

PART

2

THE DIGITAL UNDERGROUND

The date was May 9, 1990. The Pope was touring Mexico City. Hustlers from the Medellín 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 U.S. Attorney's office in Phoenix, Arizona, had issued a press release announcing a nationwide law enforcement crack-down 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 150 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 U.S. Secret Service, Assistant U.S. 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 U.S. 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 "high tech computer operators"? Where had they come from? What did they want? Were they "mischievous"? Were they dangerous? How had "misguided teenagers" managed to alarm the U.S. 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*.

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

How had “misguided teenagers” managed to alarm the U.S. Secret Service?

But the genuine roots of the modern hacker *underground* probably can 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 Hoffman as 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 television 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 titled *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 that 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, a federal surtax was 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. Rip-ping off the System found its 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 outlast the Yippie movement itself.

In the early 1970s, it required fairly limited expertise and ingenuity to cheat pay phones, 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 Line was 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 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*.

TAP articles, 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 reveled in gloating possession of the specialized knowledge necessary to beat the System.

Al Bell dropped out of the game by the late 1970s, and "Tom Edison" took over; TAP readers (some 1,400 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").

* * *

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 pay phone reveals itself as a little fortress, carefully designed and redesigned over generations, to resist coin slugs, 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 pay phone is as exquisitely evolved as a cactus.

A modern pay phone is as exquisitely evolved as a cactus.

Because the phone network predates the computer network, the scofflaws known as “phone phreaks” predate 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 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 baby-sitting), 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 United States, who pile up enormous unpaid long-distance bills to the Caribbean, South America, and Pakistan.

The simplest way to steal phone codes is to look over a victim's shoulder as he punches in his own code number on a public pay phone. 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 dialing of hundreds of numbers can be detected within hours and swiftly traced. If a stolen code is abused repeatedly, 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 dialing 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 phone company 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 California 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 information. 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 reprogrammed 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 (PBX) 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 sometimes have 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 all can be monitored by various forms of radio; this kind of "passive monitoring" is spreading explosively today. 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 such as 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. As mentioned, hackers are mostly young suburban American white males, and exist in the hundreds—but phreaks come from both sexes and from many nationalities, ages, and ethnic backgrounds, and are flourishing in the thousands.

An infestation of angry phone phreaks in one's voice-mail system is no joke.

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 antibureaucratic 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 marvelous 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 some 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 corraled 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, that is, 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 important, "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 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 existed 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, predate 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 résumé 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” computers. 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 data banks 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 un-

real estate. In the new, severe, responsible, high-stakes 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 that is

cool and elite from behavior that 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. Backstabbing slander, threats, and electronic harassment are freely employed in down-and-dirty intrahacker feuds, but this rarely forces a rival out of the scene entirely. The only real solution to the problem of an utterly losing, treacherous, and rodentlike hacker is to *turn him in to the police*. Unlike the Mafia or Medellín 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, they 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 have been learned only by exceptional cunning and stealth. Forbidden knowl-

Forbidden knowledge is the basic currency of the digital underground.

edge, 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 worldview so elitist, so closed and hermetic, that electronic police simply are 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 Techno-Revolution” 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 the bottom line, they are scoff-laws. 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.

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 antimaterialistic (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 narrow-minded 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 antimaterialistic 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 antiphreak 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 pay phones with crowbars. Allegations of "monetary losses" from computer intrusion are notoriously inflated. The act of illicitly copying a document from a computer is equated with that of directly robbing a company of, say, half a million dollars. The teenage computer intruder in possession of this "proprietary" document certainly has 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

*Police want to believe
that all hackers are
thieves.*

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 1970s, 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 exposés 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 sociopolitical worldview. He himself is not 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 that 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, Václav 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, for instance,

Goldstein 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 signaling 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 fling-

ing sticks of dynamite into their pond to see what lives on the bottom.

Telco employees regard this "exploration" as akin to flinging sticks of dynamite into their pond to see what lives on the bottom.

2600 has 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 techno-rat brothers (rarely, sisters) are a besieged 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, be-

cause 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 unpluralizable 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 that serves as an information and message-passing center for users dialing up over the phone lines through the use of modems. A "modem," or modulator-demodulator, is a device that 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 Seuss 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 hardworking 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 United States, 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 secondhand 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 nontechnical 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 likely would be practically unenforceable. It would almost be easier to “regulate,” “inspect,” and “license” the content of private mail—probably more so, because 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 reruns 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 that 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 a 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 role-playing and pseudonymous posturing are forbidden.

Boards can be grouped by their immediacy. "Chat lines" 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 phone line, store messages serially, one at a time. And some boards are open for business only 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 participate openly. 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 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. Drug-dealing 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. Extasy Elite.

Fargo 4A. Farmers of Doom. The Federation. Feds R Us. First Class. Five 0. 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 SoftWareZ 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, 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 is an actual corporation, but all take clear delight in mimicking them.

Second, governments and police. NASA Elite, The 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: Stowaways, The Hitchhikers, 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 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.

The true population of the digital underground is hard to estimate. There is constant turnover. Most hackers start young, come and go, then drop out at age twenty-two—the age of college graduation. And a large majority 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 five thousand 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 twenty-four or twenty-five 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 nonprofit 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, small-scale 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," precomposed texts that 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.

BANKAMER.ZIP	5406 06-11-91 Hacking Bank America
CHHACK.ZIP	4481 06-11-91 Chilton Hacking
CITIBANK.ZIP	4118 06-11-91 Hacking Citibank
CREDIMTC.ZIP	3241 06-11-91 Hacking Mtc Credit Company
DIGEST.ZIP	5159 06-11-91 Hackers Digest
HACK.ZIP	14031 06-11-91 How To Hack
HACKBAS.ZIP	5073 06-11-91 Basics Of Hacking
HACKDICT.ZIP	42774 06-11-91 Hackers Dictionary
HACKER.ZIP	57938 06-11-91 Hacker Info
HACKERME.ZIP	3148 06-11-91 Hackers Manual
HACKHAND.ZIP	4814 06-11-91 Hackers Handbook
HACKTHES.ZIP	48290 06-11-91 Hackers Thesis
HACKVMS.ZIP	4696 06-11-91 Hacking Vms Systems
MCDON.ZIP	3830 06-11-91 Hacking Macdonalds (Home Of The Archs)
P500UNIX.ZIP	15525 06-11-91 Phortune 500 Guide To Unix
RADHACK.ZIP	8411 06-11-91 Radio Hacking
TA0TRASH.DOC	4096 12-25-89 Suggestions For Trashing
TECHHACK.ZIP	5063 06-11-91 Technical Hacking

The preceding files are do-it-yourself manuals about computer intrusion. The list 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.



ANARC.ZIP	3641 06-11-91 Anarchy Files
ANARCHST.ZIP	63703 06-11-91 Anarchist Book
ANARCHY.ZIP	2076 06-11-91 Anarchy At Home
ANARCHY3.ZIP	6982 06-11-91 Anarchy No 3
ANARCTOY.ZIP	2361 06-11-91 Anarchy Toys
ANTIMODM.ZIP	2877 06-11-91 Anti-modem Weapons
ATOM.ZIP	4494 06-11-91 How To Make An Atom Bomb
BARBITUA.ZIP	3982 06-11-91 Barbiturate Formula
BLCKPWDR.ZIP	2810 06-11-91 Black Powder Formulas
BOMB.ZIP	3765 06-11-91 How To Make Bombs
BOOM.ZIP	2036 06-11-91 Things That Go Boom
CHLORINE.ZIP	1926 06-11-91 Chlorine Bomb
COOKBOOK.ZIP	1500 06-11-91 Anarchy Cook Book
DESTROY.ZIP	3947 06-11-91 Destroy Stuff
DUSTBOMB.ZIP	2576 06-11-91 Dust Bomb
ELECTERR.ZIP	3230 06-11-91 Electronic Terror
EXPLOS1.ZIP	2598 06-11-91 Explosives 1
EXPLOSIV.ZIP	18051 06-11-91 More Explosives
EZSTEAL.ZIP	4521 06-11-91 Ez-stealing

FLAME.ZIP	2240 06-11-91 Flame Thrower
FLASHLT.ZIP	2533 06-11-91 Flashlight Bomb
FMBUG.ZIP	2906 06-11-91 How To Make An Fm Bug
OMEEXPL.ZIP	2139 06-11-91 Home Explosives
HOW2BRK.ZIP	3332 06-11-91 How To Break In
LETTER.ZIP	2990 06-11-91 Letter Bomb
LOCK.ZIP	2199 06-11-91 How To Pick Locks
MRSHIN.ZIP	3991 06-11-91 Briefcase Locks
NAPALM.ZIP	3563 06-11-91 Napalm At Home
NITRO.ZIP	3158 06-11-91 Fun With Nitro
PARAMIL.ZIP	2962 06-11-91 Paramilitary Info
PICKING.ZIP	3398 06-11-91 Picking Locks
PIPEBOMB.ZIP	2137 06-11-91 Pipe Bomb
POTASS.ZIP	3987 06-11-91 Formulas With Potassium
PRANK.TXT	11074 08-03-90 More Pranks To Pull On Idiots!
REVENGE.ZIP	4447 06-11-91 Revenge Tactics
ROCKET.ZIP	2590 06-11-91 Rockets For Fun
SMUGGLE.ZIP	3385 06-11-91 How To Smuggle

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, actually will 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.

Blowing the arm off your high school vice-principal can be a thing of dark beauty to contemplate.

Nevertheless, if temptation is spread before people a certain number will succumb, and a small minority actually will 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 passersby. 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.

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 Ore-

gon 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 keyboard, 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 awhile, 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-dialing 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 dialing 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—one 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 8 zillion lousy space invaders.

Hackers perceive hacking 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, such as 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, such as computer games that simulate tank battles or dogfights or spaceships. Simulations are just make-believe, 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 wire fraud. 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 some-

thing, and kept it in his house on a floppy disk—this is regarded as a sign of near insanity on the part of 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

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-day 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 Ps and Qs 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-1980s, 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, because it was in his area code. Lex's own board, Legion of Doom, started in 1984. The Neon Knights ran a network of Apple-hacker 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 came 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 such as Metal Shop AE, Metal Shop Private, and 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 best-publicized computer-intrusion scandal to date. Morris said that his ingenious "worm" program was meant to explore the Internet harm-

lessly, 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 Sergeant Robert Ansley called himself "Pluto"—The Phone Company in Phoenix, Arizona, run by Ken MacLeod of the Maricopa County Sheriff's office—and Sergeant 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 are cheap to operate; very cheap, by the standards of undercover police operations.

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 ultra-mastermind 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, mouth-filling 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 crime-fighting 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 was 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 was built 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. "Compu-Phreak" 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 was flagrant. Not only was it one of the earliest groups, but members took pains to distribute their illicit knowledge widely. Some LoD members, such as "The Mentor," were

close to evangelical about it. *Legion of Doom Technical Journal* began to show up on boards throughout the underground.

LoD Technical Journal was 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 techno-bureaucratese, appears tedious and almost unreadable, scarcely 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 *data*, however, are identical. They are *public* data, presented before the federal government in an open hearing. They are not “secret.” They are not “proprietary.” They are 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 mimicry, 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 ring-leaders inventing and spreading stuff like (B). If it weren’t for these jokers, there wouldn’t *be* any trouble.

And Legion of Doom was 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.

Somewhere at the center of this conspiracy there had to be some adult masterminds.

This was a difficult charge to deny, as LoD never distributed membership badges or laminated ID cards. If it had, it likely would have died out quickly, for turnover in 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 years, and it seemed *weird* to police that they continually were 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 all 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—he 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 improved drastically 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 secondhand digital hot rods full of custom add-ons that they'd cobbled together out of chicken wire, 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 on a merry chase, and when captured in 1987, he turned out to be a bright and apparently physically harmless young fanatic, fasci-

nated 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, the members 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 was "cake." U S West (of Arizona, the Rockies, and the Pacific Northwest) was tough and aggressive, probably the heaviest RBOC around. Pacific Bell, California's PacBell, was sleek, high tech, and a longtime veteran of the L.A. phone-phreak wars. NYNEX had the misfortune to run the New York City area and was warily prepared for most anything. Even Michigan Bell, a division of the Ameritech RBOC, at least had the elementary sense to hire its own hacker as a useful scarecrow. But BellSouth, even though its corporate public relations proclaimed it to have "Everything You Expect From a Leader," was pathetic.

