A Postmodernist Interpretation of the Computer Underground

Gordon Meyer, Jim Thomas
June 10, 1990

> Transgression is not immoral. Quite to the contrary, it reconciles the law with what it forbids; it is the dialectical game of good and evil.
> -- Baudrillard (1987: 81)

> There ain't no sin and there ain't no virtue. There's just stuff people do. It's all part of the nice, but that's as far as any man got a right to say.
> -- Steinbeck (1939: 31-32)

The criminalization of "deviant acts" transforms and reduces broader social meanings to legal ones. Once a category of behaviors has become defined by statute as sanctionably deviant, the behaviors so-defined assume a new set of meanings that may obscure ones possessed by those who engage in such behaviors. "Computer deviants" provide one example.

The proliferation of computer technology has been accompanied by the growth of a computer underground (CU), often mistakenly labeled "hackers", that is perceived as criminally deviant by the media, law enforcement officials, and researchers. Drawing from ethnographic data, we offer a cultural rather than a criminological analysis of the underground by suggesting that the CU reflects an attempt to recast, re-appropriate, and reconstruct the power-knowledge relationship that increasingly dominates the ideology and actions of modern society. Our data reveal the computer underground as an invisible community with a complex and interconnected cultural lifestyle, an inchoate anti-authoritarian political consciousness, and dependent on norms of reciprocity, sophisticated socialization rituals, networks of information sharing, and an explicit value system. We interpret the CU culture as a challenge to and parody of conventional culture, as a playful attempt to reject the seriousness of technocracy, and as an ironic substitution of rational technological control of the present for an anarchic and playful future.

Stigmatizing the Computer Underground

The computer underground refers to persons engaged in one or more of several activities, including pirating, anarchy, hacking, and phreaking (1). Because computer underground participants freely share information and often are involved collectively in a single incident, media definitions invoke the generalized metaphors of "conspiracies" and "criminal rings", (e.g., Camper, 1989; Computer Hacker Ring, 1990; Zablit, 1989), "modem macho" evil-doers (Bloombecker, 1988), moral bankruptcy (E. Schwartz, 1988), "electronic trespassers" (Parker, 1983), "crazy kids dedicated to making mischief" (Sandza, 1984a: 17), "electronic vandals" (Bequai: 1987), a new or global "threat" (Markoff, 1990a; Van, 1989), saboteurs ("Computer Saboteur", 1988), monsters (Stoll, 1989: 323), secret societies of criminals (WMAQ, 1990), "'malevolent, nasty, evil-doers' who 'fill the screens of amateur [computer] users with pornography'" (Minister of Parliament Emma Nicholson, cited in

"Civil Liberties", 1990: 27), "varmints" and "bastards" (Stoll, 1989: 257), and "high-tech street gangs" ("Hacker, 18", 1989). Stoll (cited in J. Schwartz, 1990: 50) has even compared them to persons who put razorblades in the sand at beaches, a bloody, but hardly accurate, analogy. Most dramatic is Rosenblatt's (1990: 37) attempt to link hackers to pedophilia and "snuff films", a ploy clearly designed to inflame rather than educate.

These images have prompted calls for community and law enforcement vigilance (Conly and McEwen, 1990: 2; Conly, 1989; McEwen, 1989), and for application of the Racketeer Influenced and Corrupt Organizations (RICO) Act to prosecute and control the "criminals" (Cooley, 1984), which have created considerable concern for civil liberties (Markoff, 1990b; J. Schwartz, 1990). Such exaggerated discourse also fails to distinguish between underground "hobbyists", who may infringe on legal norms but have no intention of pillaging, from felonious predators, who use technology to loot (2). Such terminology creates a common stock of public knowledge that formats interpretations of CU activity in ways pre-patterned as requiring social control to protect the commonweal (e.g., Altheide, 1985).

