "Internet Inc." There are no official censors, no bosses, no board of directors, no stockholders. In principle, any node can speak as a peer to any other node, as long as it obeys the rules of the TCP/IP protocols, which are strictly technical, not social or political. (There has been some struggle over commercial use of the Internet, but that situation is changing as businesses supply their own links).

The Internet is also a bargain. The Internet as a whole, unlike the phone system, doesn't charge for long-distance service. And unlike most commercial computer networks, it doesn't charge for access time, either. In fact the "Internet" itself, which doesn't even officially exist as an entity, never "charges" for anything. Each group of people accessing the Internet is responsible for their own machine and their own section of line.

The Internet's "anarchy" may seem strange or even unnatural, but it makes a certain deep and basic sense. It's rather like the "anarchy" of the English language. Nobody rents English, and nobody owns English. As an English-speaking person, it's up to you to learn how to speak English properly and make whatever use you please of it (though the government provides certain subsidies to help you learn to read and write a bit). Otherwise, everybody just sort of pitches in, and somehow the thing evolves on its own, and somehow turns out workable. And interesting. Fascinating, even. Though a lot of people earn their living from using and exploiting and teaching English, "English" as an institution is public property, a public good. Much the same goes for the Internet. Would English be improved if the "The English Language, Inc." had a board of directors and a chief executive officer, or a President and a Congress? There'd probably be a lot fewer new words in English, and a lot fewer new ideas.

People on the Internet feel much the same way about their own institution. It's an institution that resists institutionalization. The Internet belongs to everyone and no one.

Still, its various interest groups all have a claim. Business people want the Internet put on a sounder financial footing. Government people want the Internet more fully regulated. Academics want it dedicated exclusively to scholarly research. Military people want it spy-proof and secure. And so on and so on.

All these sources of conflict remain in a stumbling balance today, and the Internet, so far, remains in a thrivingly anarchical condition. Once upon a time, the NSFnet's high-speed, high-capacity lines were known as the "Internet Backbone," and their owners could rather lord it over the rest of the Internet; but today there are "backbones" in Canada, Japan, and Europe, and even privately owned commercial Internet backbones specially created for carrying business traffic. Today, even privately owned desktop computers can become Internet nodes. You can carry one under your arm. Soon, perhaps, on your wrist.

But what does one “do” with the Internet? Four things, basically: mail, discussion groups, long-distance computing, and file transfers.

Internet mail is “e-mail,” electronic mail, faster by several orders of magnitude than the US Mail, which is scornfully known by Internet regulars as “snailmail.” Internet mail is somewhat like fax. It’s electronic text. But you don’t have to pay for it (at least not directly), and it’s global in scope. E-mail can also send software and certain forms of compressed digital imagery. New forms of mail are in the works.

The discussion groups, or “newsgroups,” are a world of their own. This world of news, debate and argument is generally known as “USENET. “ USENET is, in point of fact, quite different from the Internet. USENET is rather like an enormous billowing crowd of gossipy, news-hungry people, wandering in and through the Internet on their way to various private backyard barbecues. USENET is not so much a physical network as a set of social conventions. In any case, at the moment there are some 2,500 separate newsgroups on USENET, and their discussions generate about 7 million words of typed commentary every single day. Naturally there is a vast amount of talk about computers on USENET, but the variety of subjects discussed is enormous, and it’s growing larger all the time. USENET also distributes various free electronic journals and publications.

Both netnews and e-mail are very widely available, even outside the high-speed core of the Internet itself. News and e-mail are easily available over common phone-lines, from Internet fringe-realms like BITnet, UUCP and Fidonet. The last two Internet services, long-distance computing and file transfer, require what is known as “direct Internet access” -- using TCP/IP.

Long-distance computing was an original inspiration for ARPANET and is still a very useful service, at least for some. Programmers can maintain accounts on distant, powerful computers, run programs there or write their own. Scientists can make use of powerful supercomputers a continent away. Libraries offer their electronic card catalogs for free search. Enormous CD-ROM catalogs are increasingly available through this service. And there are fantastic amounts of free software available.