When rumor about LoD's mastery of Georgia's switching network got around to BellSouth through Bellcore and telco security scuttlebutt, at first it 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 word-analysis programs, that the Condor could start World War III from a pay phone.

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. It 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 reprogrammed 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 it didn't know wouldn't hurt it.

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 twelve-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."

What the investigators found astounded them. Proprietary telco databases had been manipulated: phone numbers had been created out of thin air, with no users' names and no addresses and, perhaps worst of all, no charges and no records of use. The new digital ReMOB (Remote Observation) diagnostic feature

had been tampered with extensively—hackers had learned to reprogram ReMOB software, so that they could listen in on any switch-routed call at their leisure! They were using telco property to *spy*!

The electrifying news went out throughout law enforcement in 1989. It had never really occurred to anyone at BellSouth that its prized and brand-new digital switching stations could be *reprogrammed*. People seemed utterly amazed that anyone could have the nerve. Of course these switching stations were “computers,” and everybody knew hackers liked to “break into computers.” But telephone people’s computers were *different* from normal people’s computers.

The exact reason *why* these computers were “different” was rather ill defined. It certainly wasn’t the extent of their security. The security on these BellSouth computers was lousy; the AIMSX computers, for instance, didn’t even have passwords. But there was no question that BellSouth strongly *felt* that its computers were very different indeed. And if there were some criminals out there who had not gotten that message, BellSouth was determined to see that message taught.

After all, a 5ESS switching station was no mere bookkeeping system for some local chain of florists. Public service depended on these stations. Public *safety* depended on these stations.

Hackers could spy on anybody in the local area!

And hackers, lurking in there call-forwarding or ReMobbing, could spy on anybody in the local area! They could spy on

telco officials! They could spy on police stations! They could spy on local offices of the Secret Service. . . .

In 1989, electronic cops and hacker-trackers began using scrambler phones and secured lines. It only made sense. There was no telling who was into those systems. Whoever they were, they sounded scary. This was some new level of antisocial daring. Could be West German hackers, in the pay of the KGB. That too had seemed a weird and farfetched notion, until Clifford Stoll had poked and prodded a sluggish Washington law-enforcement

bureaucracy into investigating a computer intrusion that turned out to be exactly that—*hackers, in the pay of the KGB!* Stoll, the systems manager for an Internet lab in Berkeley, California, had ended up on the front page of *The New York Times*, proclaimed a national hero in the first true story of international computer espionage. Stoll's counterspy efforts, which he related in a best-selling book, *The Cuckoo's Egg*, in 1989, had established the credibility of "hacking" as a possible threat to national security. The U.S. Secret Service doesn't mess around when it suspects a possible action by a foreign intelligence apparatus.

The Secret Service scrambler phones and secured lines put a tremendous kink in law enforcement's ability to operate freely; to get the word out, cooperate, prevent misunderstandings. Nevertheless, 1989 scarcely seemed the time for half-measures. If the police and Secret Service themselves were not operationally secure, then how could they reasonably demand measures of security from private enterprise? At least, the inconvenience made people aware of the *seriousness* of the threat.

If there was a final spur needed to get the police off the dime, it came in the realization that the emergency 911 system was vulnerable. The 911 system has its own specialized software, but it is run on the same digital switching systems as the rest of the telephone network. The system is not physically different from normal telephony. But it is certainly *culturally* different, because this is the area of telephonic cyberspace reserved for the police and emergency services.

Your average policeman may not know much about hackers or phone phreaks. Computer people are weird; even computer *cops* are rather weird; the stuff they do is hard to figure out. But a threat to the 911 system is anything but abstract. If the 911 system goes, people can die.

Imagine being in a car wreck, staggering to a phone booth, punching 911, and hearing "Tina" pick up the phone-sex line somewhere in New York! The situation's no longer comical, somehow.

And was it possible? No question. Hackers had attacked 911 systems before. Phreaks can max-out 911 systems just by siccing a

bunch of computer modems on them in tandem, dialing them over and over until they clog. That's very crude and low tech, but it's still a serious business.

The time had come for action. It was time to take stern measures with the underground. It was time to start picking up the dropped threads, the loose edges, the bits of braggadocio here and there; it was time to get on the stick and start putting serious casework together. Hackers weren't "invisible." They *thought* they were invisible; but the truth was, they had just been tolerated too long.

Under sustained police attention in the summer of 1989, the digital underground began to unravel as never before.

The first big break in the case came very early on: July 1989, the following month. The perpetrator of the "Tina" switch was caught and confessed. His name was "Fry Guy," a sixteen-year-old in Indiana. Fry Guy had been a very wicked young man.

Fry Guy had earned his handle from a stunt involving French fries. Fry Guy had filched the log-in of a local MacDonald's manager and had logged on to the MacDonald's mainframe on the Sprint Telenet system. Posing as the manager, Fry Guy had altered MacDonald's records and given generous raises to some teenage hamburger-flipping friends. He had not been caught.

Emboldened by success, Fry Guy moved on to credit card abuse. Fry Guy was quite an accomplished talker, with a gift for "social engineering." If you can do social engineering—fast talk, fake-outs, impersonation, conning, scamming—then card abuse comes easy. (Getting away with it in the long run is another question.)

Fry Guy had run across Urvile of the Legion of Doom on the ALTOS Chat board in Bonn, Germany. ALTOS Chat was a sophisticated board, accessible through such globe-spanning computer networks as BITNET, Tymnet, and Telenet. ALTOS was much frequented by members of Germany's Chaos Computer Club. Two Chaos hackers who hung out on ALTOS, "Jaeger" and "Pengo," had been the central villains of Clifford Stoll's *Cuckoo's Egg* case: consorting in East Berlin with a spymaster from the

KGB and breaking into American computers for hire, through the Internet.

When LoD members learned the story of Jaeger's depredations from Stoll's book, they were rather less than impressed, technically speaking. On LoD's own favorite board of the moment, Black Ice, LoD members bragged that they themselves could have done all the Chaos break-ins in a week flat! Nevertheless, LoD was grudgingly impressed by the Chaos rep, the sheer hairy-eyed daring of hash-smoking anarchist hackers who had rubbed shoulders with the fearsome big boys of international Communist espionage. LoD members sometimes traded bits of knowledge with friendly German hackers on ALTOS—phone numbers for vulnerable VAX/VMS computers in Georgia, for instance. Dutch and British phone phreaks, and the Australian clique of "Phoenix," "Nom," and "Electron," were ALTOS regulars too. In underground circles, to hang out on ALTOS was considered the sign of an elite dude, a sophisticated hacker of the international digital jet set.

Fry Guy quickly learned how to raid information from credit card consumer-reporting agencies. He had over a hundred stolen credit card numbers in his notebooks and upward of a thousand swiped long-distance access codes. He knew how to get onto ALTOS and how to talk the talk of the underground convincingly. He now wheedled knowledge of switching-station tricks from Urvile on the ALTOS system.

Combining these two forms of knowledge enabled Fry Guy to bootstrap his way up to a new form of wire fraud. First, he'd snatched credit card numbers from credit-company computers. The data he copied included names, addresses, and phone numbers of the random cardholders.

Then Fry Guy, impersonating a cardholder, called up Western Union and asked for a cash advance on "his" credit card. Western Union, as a security guarantee, would call the customer back, at home, to verify the transaction.

But, just as he had switched the Florida probation office to Tina in New York, Fry Guy switched the cardholder's number to a

local pay phone. There he would lurk in wait, muddying his trail by routing and rerouting the call through switches as far away as Canada. When the call came through, he would boldly “social engineer,” or con, the Western Union people, pretending to be the legitimate cardholder. Because he’d answered the proper phone number, the deception was not very hard. Western Union’s money was then shipped to a confederate of Fry Guy’s in his hometown in Indiana.

Fry Guy and his cohort, using LoD techniques, stole \$6,000 from Western Union between December 1988 and July 1989. They also dabbled in ordering delivery of stolen goods through card fraud. Fry Guy was intoxicated with success. The sixteen-year-old fantasized wildly to hacker rivals, boasting that he'd used ripped-off money to hire himself a big limousine and had driven out-of-state with a groupie from his favorite heavy-metal band, Motley Crue.

Armed with knowledge, power, and a gratifying stream of free money, Fry Guy now took it upon himself to call local representatives of Indiana Bell security, to brag, boast, strut, and utter tormenting warnings that his powerful friends in the notorious Legion of Doom could crash the national telephone network. Fry Guy even named a date for the scheme: the Fourth of July, a national holiday.

This egregious example of the begging-for-arrest syndrome was followed shortly by Fry Guy's arrest. After the Indiana telephone company figured out who he was, the Secret Service had DNRs—Dialed Number Recorders—installed on his home phone lines. These devices are not taps and can't record the substance of phone calls, but they do record the phone numbers of all calls going in and out. Tracing these numbers showed Fry Guy's long-distance code fraud, his extensive ties to pirate bulletin boards, and numerous personal calls to his LoD friends in Atlanta. By July 11, 1989, Prophet, Urvile, and Leftist also had Secret Service DNR "pen registers" installed on their own lines.

The Secret Service showed up in force at Fry Guy's house on July 22, 1989, to the horror of his unsuspecting parents. The

raiders were led by a special agent from the service's Indianapolis office. However, the raiders were accompanied and advised by Timothy M. Foley of the Chicago office (a gentleman about whom we will soon be hearing a great deal).

Following federal computer-crime techniques that had been standard since the early 1980s, the Secret Service searched the house thoroughly and seized all of Fry Guy's electronic equipment and note-

books. All his equipment went out the door in the custody of the Secret Service, which put a swift end to his depredations.

The Secret Service interrogated Fry Guy at length. His case was put in the charge of Deborah Daniels, the federal U.S. Attorney for the Southern District of Indiana. Fry Guy was charged with eleven counts of computer fraud, unauthorized computer access, and wire fraud. The evidence was thorough and irrefutable. For his part, Fry Guy blamed his corruption on the Legion of Doom and offered to testify against it.

Fry Guy insisted that the Legion intended to crash the phone system on a national holiday. And when AT&T crashed on Martin Luther King Day, 1990, this lent a credence to his claim that genuinely alarmed telco security and the Secret Service.

Fry Guy eventually pled guilty on May 31, 1990. On September 14 he was sentenced to forty-four months' probation and four hundred hours' community service. He could have had it much worse; but it made sense to prosecutors to take it easy on this teenage minor, while zeroing in on the notorious kingpins of the Legion of Doom.

But the case against LoD had nagging flaws. Despite the best effort of investigators, it was impossible to prove that the Legion had crashed the phone system on January 15, because it, in fact, hadn't done so. The investigations of 1989 did show that certain members of the Legion of Doom had achieved unprecedented power over the telco switching stations and that they were in

The Secret Service showed up in force, to the horror of Fry Guy's unsuspecting parents.

active conspiracy to obtain more power yet. Investigators were privately convinced that the Legion of Doom intended to do awful things with this knowledge, but mere evil intent was not enough to put them in jail.

And although the Atlanta Three—Prophet, Leftist, and especially Urvile—had taught Fry Guy plenty, they were not themselves credit card fraudsters. The only thing they'd "stolen" was long-distance service—and because they'd done much of that through phone-switch manipulation, there was no easy way to judge how much they'd "stolen," or whether this practice was even "theft" of any easily recognizable kind.

Fry Guy's theft of long-distance codes had cost the phone companies plenty. The theft of long-distance service may be a fairly theoretical "loss," but it costs genuine money and genuine time to delete all those stolen codes and to reissue new codes to the innocent owners of the corrupted ones. The owners of the codes themselves are victimized, and lose time and money and peace of mind in the hassle. And then there were the credit card victims to deal with too, and Western Union. When it came to rip-off, Fry Guy was far more of a thief than LoD. It was only when it came to actual computer expertise that Fry Guy was small potatoes.

The Atlanta Three thought most "rules" of cyberspace were for rodents and losers, but they *did* have rules. *They never crashed anything, and they never took money.* These were rough rules of thumb, and rather dubious principles when it comes to the ethical subtleties of cyberspace, but they enabled the Atlanta Three to operate with a relatively clear conscience (though never with peace of mind).

If you didn't hack for money, if you weren't robbing people of actual funds—money in the bank, that is—then nobody *really* got hurt, in LoD's opinion. "Theft of service" was a bogus issue, and "intellectual property" was a bad joke. But LoD had only elitist contempt for rip-off artists, "leechers," thieves. The members considered themselves clean. In their opinion, if you didn't smash up or crash any systems (well, not on purpose, anyhow—acci-

dents can happen, just ask Robert Morris), then it was very unfair to call you a “vandal” or a “cracker.” When you were hanging out on-line with your “pals” in telco security, you could face them down from the higher plane of hacker morality. And you could mock the police from the supercilious heights of your hacker’s quest for pure knowledge.