As Hollinger and Lanza-Kaduce (1988: 119), Kane (1989), and Pfuhl (1987) observed, the stigmatization of hackers has emerged primarily through value-laden media depictions. When in 1988 a Cornell University graduate student inadvertently infected an international computer network by planting a self-reproducing "virus", or "rogue program", the news media followed the story with considerable detail about the dangers of computer abuse (e.g., Allman, 1990; Winter, 1988). Five years earlier, in May of 1983, a group of hackers known as "The 414's" received equal media attention when they broke into the computer system of the Sloan Kettering Cancer research center. Between these dramatic and atypical events, the media have dramatized the dangers of computer renegades, and media anecdotes presented during Congressional legislative debates to curtail "computer abuse" dramatized the "computer hacking problem" (Hollinger and Lanza-Kaduce, 1988: 107). Although the accuracy and objectivity of the evidence has since been challenged (Hollinger and Lanza-Kaduce 1988: 105), the media continue to format CU activity by suggesting that any computer-related felony can be attributed to hacking. Additionally, media stories are taken from the accounts of police blotters, security personnel, and apprehended hackers, each of whom have different perspectives and definitions. This creates a self-reinforcing imagery in which extreme examples and cursively circulated data are discretely adduced to substantiate the claim of criminality by those with a vested interest in creating and maintaining such definitions. For example, Conly and McEwen (1990) list examples of law enforcement jurisdictions in which special units to fight "computer crime", very broadly defined, have been created. These broad definitions serve to expand the scope of authority and resources of the units. Nonetheless, despite criminalization, there is little evidence to support the contention that computer hacking has been sufficiently abusive or pervasive to warrant zealous prosecution (Michalowski and Pfuhl, forthcoming).

As an antidote to the conventional meanings of CU activity as simply one of deviance, we shift the social meaning of CU behavior from one of stigma to one of culture creation and meaning. Our work is tentative, in part because of the lack of previous substantive literature and in part because of the complexity of the data, which indicate a multiplicity of subcultures within the CU. This paper examines two distinct CU subcultures, phreaks and hackers, and challenges the Manichean view that hackers can be understood simply as profaners of a sacred moral and economic order.

The Computer Underground and Postmodernism

The computer underground is a culture of persons who call computer bulletin board systems (BBSs, or just "boards"), and share the interests fostered by the BBS. In conceptualizing the computer underground as a

distinct culture, we draw from Geertz's (1973: 5) definition of culture as a system of meanings that give significance to shared behaviors that must be interpreted from the perspective of those engaged in them. A culture provides not only the "systems of standards for perceiving, believing, evaluating, and acting" (Goodenough, 1981: 110), but includes the rules and symbols of interpretation and discourse for participants :

> In crude relief, culture can be understood as a set of solutions devised by a group of people to meet specific problems posed by situations they face in common... This notion of culture as a living, historical product of group problem solving allows an approach to cultural study that is applicable to any group, be it a society, a neighborhood, a family, a dance band, or an organization and its segments.
> -- Van Maanen and Barley (1985: 33)

Creating and maintaining a culture requires continuous individual or group processes of sustaining an identity through the coherence gained by a consistent aesthetic point of view, a moral conception of self, and a lifestyle that expresses those conceptions in one's immediate existence and tastes (Bell, 1976: 36). These behavioral expressions signify a variety of meanings, and as signifiers they reflect a type of code that can be interpreted semiotically, or as a sign system amenable to readings independent of either participants or of those imposed by the super-ordinate culture :

> All aspects of culture possess a semiotic value, and the most taken-for-granted phenomena can function as signs : as elements in communication systems governed by semantic rules and codes which are not themselves directly apprehended in experience. These signs are, then, as opaque as the social relations which produce them and which they re-present.
> -- Hebdige (1982: 13)

It is this symbolic cultural ethos, by which we mean the style, world view, and mood (Hebdige, 1979), that reflects the postmodernist elements of the CU and separates it from modernism. Modernist culture is characterized especially by rationality, technological enhancement, deference to centralized control, and mass communication. The emergence of computer technology has created dramatic changes in social communication, economic transactions, and information processing and sharing, while simultaneously introducing new forms of surveillance, social control, and intrusions on privacy (Marx, 1988a: 208-211; Marx and Reichman, 1985). This has contributed to a :

> ...richly confused and hugely verbal age, energized by a multitude of competing discourses, the very proliferation and plasticity of which increasingly determine what we defensively refer to as our reality.
> -- Newman (1985: 15)