File transfers allow Internet users to access remote machines and retrieve programs or text. Many Internet computers -- some two thousand of them, so far -- allow any person to access them anonymously, and to simply copy their public files, free of charge. This is no small deal, since entire books can be transferred through direct Internet access in a matter of minutes. Today, in 1992, there are over a million such public files available to anyone who asks for them (and many more millions of files are available to people with accounts). Internet file-transfers are becoming a new form of publishing, in which the reader simply electronically copies the work on demand, in any quantity he or she wants, for free. New Internet programs, such as “archie,” “gopher,” and “WAIS,” have been developed to catalog and explore these enormous archives of material.

The headless, anarchic, million-limbed Internet is spreading like bread-mold. Any computer of sufficient power is a potential spore for the Internet, and today such computers sell for less than $2,000 and are in the hands of people all over the world. ARPA’s network, designed to assure control of a ravaged society after a nuclear holocaust, has been superceded by its mutant child the Internet, which is thoroughly out of control, and spreading exponentially through the post-Cold War electronic global village. The spread of the Internet in the 90s resembles the spread of personal computing in the 1970s, though it is even faster and perhaps more important. More important, perhaps, because it may give those personal computers a means of cheap, easy storage and access that is truly planetary in scale.

The future of the Internet bids fair to be bigger and exponentially faster. Commercialization of the Internet is a very hot topic today, with every manner of wild new commercial information-service promised. The federal government, pleased with an unsought success, is also still very much in the act. NREN, the National Research and Education Network, was approved by the US Congress in fall 1991, as a five-year, $2 billion project to upgrade the Internet “backbone.” NREN will be some fifty times faster than the fastest network available today, allowing the electronic transfer of the entire Encyclopedia Britannica in one hot second. Computer networks worldwide will feature 3-D animated graphics, ra-

dio and cellular phone-links to portable computers, as well as fax, voice, and high-definition television. A multimedia global circus!

Or so it's hoped -- and planned. The real Internet of the future may bear very little resemblance to today's plans. Planning has never seemed to have much to do with the seething, fungal development of the Internet. After all, today's Internet bears little resemblance to those original grim plans for RAND's post-holocaust command grid. It's a fine and happy irony.

How does one get access to the Internet? Well -- if you don't have a computer and a modem, get one. Your computer can act as a terminal, and you can use an ordinary telephone line to connect to an Internet-linked machine. These slower and simpler adjuncts to the Internet can provide you with the netnews discussion groups and your own e-mail address. These are services worth having -- though if you only have mail and news, you're not actually "on the Internet" proper.

If you're on a campus, your university may have direct "dedicated access" to high-speed Internet TCP/IP lines. Apply for an Internet account on a dedicated campus machine, and you may be able to get those hot-dog long-distance computing and file-transfer functions. Some cities, such as Cleveland, supply "freenet" community access. Businesses increasingly have Internet access, and are willing to sell it to subscribers. The standard fee is about $40 a month -- about the same as TV cable service.

As the Nineties proceed, finding a link to the Internet will become much cheaper and easier. Its ease of use will also improve, which is fine news, for the savage UNIX interface of TCP/IP leaves plenty of room for advancements in user-friendliness. Learning the Internet now, or at least learning about it, is wise. By the turn of the century, "network literacy," like "computer literacy" before it, will be forcing itself into the very texture of your life.

For Further Reading:

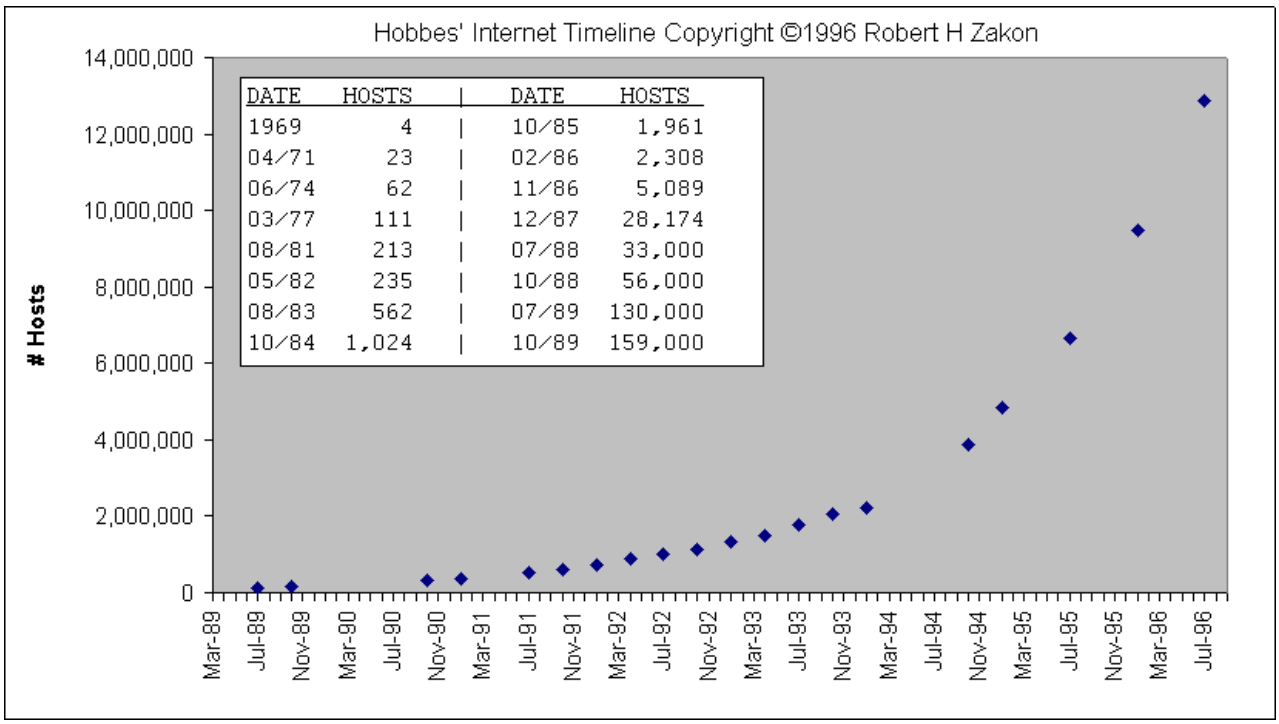
The Whole Internet Catalog & User's Guide by Ed Krol. (1992) O'Reilly and Associates, Inc. A clear, non-jargonized introduction to the intimidating business of network literacy. Many computer-documentation manuals attempt to be funny. Mr. Krol's book is "actually" funny.

The Matrix: Computer Networks and Conferencing Systems Worldwide by John Quarterman. Digital Press: Bedford, MA. (1990) Massive and highly technical compendium detailing the mind-boggling scope and complexity of our newly networked planet.

The Internet Companion by Tracy LaQuey with Jeanne C. Ryer (1992) Addison Wesley. Evangelical etiquette guide to the Internet featuring anecdotal tales of life-changing Internet experiences. Foreword by Senator Al Gore.

Zen and the Art of the Internet: A Beginner's Guide by Brendan P. Kehoe (1992) Prentice Hall. Brief but useful Internet guide with plenty of good advice on useful machines to paw over for data. Mr Kehoe's guide bears the singularly wonderful distinction of being available in electronic form free of charge. I'm doing the same with all my F&SF Science articles, including, of course, this one.

My own Internet address is bruces@well.sf.ca.us.



DATE	HOSTS	DATE	HOSTS
1969	4	10/85	1,961
04/71	23	02/86	2,308
06/74	62	11/86	5,089
03/77	111	12/87	28,174
08/81	213	07/88	33,000
05/82	235	10/88	56,000
08/83	562	07/89	130,000
10/84	1,024	10/89	159,000

“…This is a book about cops, and wild teenage whiz-kids,
and lawyers, and hairy-eyed anarchists,
and industrial technicians, and hippies,
and high-tech millionaires, and game hobbyists,
and computer security experts,
and Secret Service agents, and grifters, and thieves.
This book is about the electronic frontier of the 1990s…
…this is the story of the people of cyberspace…”

-Bruce Sterling-