But from the point of view of law enforcement and telco security, however, Fry Guy was not really dangerous. The Atlanta Three *were* dangerous. It wasn’t the crimes they were committing, but the *danger*, the potential hazard, the sheer *technical power* LoD had accumulated, that had made the situation untenable.

Fry Guy was not LoD. He’d never laid eyes on anyone in LoD; his only contacts with them had been electronic. Core members of the Legion of Doom tended to meet physically for conventions every year or so, to get drunk, give each other the hacker high sign, send out for pizza, and ravage hotel suites. Fry Guy had never done any of this. Deborah Daniels assessed Fry Guy accurately as “an LoD wannabe.”

Nevertheless Fry Guy’s crimes would be directly attributed to LoD in much future police propaganda. LoD would be described as “a closely knit group” involved in “numerous illegal activities” including “stealing and modifying individual credit histories” and “fraudulently obtaining money and property.” Fry Guy did this, but the Atlanta Three didn’t; they simply weren’t into theft, but rather intrusion. This caused a strange kink in the prosecution’s strategy. LoD was accused of “disseminating information about attacking computers to other computer hackers in an effort to shift the focus of law enforcement to those other hackers and away from the Legion of Doom.”

This last accusation (taken directly from a press release by the Chicago Computer Fraud and Abuse Task Force) sounds particularly farfetched. One might conclude at this point that investigators would have been well advised to go ahead and “shift their focus” from the Legion of Doom. Maybe they *should* concentrate on “those other hackers”—the ones who were actually stealing money and physical objects.

But the Hacker Crackdown of 1990 was not a simple policing action. It wasn't meant just to walk the beat in cyberspace—it was a *crackdown*, a deliberate attempt to nail the core of the operation, to send a dire and potent message that would settle the hash of the digital underground for good.

By this reasoning, Fry Guy wasn't much more than the electronic equivalent of a cheap streetcorner dope dealer. As long as the masterminds of LoD were still flagrantly operating, pushing their mountains of illicit knowledge right and left and whipping up enthusiasm for blatant lawbreaking, then there would be an *infinite supply* of Fry Guys.

Because LoD was flagrant, it had left trails everywhere, to be picked up by law enforcement in New York, Indiana, Florida, Texas, Arizona, Missouri, even Australia. But 1990's war on the Legion of Doom was led out of Illinois, by the Chicago Computer Fraud and Abuse Task Force.

The Computer Fraud and Abuse Task Force, led by federal prosecutor William J. Cook, had started in 1987 and had swiftly become one of the most aggressive local "dedicated computer-crime units." Chicago was a natural home for such a group. The world's first computer bulletin board system had been invented in Illinois. The state had some of the nation's first and sternest computer crime laws. Illinois State Police were markedly alert to the possibilities of white-collar crime and electronic fraud.

And William J. Cook in particular was a rising star in electronic crime-busting. He and his fellow federal prosecutors at the U.S. Attorney's office in Chicago had a tight relation with the Secret Service, especially go-getting Chicago-based agent Timothy Foley. While Cook and his Department of Justice colleagues plotted strategy, Foley was their man on the street.

Throughout the 1980s, the federal government had given prosecutors an armory of new, untried legal tools against computer crime. Cook and his colleagues were pioneers in the use of these new statutes in the real-life cut-and-thrust of the federal courtroom.

On October 2, 1986, the U.S. Senate had passed the Computer Fraud and Abuse Act unanimously, but there had been pitifully few convictions under this statute. Cook's group took its name from this statute, because it was determined to transform this powerful but rather theoretical act of Congress into a real-life engine of legal destruction against computer fraudsters and scoff-laws.

It was not a question of merely discovering crimes, investigating them, and then trying and punishing their perpetrators. The Chicago unit, like most everyone else in the business, already *knew* who the bad guys were: the Legion of Doom and the writers and editors of *Phrack*. The task at hand was to find some legal means of putting these characters away.

This approach might seem a bit dubious to someone not acquainted with the gritty realities of prosecutorial work. But prosecutors don't put people in jail for crimes they have committed; they put people in jail for crimes they have committed *that can be proved in court*. Chicago federal police put Al Capone in prison for income-tax fraud. Chicago is a big town, with a rough-and-ready bare-knuckle tradition on both sides of the law.

Fry Guy had broken the case wide open and alerted telco security to the scope of the problem. But Fry Guy's crimes would not put the Atlanta Three behind bars—much less the wacko underground journalists of *Phrack*. So on July 22, 1989, the same day that Fry Guy was raided in Indiana, the Secret Service descended upon the Atlanta Three.

Likely this was inevitable. By the summer of 1989, law enforcement was closing in on the Atlanta Three from at least six directions at once. First, there were the leads from Fry Guy, which had led to the DNR registers being installed on the lines of the Three. The DNR evidence alone would have finished them off, sooner or later.

But second, the Atlanta lads were already well known to Control-C and his telco security sponsors. LoD's contacts with telco security had made its members overconfident and even more boastful than usual; they felt that they had powerful friends in

high places and that they were being tolerated openly by telco security. But BellSouth's Intrusion Task Force was hot on the trail of LoD and sparing no effort or expense.

The Atlanta Three had also been identified by name and listed on the extensive antihacker files maintained, and retailed for pay, by private security operative John Maxfield of Detroit. Maxfield, who had extensive ties to telco security and many informants in the underground, was a *bête noire* of the *Phrack* crowd, and the dislike was mutual.

The Atlanta Three themselves had written articles for *Phrack*. This boastful act could not possibly escape telco and law enforcement attention.

“Knightmare,” a high school-age hacker from Arizona, was a close friend and disciple of Atlanta LoD, but he had been nabbed by the formidable Arizona Organized Crime and Racketeering Unit. Knightmare was on some of LoD’s favorite boards—Black Ice in particular—and was privy to their secrets. And to have Gail Thackeray, the assistant attorney general of Arizona, on one’s trail was a dreadful peril for any hacker.

And perhaps worst of all, Prophet had committed a major blunder by passing an illicitly copied BellSouth computer file to Knight Lightning, who had published it in *Phrack*. This, as we will see, was an act of dire consequence for almost everyone concerned.

On July 22, 1989, the Secret Service showed up at Leftist's house, where he lived with his parents. A massive squad of some twenty officers surrounded the building: Secret Service, federal marshals, local police, possibly BellSouth telco security; it was hard to tell in the crush. Leftist's dad, at work in his basement office, first noticed a muscular stranger in plain clothes crashing through the backyard with a drawn pistol. As more strangers poured into the house, Leftist's dad naturally assumed there was an armed robbery in progress.

Like most hacker parents, Leftist's mom and dad had only the vaguest notions of what their son had been up to all this time. Leftist had a day job repairing computer hardware. His obsession

with computers seemed a bit odd, but harmless enough, and likely to produce a well-paying career. The sudden, overwhelming raid left Leftist's parents traumatized.

Leftist himself had been out after work with his co-workers, surrounding a couple of pitchers of margaritas. As he came trucking on tequila-numbered feet up the pavement, toting a bag full of floppy disks, he noticed a large number of unmarked cars parked in his driveway. All the cars sported tiny microwave antennas.

The Secret Service had knocked the front door off its hinges, almost flattening his mom.

Inside, Leftist was greeted by Special Agent James Cool of the U.S. Secret Service, Atlanta office. Leftist was flabbergasted. He'd never met a Secret Service agent before. He could not imagine that he'd ever done anything worthy of federal attention. He'd always figured that if his activities became intolerable, one of his contacts in telco security would give him a private phone call and tell him to knock it off.

But now Leftist was pat-searched for weapons by grim professionals, and his bag of floppies was quickly seized. He and his parents were all shepherded into separate rooms and grilled at length as a score of officers scoured their home for anything electronic.

Leftist was horrified as his treasured IBM AT personal computer with its forty-meg hard disk and his recently purchased 80386 IBM clone with a whopping hundred-meg hard disk both went swiftly out the door in Secret Service custody. They also seized all his disks, all his notebooks, and a tremendous booty in dog-eared telco documents that Leftist had snatched from trash dumpsters.

Leftist figured the whole thing for a big misunderstanding. He'd never been into *military* computers. He wasn't a *spy* or a

Like most hacker parents, Leftist's mom and dad had only the vaguest notions of what their son had been up to.

Communist. He was just a good ol' Georgia hacker, and now he just wanted all these people out of the house. But it seemed they wouldn't go until he made some kind of statement.

And so, he leveled with them.

And that, Leftist said later from his federal prison camp in Talladega, Alabama, was a big mistake.

The Atlanta area was unique, in that it had three members of the Legion of Doom who actually occupied more or less the same physical locality. Unlike the rest of LoD, who tended to associate by phone and computer, Atlanta LoD actually *were* "tightly knit." It was no real surprise that the Secret Service agents apprehending Urvile at the computer labs at Georgia Tech would discover Prophet with him as well.

Urvile, a twenty-one-year-old Georgia Tech student in polymer chemistry, posed quite a puzzling case for law enforcement. Urvile—also known as "Necron 99," as well as other handles, for he tended to change his cover alias about once a month—was both an accomplished hacker and a fanatic simulation-gamer.

Simulation games are an unusual hobby; but then hackers are unusual people, and their favorite pastimes tend to be somewhat out of the ordinary. The best-known American simulation game is probably *Dungeons & Dragons*, a multiplayer parlor entertainment played with paper, maps, pencils, statistical tables, and a variety of oddly shaped dice. Players pretend to be heroic characters exploring a wholly invented fantasy world. The fantasy worlds of simulation gaming are commonly pseudomedieval, involving swords and sorcery—spell-casting wizards, knights in armor, unicorns and dragons, demons and goblins.

Urvile and his fellow gamers preferred their fantasies highly technological. They made use of a game known as "GURPS," the "Generic Universal Role Playing System," published by a company called Steve Jackson Games (SJG).

GURPS served as a framework for creating a wide variety of artificial fantasy worlds. Steve Jackson Games published a smorgasboard of books, full of detailed information and gaming hints,

which were used to flesh-out many different fantastic backgrounds for the basic GURPS framework. Urvile made extensive use of two SJG books called *GURPS High-Tech* and *GURPS Special Ops*.

In the artificial fantasy world of *GURPS Special Ops*, players entered a modern fantasy of intrigue and international espionage. On beginning the game, players started small and powerless, perhaps as minor-league CIA agents or penny-ante arms dealers. But as players persisted through a series of game sessions (which generally lasted for hours, over long, elaborate campaigns that might be pursued for months on end), they would achieve new skills, new knowledge, new power. They would acquire and hone new abilities, such as marksmanship, karate, wiretapping, or Watergate burglary. They could also win various kinds of imaginary booty, such as Berettas, or martini shakers, or fast cars with ejection seats and machine guns under the headlights.

As might be imagined from the complexity of these games, Urvile's gaming notes were very detailed and extensive. Urvile was a "dungeonmaster," inventing scenarios for his fellow gamers, giant simulated adventure-puzzles for his friends to unravel. Urvile's game notes covered dozens of pages with all sorts of exotic lunacy, all about ninja raids on Libya and break-ins on encrypted Red Chinese supercomputers. His notes were written on scrap paper and kept in loose-leaf binders.

The handiest scrap paper around Urvile's college digs were the many pounds of BellSouth printouts and documents that he had snatched out of telco dumpsters. His notes were written on the back of misappropriated telco property. Worse yet, the gaming notes were interspersed chaotically with Urvile's hand-scrawled records involving *actual computer intrusions* that he had committed.

Not only was it next to impossible to tell Urvile's fantasy game notes from cyberspace "reality," but Urvile himself barely made this distinction. It's no exaggeration to say that to Urvile it was *all* a game. Urvile was very bright, highly imaginative, and quite

careless of other people's notions of propriety. His connection to "reality" was not something to which he paid a great deal of attention.

Hacking was a game for Urvile. It was an amusement he was carrying out, it was something he was doing for fun. And Urvile was an obsessive young man. He could no more stop hacking than he could stop in the middle of a jigsaw puzzle, or stop in the middle of reading a Stephen Donaldson fantasy trilogy. (The name “Urvile” came from a best-selling Donaldson novel.)