By Postmodernism we mean a reaction against "cultural modernity" and a destruction of the constraints of the present "maximum security society" (Marx, 1988b) that reflect an attempt to gain control of an alternative future. In the CU world, this constitutes a conscious resistance to the domination of but not the fact of technological encroachment into all realms of our social existence. The CU represents a reaction against modernism by offering an ironic response to the primacy of a master technocratic language, the incursion of computers into realms once considered private, the politics of techno-society, and the sanctity of established civil and state authority. Postmodernism is characterized not so much by a single definition as by a number of

interrelated characteristics, including, but not limited to :

1. Dissent for dissent's sake (Lyotard, 1988).
2. The collapse of the hierarchical distinction between mass and popular culture (Featherstone, 1988: 203).
3. A stylistic promiscuity favoring eclecticism and the mixing of codes (Featherstone, 1988: 203).
4. Parody, pastiche, irony, playfulness and the celebration of the surface "depthlessness" of culture (Featherstone, 1988: 203).
5. The decline of the originality/genius of the artistic producer and the assumption that art can only be repetitious (Featherstone 1988: 203).
6. The stripping away of social and perceptual coordinates that let one "know where one is" (Latimer, 1984: 121).
7. A search for new ways to make the unpresentable presentable, and break down the barriers that keep the profane out of everyday life (Denzin, 1988: 471).
8. The introduction of new moves into old games or inventing new games that are evaluated pragmatically rather than from some uniform stand point of "truth" or philosophical discourse (Callinicos, 1985: 86).
9. Emphasis on the visual over the literary (Lash, 1988: 314).
10. Devaluation of formalism and juxtaposition of signifiers taken from the banalities of everyday life (Lash, 1988: 314).
11. Contesting of rationalist and/or didactive views of culture (Lash, 1988: 314).
12. Asking not what a cultural text means, but what it does (Lash, 1988: 314).
13. Operation through the spectator's immersion, the relatively unmediated investment of his/her desire in the cultural object (Lash, 1988: 314).
14. Acknowledgement of the decenteredness of modern life and "plays with the apparent emptiness of modern life as well as the lack of coherence in modern symbol systems" (Manning, 1989: 8).

"Post-Modernism" in its positive form constitutes an intellectual attack upon the atomized, passive and indifferent mass culture which, through the saturation of electronic technology, has reached its zenith in Post-War American (Newman, 1985: 5). It is this style of playful rebellion, irreverent subversion, and juxtaposition of fantasy with high-tech reality that impels us to interpret the computer underground as a postmodernist culture.

Data and Method

Obtaining data from any underground culture requires tact. BBS operators protect the privacy of users and access to elite boards, or at least to their relevant security levels, virtually always requires completion of a preliminary questionnaire, a screening process, and occasional voice verification. Researchers generally do not themselves violate laws or dominant norms, so they depend on their informants for potentially "dirty information" (Thomas and Marquart, 1988). Our own data are no exception and derive from several sources.

First, the bulk of our data come from computer bulletin board systems. BBSs are personal computers (PCs) that have been equipped with a telephone modem and special software that connects users to other PCs by telephone. After "logging in" by supplying a valid user name and password, the user can receive and leave messages to other users of the system. These messages are rarely private and anyone calling the BBS can freely read and respond to them. There is usually the capacity to receive (download) or send (upload) text files ("G-philes") or software programs between the caller and host system.

We logged the message section of CU BBSs to compile documentary evidence of the issues deemed important for discussion by participants. Logs are "captured" (recorded using the computer buffer) messages left on the

board by users. Calculating the quantity of logged data is difficult because of formatting variance, but we estimate that our logs exceed 10000 printed pages. The logs cited here are verbatim with the exception of minor editing changes in format and extreme typographical errors.

Identifying underground BBSs can be difficult, and to the uninitiated they may appear to be licit chat or shareware boards. For callers with sufficient access, however, there exist backstage realms in which "cracking" information is exchanged and private text or software files made available. With current technology, establishing a BBS requires little initial skill. Most boards are short-lived and serve only local or regional callers. Because of the generally poor quality and amateur nature of these systems, we focused on national elite boards. We considered a board "elite" if it met all of the following characteristics : at least one quarter of the users were registered outside the state of the board called; the phone line were exclusively for BBS use and available 24 hours a day; and the information and files/warez were current "state of the field". Elite CU members argue that there are less than ten "truly elite" p/hacker boards nationally.