Urvile's airy, bulletproof attitude seriously annoyed his interrogators. First of all, he didn't consider that he'd done anything wrong. There was scarcely a shred of honest remorse in him. On the contrary, he seemed privately convinced that his police interrogators were operating in a demented fantasy world all their own. Urvile was too polite and well behaved to say this straight out, but his reactions were askew and disquieting.

For instance, there was the business about LoD's ability to monitor phone calls to the police and Secret Service. Urvile agreed that this was quite possible and posed no big problem for LoD. In fact, he and his friends had kicked the idea around on the Black Ice board, much as they had discussed many other nifty notions, such as building personal flamethrowers and jury-rigging fistsful of blasting caps. They had hundreds of dial-up numbers for government agencies that they'd gotten through scanning Atlanta phones or had pulled from raided VAX/VMS mainframe computers.

Basically, they'd never gotten around to listening in on the cops because the idea wasn't interesting enough to bother with. Besides, if they'd been monitoring Secret Service phone calls, obviously they'd never have been caught in the first place. Right?

The Secret Service was less than satisfied with this rapierlike hacker logic.

Then there was the issue of crashing the phone system. No problem, Urvile admitted sunnily. Atlanta LoD could have shut down phone service all over Atlanta any time it liked. *Even the*

911 service? Nothing special about that, Urvile explained patiently. Bring the switch to its knees, with say the UNIX "makedir" bug, and 911 goes down too as a matter of course. The 911 system wasn't very interesting, frankly. It might be tremendously interesting to cops (for odd reasons of their own), but as technical challenges went, the 911 service was yawnsville.

So of course the Atlanta Three could crash service. They probably could have crashed service all over BellSouth territory, if they'd worked at it for a while. But Atlanta LoD weren't crashers. Only losers and rodents were crashers. LoD were *elite*.

Urvile privately was convinced that sheer technical expertise could win him free of any kind of problem. As far as he was concerned, elite status in the digital underground had placed him permanently beyond the intellectual grasp of cops and straights. Urvile had a lot to learn.

Of the three LoD stalwarts, Prophet was in the most direct trouble. Prophet was a UNIX programming expert who burrowed in and out of the Internet as a matter of course. He'd started his hacking career at around age fourteen, meddling with a UNIX mainframe system at the University of North Carolina.

Prophet himself had written the handy Legion of Doom file "UNIX Use and Security From the Ground Up." UNIX (pronounced "you-nicks") is a powerful, flexible computer operating system for multiuser, multitasking computers. In 1969, when UNIX was created in Bell Labs, such computers were exclusive to large corporations and universities, but today UNIX is run on thousands of powerful home machines. UNIX was particularly well suited to telecommunications programming and had become a standard in the field. Naturally, UNIX also became a standard for the elite hacker and phone phreak.

Lately Prophet had not been so active as Leftist and Urvile, but Prophet was a recidivist. In 1986, when he was eighteen, Prophet had been convicted of "unauthorized access to a computer network" in North Carolina. He'd been discovered breaking into the Southern Bell Data Network, a UNIX-based internal

telco network supposedly closed to the public. He'd gotten a typical hacker sentence: six months suspended, 120 hours community service, and three years' probation.

After that humiliating bust, Prophet had gotten rid of most of his tonnage of illicit phreak and hacker data and had tried to go straight. He was, after all, still on probation. But by the autumn of 1988, the temptations of cyberspace had proved too much for young Prophet, and he was shoulder to shoulder with Urvile and Leftist into some of the hairiest systems around.

In early September 1988, he'd broken into BellSouth's centralized automation system, AIMSX, or "Advanced Information Management System." AIMSX was an internal business network for BellSouth, where telco employees stored electronic mail, databases, memos, and calendars, and did text processing. Because AIMSX did not have public dial-ups, it was considered utterly invisible to the public and was not well secured—it didn't even require passwords. Prophet abused an account known as "waal," the personal account of an unsuspecting telco employee. Disguised as the owner of waal, Prophet made about ten visits to AIMSX.

Prophet did not damage or delete anything in the system. His presence in AIMSX was harmless and almost invisible. But he could not rest content with that.

One particular piece of processed text on AIMSX was a telco document known as "Bell South Standard Practice 660-225-104SV Control Office Administration of Enhanced 911 Services for Special Services and Major Account Centers dated March 1988."

Prophet had not been looking for this document. It was merely one among hundreds of similar documents with impenetrable titles. However, having blundered over it in the course of his illicit wanderings through AIMSX, he decided to take it with him as a trophy. It might prove very useful in some future boasting, bragging, and strutting session. So, some time in September 1988, Prophet ordered the AIMSX mainframe computer to copy

this document (henceforth called simply “the E911 Document”) and to transfer this copy to his home computer.

No one noticed that Prophet had done this. He had “stolen” the E911 Document in some sense, but notions of property in cyberspace can be tricky. BellSouth noticed nothing

Prophet decided to take the E911 Document with him as a trophy.

wrong, because BellSouth still had its original copy. It had not been “robbed” of the document itself. Many people were supposed to copy this document—specifically, people who worked for the nineteen BellSouth “special services and major account centers,” scattered throughout the southeastern United States. That was what it was for, why it was present on a computer network in the first place: so that it could be copied and read—by telco employees. But now the data had been copied by someone who wasn’t supposed to look at it.

Prophet now had his trophy. But he further decided to store yet another copy of the E911 Document on another person’s computer. This unwitting person was a computer enthusiast named Richard Andrews who lived near Joliet, Illinois. Richard Andrews was a UNIX programmer by trade, and ran a powerful UNIX board called Jolnet, in the basement of his house.

Prophet, using the handle “Robert Johnson,” had obtained an account on Richard Andrews’ computer. And there he stashed the E911 Document, by storing it in his own private section of Andrews’ computer.

Why did Prophet do this? If he had eliminated the E911 Document from his own computer and kept it hundreds of miles away, on another machine, under an alias, then he might have been fairly safe from discovery and prosecution—although his sneaky action had certainly put the unsuspecting Richard Andrews at risk.

But, like most hackers, Prophet was a packrat for illicit data. When it came to the crunch, he could not bear to part with his

trophy. When Prophet's place in Decatur, Georgia, was raided in July 1989, there was the E911 Document, a smoking gun. And there was Prophet in the hands of the Secret Service, doing his best to "explain."

Our story now takes us away from the raids of the summer of 1989, leaving the Atlanta Three "cooperating fully" with their numerous investigators. And they did cooperate, as their sentencing memorandum from the U.S. District Court of the Northern Division of Georgia explained—just before all three of them were sentenced to various federal prisons in November 1990.

We must now catch up on the other aspects of the war on the Legion of Doom. It was a war on a network—in fact, a network of three networks, which intertwined and interrelated in a complex fashion. The Legion itself, with Atlanta LoD, and its hanger-on Fry Guy, was the first. The second was *Phrack* magazine, with its editors and contributors.

The third network involved the electronic circle around a hacker known as "Terminus."

The war against these hacker networks was carried out by a law enforcement network. Atlanta LoD and Fry Guy were pursued by U.S. Secret Service agents and federal prosecutors in Atlanta, Indiana, and Chicago. Terminus found himself pursued by the Secret Service and federal prosecutors from Baltimore and Chicago. And the war against *Phrack* was almost entirely a Chicago operation.

The investigation of Terminus involved a great deal of energy, mostly from the Chicago Task Force, but it was to be the least known and least publicized of the crackdown operations. Terminus, who lived in Maryland, was a UNIX programmer and consultant, fairly well known (under his given name) in the UNIX community, as an acknowledged expert on AT&T minicomputers. Terminus idolized AT&T, especially Bellcore, and longed for public recognition as a UNIX maven; his highest ambition was to work for Bell Labs.

But Terminus had odd friends and a spotted history. He had once been the subject of an admiring interview in *Phrack* (Vol-

ume II, Issue 14, Phile 2—dated May 1987). In this article, *Phrack* co-editor Taran King described Terminus as an electronics engineer, five foot nine inches tall, brown-haired, born in 1959—at twenty-eight years old, quite mature for a hacker.

Terminus had once been sysop of a phreak/hack underground board called MetroNet, which ran on an Apple II. Later he'd replaced MetroNet with an underground board called MegaNet, specializing in IBMs. In his younger days, Terminus had written one of the very first and most elegant code-scanning programs for the IBM-PC. This program had been distributed widely in the underground. Uncounted legions of PC-owning phreaks and hackers had used Terminus' scanner program to rip off telco codes. This feat had not escaped the attention of telco security; it hardly could, because Terminus' earlier handle, "Terminal Technician," was proudly written right on the program.

When he became a full-time computer professional (specializing in telecommunications programming), he adopted the handle Terminus, meant to indicate that he had "reached the final point of being a proficient hacker." He'd moved up to the UNIX-based Netsys board on an AT&T computer, with four phone lines and an impressive 240 megs of storage. Netsys carried complete issues of *Phrack*, and Terminus was quite friendly with its publishers, Taran King and Knight Lightning.

In the early 1980s, Terminus had been a regular on Plovernet, Pirate-80, Sherwood Forest, and Shadowland, all well-known pirate boards, all heavily frequented by the Legion of Doom. As it happened, Terminus was never officially "in LoD," because he'd never been given the official LoD high sign and back slap by Legion maven Lex Luthor. Terminus had never physically met anyone from LoD. But that scarcely mattered much—the Atlanta Three themselves had never been officially vetted by Lex either.

As far as law enforcement was concerned, the issues were clear. Terminus was a full-time, adult computer professional with particular skills at AT&T software and hardware—but Terminus reeked of the Legion of Doom and the underground.

On February 1, 1990—half a month after the Martin Luther

King Day Crash—U.S. Secret Service agents Tim Foley from Chicago and Jack Lewis from the Baltimore office, accompanied by AT&T security officer Jerry Dalton, traveled to Middletown, Maryland. There they grilled Terminus in his home (to the stark terror of his wife and small children) and, in their customary fashion, hauled his computers out the door.

The Netsys machine proved to contain a plethora of arcane UNIX software—proprietary source code formally owned by AT&T. Software such as: UNIX System Five Release 3.2; UNIX SV Release 3.1; UUCP communications software; KORN SHELL; RFS; IWB; WWB; DWB; the C++ programming language; PMON; TOOL CHEST; QUEST; DACT; and S FIND.

In the long-established piratical tradition of the underground, Terminus had been trading this illicitly copied software with a small circle of fellow UNIX programmers. Very unwisely, he had stored seven years of his electronic mail on his Netsys machine, which documented all the friendly arrangements he had made with his various colleagues.

Terminus had not crashed the AT&T phone system on January 15. He was, however, blithely running a not-for-profit AT&T software-piracy ring. This was not an activity AT&T found amusing. AT&T security officer Jerry Dalton valued this “stolen” property at over \$300,000.

AT&T's entry into the tussle of free enterprise had been complicated by the new, vague ground rules of the information economy. Until the breakup of Ma Bell, AT&T was forbidden to sell computer hardware or software. Ma Bell was the phone company; Ma Bell was not allowed to use the enormous revenue from telephone utilities in order to finance any entry into the computer market.

AT&T nevertheless invented the UNIX language. And somehow AT&T managed to make UNIX a minor source of income. Weirdly, UNIX was not sold as computer software, but actually retailed under an obscure regulatory exemption allowing sales of surplus equipment and scrap. Any bolder attempt to promote or retail UNIX would have aroused angry legal opposition from com-

puter companies. Instead, UNIX was licensed to universities, at modest rates, where the acids of academic freedom ate away steadily at AT&T's proprietary rights.

Come the breakup, AT&T recognized that UNIX was a potential goldmine. By now, large chunks of UNIX code had been created that were not AT&T's and were being sold by others. An entire rival UNIX-based operating system had arisen in Berkeley, California (one of the world's great founts of ideological hackerdom). Today, hackers commonly consider Berkeley UNIX to be technically superior to AT&T's System V UNIX, but AT&T has not allowed mere technical elegance to intrude on the real-world business of marketing proprietary software. AT&T has made its own code deliberately incompatible with other folks' UNIX and has written code that it can prove is copyrightable, even if that code happens to be somewhat awkward—"kludgey." AT&T UNIX user licenses are serious business agreements, replete with very clear copyright statements and nondisclosure clauses.

AT&T has not exactly kept the UNIX cat in the bag, but it kept a grip on its scruff with some success. By the rampant, explosive standards of software piracy, AT&T UNIX source code is heavily copyrighted, well guarded, well licensed. Traditionally UNIX was run only on mainframe machines, owned by large groups of suit-and-tie professionals, rather than on bedroom machines where people can get up to easy mischief.

And AT&T UNIX source code is serious high-level programming. The number of skilled UNIX programmers with any actual motive to swipe UNIX source code is small. It's tiny, compared to the tens of thousands prepared to rip off, say, entertaining PC games such as "Leisure Suit Larry."

But by 1989, the warez-d00d underground, in the persons of Terminus and his friends, was gnawing at AT&T UNIX. And the property in question was not sold for twenty bucks over the counter at the local branch of Babbage's or Egghead's; this was massive, sophisticated, multiline, multiauthor corporate code worth tens of thousands of dollars.

It must be recognized at this point that Terminus' purported

ring of UNIX software pirates had not actually made any money from their suspected crimes. The \$300,000 figure bandied about for the contents of Terminus' computer did not mean that Terminus was in actual illicit possession of three hundred thousand of AT&T's dollars. Terminus was shipping software back and forth, privately, person to person, for free. He was not making a commercial business of piracy. He hadn't asked for money; he didn't take money. He lived quite modestly.

They were humble digital drudges, wandering with mop and bucket through the Great Technological Temple of AT&T.

AT&T employees—as well as freelance UNIX consultants, such as Terminus—commonly worked with “proprietary” AT&T software, both in the office and at home on their private machines. AT&T rarely sent security officers out to comb the hard disks of its con-

sultants. Cheap freelance UNIX contractors were quite useful to AT&T; they didn't have health insurance or retirement programs, much less union membership in the Communication Workers of America. They were humble digital drudges, wandering with mop and bucket through the Great Technological Temple of AT&T; but when the Secret Service arrived at their homes, it seemed they were eating with company silverware and sleeping on company sheets! Outrageously, they behaved as if the things they worked with every day belonged to them!

And these were no mere hacker teenagers with their hands full of trash paper and their noses pressed to the corporate windowpane. These guys were UNIX wizards, not only carrying AT&T data in their machines and their heads, but eagerly networking about it, over machines that were far more powerful than anything previously imagined in private hands. How do you keep people disposable, yet assure their awestruck respect for your property? It was a dilemma.

Much UNIX code was public domain, available for free. Much “proprietary” UNIX code had been extensively rewritten, perhaps

altered so much that it became an entirely new product—or perhaps not. Intellectual property rights for software developers were, and are, extraordinarily complex and confused. And software “piracy,” like the private copying of videos, is one of the most widely practiced “crimes” in the world today.

The U.S. Secret Service was not expert in UNIX or familiar with the customs of its use. The USSS, considered as a body, did not have one single person in it who could program in a UNIX environment—no, not even one. The Secret Service was making extensive use of expert help, but the “experts” it had chosen were AT&T and Bellcore security officials, the very victims of the purported crimes under investigation, the very people whose interest in AT&T’s “proprietary” software was most pronounced.

On February 6, 1990, Terminus was arrested by Agent Lewis. Eventually Terminus would be sent to prison for his illicit use of a piece of AT&T software.

The issue of pirated AT&T software would bubble along in the background during the war on the Legion of Doom. Some half-dozen of Terminus’ on-line acquaintances, including people in Illinois, Texas, and California, were grilled by the Secret Service in connection with the illicit copying of software. Except for Terminus, however, none was charged with a crime. None of them shared his peculiar prominence in the hacker underground.

But that did not mean that these people would, or could, stay out of trouble. The transferral of illicit data in cyberspace is hazy and ill-defined business, with paradoxical dangers for everyone concerned: hackers, signal carriers, board owners, cops, prosecutors, even random passersby. Sometimes well-meant attempts to avert trouble or punish wrongdoing bring more trouble than would simple ignorance, indifference, or impropriety.

Terminus’ Netsys board was not a common-or-garden bulletin board system, though it had most of the usual functions of a board. Netsys was not a stand-alone machine, but part of the globe-spanning UUCP cooperative network. The UUCP network uses a set of UNIX software programs called “UNIX-to-UNIX Copy,” which allows UNIX systems to throw data to one another

at high speed through the public telephone network. UUCP is a radically decentralized, not-for-profit network of UNIX computers. There are tens of thousands of these UNIX machines. Some are small, but many are powerful and also link to other networks. UUCP has certain arcane links to major networks such as JANET, EasyNet, BITNET, JUNET, VNET, DASnet, PeaceNet, and FidoNet, as well as the gigantic Internet. (The so-called Internet is not actually a network itself but rather an "internetwork" connections standard that allows several globe-spanning computer networks to communicate with one another. Readers fascinated by the weird and intricate tangles of modern computer networks may enjoy John S. Quarterman's authoritative 719-page explication, *The Matrix*, Digital Press, 1990.)

A skilled user of Terminus' UNIX machine could send and receive electronic mail from almost any major computer network in the world. Netsys was not called a "board" per se, but rather a "node." Nodes were larger, faster, and more sophisticated than mere boards, and for hackers, to hang out on internationally connected nodes was quite the step up from merely hanging out on local boards.

Terminus' Netsys node in Maryland had a number of direct links to other, similar UUCP nodes, run by people who shared his interests and at least something of his free-wheeling attitude. One of these nodes was Jolnet, owned by Richard Andrews, who, like Terminus, was an independent UNIX consultant. Jolnet also ran UNIX and could be contacted at high speed by mainframe machines from all over the world. Jolnet was quite a sophisticated piece of work, technically speaking, but it was still run by an individual, as a private, not-for-profit hobby. Jolnet was used mostly by other UNIX programmers—for mail, storage, and access to networks. Jolnet supplied network access to about two hundred people as well as a local junior college.

Among its various features and services, Jolnet also carried *Phrack* magazine.

For reasons of his own, Richard Andrews had become suspicious of a new user called "Robert Johnson." Andrews took it

upon himself to have a look at what "Robert Johnson" was storing in Jolnet. And Andrews found the E911 Document.

"Robert Johnson" was Prophet from the Legion of Doom, and the E911 Document was illicitly copied data from Prophet's raid on the BellSouth computers.

The E911 Document, a particularly illicit piece of digital property, was about to resume its long, complex, and disastrous career.

It struck Andrews as fishy that someone not a telephone employee should have a document referring to the Enhanced 911 System. Besides, the document itself bore an obvious warning.

**WARNING: NOT FOR USE OR DISCLOSURE OUTSIDE
BELLSOUTH OR ANY OF ITS SUBSIDIARIES EXCEPT
UNDER WRITTEN AGREEMENT.**

These standard nondisclosure tags are often appended to all sorts of corporate material. Telcos as a species are particularly notorious for stamping most everything in sight as "not for use or disclosure." Still, this particular piece of data was about the 911 System. That sounded bad to Rich Andrews.

Andrews was not prepared to ignore this sort of trouble. He thought it would be wise to pass the document along to a friend and acquaintance on the UNIX network, for consultation. So, around September 1988, Andrews sent yet another copy of the E911 Document electronically to an AT&T employee, one Charles Boykin, who ran a UNIX-based node called "attctc" in Dallas, Texas.

Attctc was the property of AT&T and was run from AT&T's Customer Technology Center in Dallas, hence the name "attctc." Attctc was better known as "Killer," the name of the machine that the system was running on. Killer was a hefty, powerful, AT&T 3B2 500 model, a multiuser, multitasking UNIX platform with 32 meg of memory and a mind-boggling 3.2 Gigabytes of storage. When Killer had first arrived in Texas, in 1985, the 3B2

had been one of AT&T's great white hopes for going head-to-head with IBM for the corporate computer-hardware market. Killer had been shipped to the Customer Technology Center in the Dallas Infomart, essentially a high-technology mall, and there it sat, a demonstration model.

Charles Boykin, a veteran AT&T hardware and digital communications expert, was a local technical backup man for the AT&T 3B2 system. As a display model in the Infomart mall, Killer had little to do, and it seemed a shame to waste the system's capacity. So Boykin ingeniously wrote some UNIX bulletin board software for Killer and plugged the machine in to the local phone network. Killer's debut in late 1985 made it the first publicly available UNIX site in the state of Texas. Anyone who wanted to play was welcome.

The machine immediately attracted an electronic community. It joined the UUCP network and offered network links to over eighty other computer sites, all of which became dependent on Killer for their links to the greater world of cyberspace. And it wasn't just for the big guys; personal computer users also stored freeware programs for the Amiga, the Apple, the IBM, and the Macintosh on Killer's vast 3,200 meg archives. At one time, Killer had the largest library of public-domain Macintosh software in Texas.

Eventually, Killer attracted about 1,500 users, all busily communicating, uploading and downloading, getting mail, gossiping, and linking to arcane and distant networks.

Boykin received no pay for running Killer. He considered it good publicity for the AT&T 3B2 system (whose sales were somewhat less than stellar), but he also simply enjoyed the vibrant community his skill had created. He gave away the bulletin board UNIX software he had written, free of charge.

In the UNIX programming community, Charlie Boykin had the reputation of a warm, open-hearted, level-headed kind of guy. In 1989, a group of Texan UNIX professionals voted Boykin "System Administrator of the Year." He was considered a fellow you could trust for good advice.

In September 1988, without warning, the E911 Document came plunging into Boykin's life, forwarded by Richard Andrews. Boykin immediately recognized that the document was hot property. He was not a voice-communications man and knew little about the ins and outs of the Baby Bells, but he certainly knew what the 911 System was, and he was angry to see confidential data about it in the hands of a nogoodnik. This was clearly a matter for telco security. So, on September 21, 1988, Boykin made yet *another* copy of the E911 Document and passed this one along to a professional acquaintance of his, one Jerome Dalton, from AT&T Corporate Information Security. Jerry Dalton was the very fellow who would later raid Terminus' house.

From AT&T's security division, the E911 Document went to Bellcore.

Bellcore (or BELL COmmunications REsearch) had once been the central laboratory of the Bell System. Bell Labs employees had invented the UNIX programming language. Now Bellcore was a quasi-independent, jointly owned company that acted as the research arm for all seven of the Baby Bell RBOCs. Bellcore was in a good

Kluepfel recognized the document for what it was: a trophy from a hacker break-in.

position to coordinate security technology and consultation for the RBOCs, and the gentleman in charge of this effort was Henry M. Kluepfel, a veteran of the Bell System who had worked there for twenty-four years.

On October 13, 1988, Dalton passed the E911 Document to Henry Kluepfel. Kluepfel, a veteran expert witness in telecommunications fraud and computer-fraud cases, had certainly seen worse trouble than this. He recognized the document for what it was: a trophy from a hacker break-in.

However, whatever harm had been done in the intrusion was presumably old news. At this point Kluepfel apparently decided there was little to be done. He made a careful note of the circumstances and shelved the problem for the time being.

Whole months passed.

February 1989 arrived. The Atlanta Three were living it up in Bell South's switches and had not yet met their comeuppance. The Legion was thriving. So was *Phrack* magazine. A good six months had passed since Prophet's AIMSX break-in. Prophet, as hackers will, grew weary of sitting on his laurels. Knight Lightning and Taran King, the editors of *Phrack*, were always begging him for material they could publish. Prophet decided that the heat must be off by this time, and that he could safely brag, boast, and strut.

So he sent a copy of the E911 Document—yet another one—from Rich Andrews' Jolnet machine to Knight Lightning's BITNET account at the University of Missouri.

Let's review the fate of the Document so far.

0. The original E911 Document. This in the AIMSX system on a mainframe computer in Atlanta, available to hundreds of people, but all of them, presumably, BellSouth employees. An unknown number of them may have their own copies of this document, but they are all professionals and all trusted by the phone company.
1. Prophet's illicit copy, at home on his own computer in Decatur, Georgia.
2. Prophet's backup copy, stored on Rich Andrews' Jolnet machine in the basement of Andrews' house near Joliet, Illinois.
3. Charles Boykin's copy on Killer in Dallas, Texas, sent by Rich Andrews from Joliet.
4. Jerry Dalton's copy at AT&T Corporate Information Security in New Jersey, sent by Boykin from Dallas.
5. Henry Kluepfel's copy at Bellcore security headquarters in New Jersey, sent by Dalton.
6. Knight Lightning's copy, sent by Prophet from Rich Andrews' machine, and now in Columbia, Missouri.

We can see that the “security” situation of this proprietary document, once dug out of AIMSX, swiftly became bizarre. Without any money changing hands, without any particular special effort, these data had been reproduced at least six times and had spread itself all over the continent. By far the worst, however, was yet to come.

In February 1989, Prophet and Knight Lightning bargained electronically over the fate of this trophy. Prophet wanted to boast but, at the same time, scarcely wanted to be caught.

For his part, Knight Lightning was eager to publish as much of the document as he could manage. Knight Lightning was a fledgling political science major with a particular interest in freedom-of-information issues. He would gladly publish almost anything that would reflect glory on the prowess of the underground and embarrass the telcos. However, Knight Lightning himself had contacts in telco security, and sometimes consulted them on material he’d received that might be too dicey for publication.

Prophet and Knight Lightning decided to edit the E911 Document so as to delete most of its identifying traits. First of all, its large NOT FOR USE OR DISCLOSURE warning had to go. Then there were other matters. For instance, it listed the office telephone numbers of several BellSouth 911 specialists in Florida. If these phone numbers were published in *Phrack*, the BellSouth employees involved would very likely be hassled by phone phreaks, which would anger BellSouth no end and pose a definite operational hazard for both Prophet and *Phrack*.

So Knight Lightning cut the Document almost in half, removing the phone numbers and some of the touchier and more specific information. He passed it back electronically to Prophet; Prophet was still nervous, so Knight Lightning cut a bit more. They finally agreed that it was ready to go and that it would be published in *Phrack* under the pseudonym “The Eavesdropper.”

And this was done on February 25, 1989.

The twenty-fourth issue of *Phrack* featured a chatty interview with coed phone-phreak “Chanda Leir,” three articles on

BITNET and its links to other computer networks, an article on 800 and 900 numbers by "Unknown User," "VaxCat's" article on telco basics (slyly entitled "Lifting Ma Bell's Veil of Secrecy,") and the usual "Phrack World News."

The News section, with painful irony, featured an extended account of the sentencing of "Shadowhawk," an eighteen-year-old Chicago hacker who had just been put in federal prison by William J. Cook himself.

And then there were the two articles by The Eavesdropper. The first was the heavily edited E911 Document, now titled "Control Office Administration Of Enhanced 911 Services for Special Services and Major Account Centers." Eavesdropper's second article was a glossary of terms explaining the blizzard of telco acronyms and buzzwords in the E911 Document.

The hapless document was now distributed, in the usual *Phrack* routine, to a good 150 sites. Not 150 *people*, mind you—150 *sites*, some of them linked to UNIX nodes or bulletin board systems, which themselves had readerships of tens, dozens, even hundreds of people.

This was February 1989. Nothing happened immediately. Summer came, and the Atlanta crew was raided by the Secret Service. Fry Guy was apprehended. Still nothing whatever happened to *Phrack*. Six more issues of *Phrack* came out, thirty in all, more or less on a monthly schedule. Knight Lightning and co-editor Taran King went untouched.

Phrack tended to duck and cover whenever the heat came down. During the summer busts of 1987 (hacker busts tended to cluster in summer, perhaps because hackers were easier to find at home than in college), *Phrack* had ceased publication for several months and laid low. Several LoD hangers-on had been arrested, but nothing had happened to the *Phrack* crew, the premier gossips of the underground. In 1988, *Phrack* had been taken over by a new editor, "Crimson Death," a raucous youngster with a taste for anarchy files.

The year 1989, however, looked like a bounty year for the underground. Knight Lightning and co-editor Taran King took up

the reins again, and *Phrack* flourished. Atlanta LoD went down hard in the summer of 1989, but *Phrack* rolled merrily on. Prophet's E911 Document seemed unlikely to cause *Phrack* any trouble. By January 1990, it had been available in *Phrack* for almost a year. Kluepfel and Dalton, officers of Bellcore and AT&T security, had possessed the document for sixteen months—in fact, they'd had it even before Knight Lightning himself and had done nothing in particular to stop its distribution. They hadn't even told Rich Andrews or Charles Boykin to erase the copies from their UNIX nodes, Jolnet and Killer.

But then came the monster Martin Luther King Day Crash of January 15, 1990.

A flat three days later, on January 18, four agents showed up at Knight Lightning's fraternity house. One was Timothy Foley, the second Barbara Golden, both of them Secret Service agents from the Chicago office. Also along was a University of Missouri security officer, and Reed Newlin, a security man from Southwestern Bell, the RBOC having jurisdiction over Missouri.

Foley accused Knight Lightning of causing the nationwide crash of the phone system.

Knight Lightning was aghast at this allegation. On the face of it, the suspicion was not entirely implausible—though Knight Lightning knew that he himself hadn't done it. Plenty of hot-dog hackers had bragged that they could crash the phone system, however. Shadowhawk, for instance, the Chicago hacker whom William Cook had recently put in jail, had several times boasted on boards that he could "shut down AT&T's public switched network."

And now this event, or something that looked just like it, had actually taken place. The crash had lit a fire under the Chicago Task Force. And the former fence-sitters at Bellcore and AT&T were now ready to roll. The consensus among telco security—already horrified by the skill of the BellSouth intruders—was that the digital underground was out of hand. LoD and *Phrack* must go.

And in publishing Prophet's E911 Document, *Phrack* had pro-

vided law enforcement with what appeared to be a powerful legal weapon.

Foley confronted Knight Lightning about the E911 Document.

Knight Lightning was cowed. He immediately began "cooperating fully" in the usual tradition of the digital underground.

Knight Lightning was grilled for four hours by Foley and his cohorts. He handed over his electronic mailing list of *Phrack* subscribers. He admitted that Prophet had passed him the E911 Document, and he admitted that he had known it was stolen booty from a hacker raid on a telephone company. Knight Lightning signed a statement to this effect and agreed, in writing, to cooperate with investigators.

Next day—January 19, 1990, a Friday—the Secret Service returned with a search warrant and thoroughly searched Knight Lightning's upstairs room in the fraternity house. Interestingly, they left him in possession of his computer, his floppy disks, and his modem. (The computer had no hard disk, and in Foley's judgment was not a store of evidence.) But this was a very minor bright spot among Knight Lightning's rapidly multiplying troubles. By this time he was in plenty of hot water, not only with federal police, prosecutors, telco investigators, and university security, but with the elders of his own campus fraternity, who were outraged to think that they had been unwittingly harboring a federal computer criminal.

On Monday the 29th, Knight Lightning was summoned to Chicago, where he was further grilled by Foley and USSS veteran agent Barbara Golden, this time with an attorney present. And on February 6, he was formally indicted by a federal grand jury.

The trial of Knight Lightning, which occurred on July 24–27, 1990, was the crucial show trial of the Hacker Crackdown. We will examine the trial at some length in Part Four of this book.

In the meantime, we must continue our dogged pursuit of the E911 Document.

It must have been clear by January 1990 that the E911 Document, in the form *Phrack* had published it back in February 1989, had gone off at the speed of light in at least 150 different direc-

tions. To attempt to put this electronic genie back in the bottle was flatly impossible.

And yet, the E911 Document was *still* stolen property, formally and legally speaking. Any electronic transference of this document, by anyone unauthorized to have it, could be interpreted as an act of wire fraud. Interstate transfer of stolen property, including electronic property, was a federal crime.

The Chicago Computer Fraud and Abuse Task Force had been assured that the E911 Document was worth a hefty sum of money. In fact, they had a precise estimate of its worth from BellSouth security personnel: \$79,449. A sum of this scale seemed to warrant vigorous prosecution. Even if the damage could not be undone, at least this large sum offered a good legal pretext for stern punishment of the thieves. It seemed likely to impress judges and juries. And it could be used in court to mop up the Legion of Doom.

The Atlanta crowd was already in the bag by the time the Chicago Task Force had gotten around to *Phrack*. But the Legion was a hydra-headed thing. In late 1989, a brand-new Legion of Doom board, Phoenix Project, had gone up in Austin, Texas. Phoenix Proj-

ect was sysoped by no less a man than the Mentor himself, ably assisted by University of Texas student and hardened Doomster "Erik Bloodaxe."

As we have seen from his *Phrack* manifesto, Mentor was a hacker zealot who regarded computer intrusion as something close to a moral duty. Phoenix Project was an ambitious effort, intended to revive the digital underground to what Mentor considered the full flower of the early 1980s. The Phoenix board would also boldly bring elite hackers face-to-face with the telco "opposition." On Phoenix, America's cleverest hackers supposedly would shame the telco squareheads out of their stick-in-the-

The Mentor was a hacker zealot who regarded computer intrusion as something close to a moral duty.

mud attitudes and perhaps convince them that the Legion of Doom elite were really an all-right crew. The premiere of Phoenix Project was heavily trumpeted by *Phrack*, and Phoenix Project carried a complete run of *Phrack* issues, including the E911 Document as *Phrack* had published it.

Phoenix Project was only one of many—possibly hundreds—of nodes and boards all over America that were in guilty possession of the E911 Document. But Phoenix was an outright, unashamed Legion of Doom board. Under Mentor's guidance, it was flaunting itself in the face of telco security personnel. Worse yet, it was actively trying to *win them over* as sympathizers for the digital underground elite. Phoenix had no cards or codes on it. Its hacker elite considered Phoenix at least technically legal. But Phoenix was a corrupting influence, where hacker anarchy was eating away like digital acid at the underbelly of corporate propriety.

The Chicago Computer Fraud and Abuse Task Force now prepared to descend upon Austin, Texas.

Oddly, not one but *two* trails of the task force's investigation led toward Austin. The city of Austin, like Atlanta, had made itself a bulwark of the Sunbelt's Information Age, with a strong university research presence and a number of cutting-edge electronics companies, including Motorola, Dell, CompuAdd, IBM, Sematech, and MCC.

Where computing machinery went, hackers generally followed. Austin boasted not only Phoenix Project, currently LoD's most flagrant underground board, but a number of UNIX nodes.

One of these nodes was Elephant, run by a UNIX consultant named Robert Izenberg. Izenberg, in search of a relaxed southern lifestyle and a lower cost of living, had recently migrated to Austin from New Jersey. In New Jersey, Izenberg had worked for an independent contracting company, programming UNIX code for AT&T itself. Terminus had been a frequent user on Izenberg's privately owned Elephant node.

Having interviewed Terminus and examined the records on

Netsys, the Chicago Task Force was now convinced that it had discovered an underground gang of UNIX software pirates that was demonstrably guilty of interstate trafficking in illicitly copied AT&T source code. Izenberg was swept into the dragnet around Terminus, the self-proclaimed ultimate UNIX hacker.

Izenberg, in Austin, had settled down into a UNIX job with a Texan branch of IBM. He was no longer working as a contractor for AT&T, but he had friends in New Jersey, and he still logged on to AT&T UNIX computers back in New Jersey, more or less whenever it pleased him. Izenberg's activities appeared highly suspicious to the task force. He might well be breaking into AT&T computers, swiping AT&T software, and passing it to Terminus and other possible confederates, through the UNIX node network. And this data was worth, not merely \$79,499, but hundreds of thousands of dollars!

On February 21, 1990, Robert Izenberg arrived home from work at IBM to find that all the computers had vanished mysteriously from his Austin apartment. Naturally he assumed that he had been robbed. His Elephant node, his other machines, his notebooks, his disks, his tapes, all gone! However, nothing much else seemed disturbed—the place had not been ransacked.

The puzzle became much stranger some five minutes later. Austin U.S. Secret Service Agent Al Soliz, accompanied by University of Texas campus-security officer Larry Coutorie and the ubiquitous Tim Foley, made their appearance at Izenberg's door. They were in plain clothes: slacks, polo shirts. They came in, and Tim Foley accused Izenberg of belonging to the Legion of Doom.

Izenberg told them that he had never heard of the Legion of Doom. And what about a certain stolen E911 Document, which posed a direct threat to the police emergency lines? Izenberg claimed that he'd never heard of that either.

His interrogators found this difficult to believe. Didn't he know Terminus?

Who?

19.2 kilobaud, and which had just gone out Izenberg's door in Secret Service custody) was likely hot property. Izenberg was taken aback to hear this; but then again, most of Izenberg's equipment, like that of most freelance professionals in the industry, was discounted, passed hand-to-hand through various kinds of barter and gray market. There was no proof that the modem was stolen, and even if it was, Izenberg hardly saw how that gave them the right to take every electronic item in his house.

Still, if the U.S. Secret Service figured it needed his computer for national security reasons—or whatever—then Izenberg would not kick. He figured he would somehow make the sacrifice of his twenty thousand dollars' worth of professional equipment, in the spirit of full cooperation and good citizenship.

Robert Izenberg was not arrested. Izenberg was not charged with any crime. His UUCP node—full of some 140 megabytes of the files, mail, and data of himself and his dozen or so entirely innocent users—went out the door as “evidence.” Along with the disks and tapes, Izenberg had lost about 800 megabytes of data.

Six months would pass before Izenberg decided to phone the Secret Service and ask how the case was going. That was the first time that Robert Izenberg would ever hear the name of William Cook. As of January 1992, a full two years after the seizure, Izenberg, still not charged with any crime, would be struggling through the morass of the courts, in hope of recovering his thousands of dollars' worth of seized equipment.

In the meantime, the Izenberg case received absolutely no press coverage. The Secret Service had walked into an Austin home, removed a UNIX bulletin board system, and met with no operational difficulties whatsoever.

Except that word of a crackdown had percolated through the Legion of Doom. The Mentor voluntarily shut down the Phoenix Project. It seemed a pity, especially as telco security employees had, in fact, shown up on Phoenix, just as he had hoped—along with the usual motley crowd of LoD heavies, hangers-on, phreaks, hackers, and wannabes. There was “Sandy” Sandquist from U.S. Sprint security, and some guy named Henry Kluepfel, from

Bellcore itself! Kluepfel had been trading friendly banter with hackers on Phoenix since January 30 (two weeks after the Martin Luther King Day Crash). The presence of such a stellar telco official seemed quite the coup for Phoenix Project.

Still, Mentor could judge the climate. Atlanta in ruins, *Phrack* in deep trouble, something weird going on with UNIX nodes—discretion was advisable. Phoenix Project went off-line.

Kluepfel, of course, had been monitoring this LoD bulletin board for his own purposes—and those of the Chicago unit. As far back as June 1987, Kluepfel had logged on to a Texas underground board called Phreak Klass 2600. There he'd discovered a Chicago youngster named "Shadowhawk," strutting and boasting about rifling AT&T computer files, and bragging of his ambitions to riddle AT&T's Bellcore computers with Trojan horse programs. Kluepfel had passed the news to Cook in Chicago, Shadowhawk's computers had gone out the door in Secret Service custody, and Shadowhawk himself had gone to jail.

Now it was Phoenix Project's turn. Phoenix Project postured about "legality" and "merely intellectual interest," but it reeked of the underground. It had *Phrack* on it. It had the E911 Document. It had a lot of dicey talk about breaking into systems, including some bold and reckless stuff about a supposed "decryption service" that Mentor and friends were planning to run, to help crack encrypted passwords off of hacked systems.

Mentor was an adult. There was a bulletin board at his place of work as well. Kluepfel logged onto this board too and discovered it was called Illuminati. It was run by some company called Steve Jackson Games.

On March 1, 1990, the Austin crackdown went into high gear.

On the morning of March 1—a Thursday—twenty-one-year-old University of Texas student Erik Bloodaxe, co-sysop of Phoenix Project and an avowed member of the Legion of Doom, was wakened by a police revolver leveled at his head.

Bloodaxe watched, jittery, as Secret Service agents appropriated his 300 baud terminal and, rifling his files, discovered his treasured source code for Robert Morris' notorious Internet

worm. But Bloodaxe, a wily operator, had suspected that something like this might be coming. All his best equipment had been hidden away elsewhere. The raiders took everything electronic, however, including his telephone. They were stymied by his hefty arcade-style Pac-Man game and left it in place, as it was simply too heavy to move.

Bloodaxe was not arrested. He was not charged with any crime. A good two years later, the police still had what they had taken from him, however.

The Mentor was less wary. The dawn raid roused him and his wife from bed in their underwear, and six Secret Service

agents, accompanied by an Austin policeman and Henry Kluepfel himself, made a rich haul. Off went the works, into the agents' white Chevrolet minivan: an IBM PC AT clone with 4 meg of RAM and a 120-meg hard disk; a Hewlett-Packard LaserJet II printer; a completely legitimate and highly expensive SCO-Xenix 286 operating system; Pagemaker disks and documentation; and a Microsoft Word word processing program. Mentor's wife had her incomplete academic thesis stored on the hard disk; that went too, and so did the couple's telephone. As of two years later, all this property remained in police custody.

Mentor remained under guard in his apartment as agents prepared to raid Steve Jackson Games. The fact that this was a business headquarters and not a private residence did not deter the agents. It was still very early; no one was at work yet. The agents prepared to break down the door, but Mentor, eavesdropping on the Secret Service walkie-talkie traffic, begged them not to do it and offered his key to the building.

The exact details of the next events are unclear. The agents would not let anyone else into the building. Their search warrant, when produced was unsigned. Apparently they breakfasted from the local Whataburger, as the litter from hamburgers was later

*The 21-year-old
University of Texas
student was awakened by a
police revolver leveled at
his head.*

found inside. They also sampled extensively a bag of jellybeans kept by an SJG employee. Someone tore a "Dukakis for President" sticker from the wall.

SJG employees, diligently showing up for the day's work, were met at the door and briefly questioned by U.S. Secret Service agents. The employees watched in astonishment as agents wielding crowbars and screwdrivers emerged with captive machines. They attacked outdoor storage units with boltcutters. The agents wore blue nylon windbreakers with SECRET SERVICE stenciled across the back, with running shoes and jeans.

Jackson's company lost three computers, several hard disks, hundreds of floppy disks, two monitors, three modems, a laser printer, various power cords, cables, and adapters (and, oddly, a small bag of screws, bolts, and nuts). The seizure of Illuminati BBS deprived SJG of all the programs, text files, and private e-mail on the board. The loss of two other SJG computers was a severe blow as well, because it caused the loss of electronically stored contracts, financial projections, address directories, mailing lists, personnel files, business correspondence, and, not least, the drafts of forthcoming games and gaming books.

No one at Steve Jackson Games was arrested. No one was accused of any crime. No charges were filed. Everything appropriated was officially kept as "evidence" of crimes never specified.

After the *Phrack* show trial, the Steve Jackson Games scandal was the most bizarre and aggravating incident of the Hacker Crackdown of 1990. This raid by the Chicago Task Force on a science-fiction gaming publisher was to rouse a swarming host of civil liberties issues and gave rise to an enduring controversy that was still recomplicating itself, and growing in the scope of its implications, a full two years later.

The pursuit of the E911 Document stopped with the Steve Jackson Games raid. As we have seen, there were hundreds, perhaps thousands of computer users in America with the E911 Document in their possession. Theoretically, the task force had a perfect legal right to raid any of these people, and legally could have seized the machines of anybody who subscribed to *Phrack*.

However, there was no copy of the E911 Document on Jackson's Illuminati board. And there the Chicago raiders stopped dead; they have not raided anyone since.

It might be assumed that Rich Andrews and Charlie Boykin, who had brought the E911 Document to the attention of telco security, might be spared any official suspicion. But as we have seen, the willingness to "cooperate fully" offers little, if any, assurance against federal antihacker prosecution.

Richard Andrews found himself in deep trouble, thanks to the E911 Document. Andrews lived in Illinois, the native stomping grounds of the Chicago Task Force. On February 3 and 6, both his home and his place of work were raided by USSS. His machines went out the door too, and he was grilled at length (though not arrested). Andrews proved to be in purportedly guilty possession of: UNIX SVR 3.2; UNIX SVR 3.1; UUCP; PMON; WWB; IWB; DWB; NROFF; KORN SHELL '88; C++; and QUEST, among other items. Andrews had received this proprietary code—which AT&T officially valued at well over \$250,000—through the UNIX network, much of it supplied to him by Terminus as a personal favor. Perhaps worse yet, Andrews admitted to returning the favor, by passing Terminus a copy of AT&T proprietary STAR-LAN source code.

Even Charles Boykin, himself an AT&T employee, entered some very hot water. By 1990, he'd almost forgotten about the E911 problem he'd reported in September 1988; in fact, since that date, he'd passed two more security alerts to Jerry Dalton, concerning matters that Boykin considered far worse than the E911 Document.

But by 1990, year of the crackdown, AT&T Corporate Information Security was fed up with Killer. This machine offered no direct income to AT&T and was providing aid and comfort to a cloud of suspicious yokels from outside the company, some of them actively malicious toward AT&T, its property, and its corporate interests. Whatever goodwill and publicity had been won among Killer's 1,500 devoted users was considered no longer worth the security risk. On February 20, 1990, Jerry Dalton ar-

rived in Dallas and simply unplugged the phone jacks, to the puzzled alarm of Killer's many Texan users. Killer went permanently off-line, with the loss of vast archives of programs and huge quantities of electronic mail; it was never restored to service. AT&T showed no particular regard for the "property" of these 1,500 people. Whatever "property" the users had been storing on AT&T's computer simply vanished completely.

Boykin, who had himself reported the E911 problem, now found himself under a cloud of suspicion. In a weird private-security replay of the Secret Service seizures, Boykin's own home was visited by AT&T Security and his own machines were carried out the door.

However, there were marked special features in the Boykin case. Boykin's disks and his personal computers were examined swiftly by his corporate employers and returned politely in just two days (unlike Secret Service seizures, which commonly take months or years). Boykin was not charged with any crime or wrongdoing, and he kept his job with AT&T (though he retired in September 1991, at the age of fifty-two).

It's interesting to note that the U.S. Secret Service somehow failed to seize Boykin's Killer node and carry AT&T's own computer out the door. Nor did they raid his home. They seemed perfectly willing to take the word of AT&T Security that AT&T's employee and AT&T's Killer node were free of hacker contraband and on the up-and-up.

It's digital water-under-the-bridge at this point, as Killer's 3,200 megabytes of Texan electronic community were erased in 1990 and Killer itself was shipped out of the state.

But the experiences of Andrews and Boykin, and the users of their systems, remained side issues. They did not begin to assume the social, political, and legal importance that gathered, slowly but inexorably, around the issue of the raid on Steve Jackson Games.

We must now turn our attention to Steve Jackson Games itself, and explain what SJG was, what it really did, and how it had

managed to attract this particularly odd and virulent kind of trouble. The reader may recall that this is not the first but the second time that the company has appeared in this narrative; a Steve Jackson game called GURPS was a favorite pastime of Atlanta hacker Urvile, and Urvile's science-fictional gaming notes had been mixed up promiscuously with notes about his actual computer intrusions.

First, Steve Jackson Games, Inc., was *not* a publisher of "computer games." SJG published "simulation games," parlor games that were played on paper, with pencils, and dice, and printed guidebooks full of rules and statistics tables. No computers were involved in the games themselves. When you bought a Steve Jackson Game, you did not receive any software disks. What you got was a plastic bag with some cardboard game tokens, maybe a few maps or a deck of cards. Most of the products were books.

However, computers *were* deeply involved in the Steve Jackson Games business. Like almost all modern publishers, Steve Jackson and his fifteen employees used computers to write text, keep accounts, and run the business generally. They also used a computer to run their official bulletin board system for Steve Jackson Games, a board called Illuminati. On Illuminati, simulation gamers who happened to own computers and modems could associate, trade mail, debate the theory and practice of gaming, and keep up with the company's news and its product announcements.

Illuminati was a modestly popular board, run on a small computer with limited storage, only one phone line, and no ties to large-scale computer networks. It did, however, have hundreds of users, many of them dedicated gamers willing to call from out of state.

Illuminati was *not* an "underground" board. It did not feature hints on computer intrusion, or "anarchy files," or illicitly posted credit card numbers, or long-distance access codes. Some of Illuminati's users, however, were members of the Legion of Doom. And so was one of Steve Jackson's senior employees—the Mentor. Mentor wrote for *Phrack* and also ran an underground board,

Phoenix Project—but Mentor was not a computer professional. Mentor was the managing editor of Steve Jackson Games and a professional game designer by trade. These LoD members did not use Illuminati to help their *hacking* activities. They used it to help their *game-playing* activities—and they were even more dedicated to simulation gaming than they were to hacking.

Illuminati involved flying saucers, the CIA, the KGB, the phone companies, the Ku Klux Klan, and the Boy Scouts.

Illuminati got its name from a card game that Steve Jackson himself, the company's founder and sole owner, had invented. This multiplayer card game was one of Mr. Jackson's best-known, most successful, most technically innovative products. Illuminati was a

game of paranoid conspiracy in which various antisocial cults warred covertly to dominate the world. Illuminati was hilarious, and great fun to play, involving flying saucers, the CIA, the KGB, the phone companies, the Ku Klux Klan, South American Nazis, cocaine cartels, the Boy Scouts, and dozens of other splinter groups from the twisted depths of Mr. Jackson's professionally fervid imagination. For the uninitiated, any public discussion of the Illuminati card game sounded, by turns, utterly menacing or completely insane.

And then there was SJG's Car Wars, in which souped-up armored hot rods with rocket launchers and heavy machine guns did battle on the American highways of the future. The lively Car Wars discussion on the Illuminati board featured many meticulous, painstaking discussions of the effects of grenades, landmines, flamethrowers, and napalm. It sounded like hacker anarchy files run amuck.

Mr. Jackson and his coworkers earned their daily bread by supplying people with make-believe adventures and weird ideas. The more far-out, the better.

Simulation gaming is an unusual hobby, but gamers have not generally had to beg the permission of the Secret Service to exist.

Wargames and role-playing adventures are an old and honored pastime, much favored by professional military strategists. Once little known, these games are now played by hundreds of thousands of enthusiasts throughout North America, Europe, and Japan. Gaming books, once restricted to hobby outlets, now commonly appear in chain stores such as B. Dalton's and Waldenbooks, and sell vigorously.

Steve Jackson Games, Inc., of Austin, Texas, was a games company of the middle rank. In 1989, SJG grossed about a million dollars. Jackson himself had a good reputation in his industry as a talented and innovative designer of rather unconventional games, but his company was something less than a titan of the field—certainly not like the multimillion-dollar TSR Inc., or Britain's gigantic Games Workshop.

SJG's Austin headquarters was a modest two-story brick office suite, cluttered with phones, photocopiers, fax machines, and computers. It bustled with semiorganized activity and was littered with glossy promotional brochures and dog-eared science-fiction novels. Attached to the offices was a large tin-roofed warehouse piled twenty feet high with cardboard boxes of games and books. Despite the weird imaginings that went on within it, the SJG headquarters was quite a quotidian, everyday sort of place. It looked like what it was: a publisher's digs.

Both *Car Wars* and *Illuminati* were well-known, popular games. But the mainstay of the Jackson organization was their Generic Universal Role-Playing System, "GURPS." The GURPS system was considered solid and well designed, an asset for players. But perhaps the most popular feature of the GURPS system was that it allowed gaming masters to design scenarios that closely resembled well-known books, movies, and other works of fantasy. Jackson had licensed and adapted works from many science fiction and fantasy authors. There was *GURPS Conan*, *GURPS Riverworld*, *GURPS Horseclans*, *GURPS Witch World*, names eminently familiar to science-fiction readers. And there was *GURPS Special Ops*, from the world of espionage fantasy and unconventional warfare.

And then there was *GURPS Cyberpunk*.

“Cyberpunk” was a term given to certain science-fiction writers who had entered the genre in the 1980s. Cyberpunk, as the label implies, had two general distinguishing features. First, its writers had a compelling interest in information technology, an interest closely akin to science fiction’s earlier fascination with space travel. And second, these writers were “punks,” with all the distinguishing features that that implies: Bohemian artiness, youth run wild, an air of deliberate rebellion, funny clothes and hair, odd politics, a fondness for abrasive rock and roll; in a word, trouble.

The cyberpunk SF writers were a small group of mostly college-educated white middle-class litterateurs, scattered through the United States and Canada. Only one, Rudy Rucker, a professor of computer science in Silicon Valley, could rank with even the humblest computer hacker. Except for Professor Rucker, the cyberpunk authors were not programmers or hardware experts; they considered themselves artists (as, indeed, did Professor Rucker). However, these writers all owned computers, and took an intense and public interest in the social ramifications of the information industry.

The cyberpunks had a strong following among the global generation that had grown up in a world of computers, multinational networks, and cable television. Their outlook was considered somewhat morbid, cynical, and dark, but then again, so was the outlook of their generational peers. As that generation matured and increased in strength and influence, so did the cyberpunks. As science-fiction writers went, they were doing fairly well for themselves. By the late 1980s, their work had attracted attention from gaming companies, including Steve Jackson Games, which was planning a cyberpunk simulation for the flourishing GURPS gaming system.

The time seemed ripe for such a product, which had already been proven in the marketplace. The first games company out of the gate, with a product boldly called *Cyberpunk* in defiance of possible infringement-of-copyright suits, had been an upstart

group called R. Talsorian. Talsorian's Cyberpunk was a fairly decent game, but the mechanics of the simulation system left a lot to be desired. Commercially, however, the game did very well.

The next cyberpunk game had been the even more successful Shadowrun by FASA Corporation. The mechanics of this game were fine, but the scenario was rendered moronic by sappy fantasy elements such as elves, trolls, wizards, and dragons—all highly ideologically incorrect, according to the hard-edged, high-tech standards of cyberpunk science fiction.

Other game designers were chomping at the bit. Prominent among them was the Mentor, a gentleman who, like most of his friends in the Legion of Doom, was quite the cyberpunk devotee. Mentor reasoned that the time had come for a *real* cyberpunk gaming book—one that the princes of computer-mischief in the Legion of Doom could play without laughing themselves sick. This book, *GURPS Cyberpunk*, would reek of culturally on-line authenticity.

Mentor was particularly well qualified for this task. Naturally, he knew far more about computer intrusion and digital skullduggery than any previously published cyberpunk author. Not only that, but he was good at his work. A vivid imagination combined with an instinctive feeling for the working of systems and, especially, the loopholes within them are excellent qualities for a professional game designer.

By March 1, *GURPS Cyberpunk* was almost complete, ready to print and ship. Steve Jackson expected vigorous sales for this item, which, he hoped, would keep the company financially afloat for several months. *GURPS Cyberpunk*, like the other GURPS "modules," was not a "game" like a Monopoly set, but a *book*: a bound paperback book the size of a glossy magazine, with a slick color cover, and pages full of text, illustrations, tables, and footnotes. It was advertised as a game and was used as an aid to game-playing, but it was a book, with an ISBN number, published in Texas, copyrighted, and sold in bookstores.

And now that book, stored on a computer, had gone out the door in the custody of the Secret Service.

The day after the raid, Steve Jackson visited the local Secret Service headquarters with a lawyer in tow. There he confronted Tim Foley (still in Austin at that time) and demanded his book back. But there was trouble. *GURPS Cyberpunk*, alleged a Secret Service agent to astonished businessman Steve Jackson, was “a manual for computer crime.”

“It’s science fiction,” Jackson said.

“No, this is real.” This statement was repeated several times, by several agents. Jackson’s ominously accurate game had passed from pure, obscure, small-scale fantasy into the impure, highly publicized, large-scale fantasy of the Hacker Crackdown.

No mention was made of the real reason for the search. According to their search warrant, the raiders had expected to find the E911 Document stored on Jackson’s bulletin board system. But that warrant was sealed—a procedure that most law enforcement agencies will use only when lives are demonstrably in danger. The raiders’ motives were not discovered until the Jackson search warrant was unsealed by his lawyers many months later. The Secret Service, and the Chicago Computer Fraud and Abuse Task Force, said absolutely nothing to Steve Jackson about any threat to the police 911 System. They said nothing about the Atlanta Three, nothing about *Phrack* or Knight Lightning, nothing about Terminus.

Jackson was left to believe that his computers had been seized because he intended to publish a science-fiction book that law enforcement considered too dangerous to see print.

This misconception was repeated again and again, for months, to an ever-widening public audience. It was not the truth of the case; but as months passed, and this misconception was printed again and again publicly, it became one of the few publicly known “facts” about the mysterious Hacker Crackdown. The Secret Service had seized a computer to stop the publication of a cyberpunk science-fiction book.

The second section of this book, “The Digital Underground,” is almost finished now. We have become acquainted with all the major figures of this case who actually belong to the underground

milieu of computer intrusion. We have some idea of their history, their motives, their general modus operandi. We now know, I hope, who they are, where they came from, and more or less what they want. In the next section of this book, "Law and Order," we leave this milieu and directly enter the world of America's computer-crime police.

The Secret Service had seized a computer to stop the publication of a "cyberpunk" science-fiction book.

At this point, however, I have another figure to introduce: myself.

My name is Bruce Sterling. I live in Austin, Texas, where I am a science-fiction writer by trade: specifically, a *cyberpunk* science-fiction writer.

Like my cyberpunk colleagues in the United States and Canada, I've never been entirely happy with this literary label—especially after it became a synonym for a computer criminal. But I did once edit a book of stories by my colleagues, called *Mirrorshades: The Cyberpunk Anthology*, and I've long been a writer of literary-critical cyberpunk manifestos. I am not a hacker of any description, though I do have readers in the digital underground.

When the Steve Jackson Games seizure occurred, I naturally took an intense interest. If cyberpunk books were being banned by federal police in my own hometown, I reasonably wondered whether I myself might be next. Would my computer be seized by the Secret Service? At the time, I was in possession of an aging Apple IIe without so much as a hard disk. If I were to be raided as an author of computer-crime manuals, the loss of my feeble word processor would likely provoke more snickers than sympathy.

I'd known Steve Jackson for many years. We knew one another as colleagues, for we frequented the same local science-fiction conventions. I'd played Jackson games and recognized his cleverness; but he certainly had never struck me as a potential mastermind of computer crime.

I also knew a little about computer bulletin board systems. In the mid-1980s I had taken an active role in an Austin board named SMOF-BBS, one of the first boards dedicated to science fiction. I had a modem, and on occasion I'd logged on to Illuminati, which always looked entertainingly wacky but certainly harmless enough.

At the time of the Jackson seizure, I had no experience whatsoever with underground boards. But I knew that no one on Illuminati talked about breaking into systems illegally or about robbing phone companies. Illuminati didn't even offer pirated computer games. Steve Jackson, like many creative artists, was markedly touchy about theft of intellectual property.

It seemed to me that Jackson was either seriously suspected of some crime—in which case, he would be charged soon, and would have his day in court—or else he was innocent, in which case the Secret Service would quickly return his equipment and everyone would have a good laugh. I rather expected the good laugh. The situation was not without its comic side. The raid, known as the “Cyberpunk Bust” in the science-fiction community, was winning a great deal of free national publicity both for Jackson himself and the cyberpunk science-fiction writers generally.

Besides, science-fiction people are used to being misinterpreted. Science fiction is a colorful, disreputable, slipshod occupation, full of unlikely oddballs, which, of course, is why we like it. Weirdness can be an occupational hazard in our field. People who wear Halloween costumes are sometimes mistaken for monsters.

Once upon a time—back in 1939, in New York City—science fiction and the U.S. Secret Service collided in a comic case of mistaken identity. This weird incident involved a literary group quite famous in science fiction, known as “the Futurians,” whose membership included such future genre greats as Isaac Asimov, Frederik Pohl, and Damon Knight. The Futurians were every bit as offbeat and wacky as any of their spiritual descendants, includ-

ing the cyberpunks, and were given to communal living, spontaneous group renditions of light opera, and midnight fencing exhibitions on the lawn. The Futurians didn't have bulletin board systems, but they did have the technological equivalent in 1939—mimeographs and a private printing press. These were in steady use, producing a stream of science-fiction fan magazines, literary manifestos, and weird articles, which were picked up in ink-sticky bundles by a succession of strange, gangly, spotty young men in fedoras and overcoats.

The neighbors grew alarmed at the antics of the Futurians and reported them to the Secret Service as suspected counterfeiters. In the winter of 1939, a squad of USSS agents with drawn guns burst into Futurian House, prepared to confiscate the forged currency and illicit printing presses. There they discovered a slumbering science-fiction fan named George Hahn, a guest of the Futurian commune who had just arrived in New York. Hahn managed to explain himself and his group, and the Secret Service agents left the Futurians in peace henceforth. (Alas, Hahn died in 1991, just before I had discovered this astonishing historical parallel and just before I could interview him for this book.)

But the Jackson case did not come to a swift and comic end. No quick answers came his way, or mine; no swift reassurances that all was right in the digital world, that matters were well in hand after all. Quite the opposite. In my alternate role as a sometime pop-science journalist, I interviewed Jackson and his staff for an article for a British magazine. The strange details of the raid left me more concerned than ever. Without its computers, the company had been crippled financially and operationally. Half the SJG workforce, a group of entirely innocent people, had been fired, deprived of their livelihoods by the seizure. It began to dawn on me that authors—American writers—might well have their computers seized, under sealed warrants, without any criminal charge; and that, as Steve Jackson had discovered, there was no immediate recourse for this. This was no joke; this wasn't science fiction; this was real.

I determined to put science fiction aside until I had discovered what had happened and where this trouble had come from. It was time to enter the purportedly real world of electronic free expression and computer crime. Hence, this book. Hence, the world of the telcos; and the world of the digital underground; and next, the world of the police.