We obtained the names and numbers of BBSs from the first boards we called, and used a snowball technique to supplement the list. We obtained additional numbers from CU periodicals, and, as we became more familiar with the culture, users also added to the list. Our aggregate data include no less than 300 Bulletin board systems, of which at least 50 attract phreaks and hackers, and voice or on-line interviews with no less than 45 sysops (operators of BBS systems) and other active CU participants.

A second data source included open-ended voice and on-line interviews with hackers, phreaks and pirates. The data include no less than 25 face-to-face, 25 telephone, and 60 on-line interviews obtained as we became familiar with our informants. Third, data acquisition included as much participation as legally possible in CU activities (3). This served to justify our presence in the culture and provided information about the mundane activity of the CU.

Finally, we obtained back and current issues of the primary underground computerized magazines, which are distributed on national BBSs as text files. These contain information relevant to the particular subculture, and included *Phrack*, *Activist Times Incorporated* (ATI), *P/Hun*, *2600 Magazine*, *Pirate*, *TAP*, and *Legion of Doom* (LoD/H). We also draw data from national and international electronic mail (e-mail) systems on which an active information-sharing CU network has developed and spread.

Assessing the validity and reliability of data obtained in this manner creates special problems. One is that of sampling. The number of boards, their often ephemeral existence, and the problem of obtaining access all make conventional sampling impossible. We focused on national boards and engaged in theoretical sampling (Glaser and Strauss, 1967: 45-77). We consider our sample representative, and accept Bordieu's observation that :

> If, following the canon dictated by orthodox methodology, you take a random sample, you mutilate the very object you have set out to construct. If, in a study of the field of lawyers, for instance, you do not draw the President of the Supreme Court, or if, in an inquiry into the French intellectual field of the 1950s, you leave out Jean-Paul Sartre, or Princeton University in a study of American academics, your field is destroyed, insofar as these personas or institutions alone mark a crucial position -- there are positions in a field which command the whole structure.
> -- Bordieu, interviewed in Wacquant (1989: 38).

We judge our sample of participants adequate for several reasons. First, we presume that the members with whom we have had contact comprise the elite members of the culture, as determined by the nature of the boards they were on, references to them on national boards, the level of expertise displayed in their messages, and their appearance in the "user lists" of elite boards. We consider the BBSs to be "typical exemplars" because of their

status in the culture, because of the level of sophistication both of users and of message content, and because of references to these boards as "elite" in CU periodicals.

The Computer Underground

The computer underground is both a life style and a social network. As a lifestyle, it provides identity and roles, an operational ideology, and guides daily routine. As a social network, it functions as a communications channel between persons engaged in one of three basic activities : hacking, phreaking, and pirating (4). Each subgroup possesses an explicit style that includes an ethic and "code of honor", cohesive norms, career paths, and other characteristics that typify a culture (Meyer, 1989a, 1989b; Meyer and Thomas, 1989).

Hebdige (1982: 113-117) used the concept of homology to describe the structural unity that binds participants and provides the "symbolic fit between the values and life-styles of a group" and how it expresses or reinforces its focal concerns. Homology refers to the affinity and similarities members of a group share that give it the particular cultural identity. These shared alternative values and actions connect CU members to each other and their culture, and create a celebration of "otherness" from the broader culture.

Hackers

> (Tune : "Put Another Nickel in") Put another password in, Bomb it out, and try again, Try to get past logging in, Were hacking, hacking, hacking. Try his first wife's maiden name, This is more than just a game, It's real fun, but just the same It's hacking, hacking, hacking. Sys-call, let's try sys-call. Remember, that great bug from Version 3, Of R S X, It's here ! Whoopee ! Put another sys-call in, Run those passwords out and then, Dial back up, we're logging on, We're hacking, hacking, hacking.
> -- The Hacker Anthem, by Chesire Catalyst

Hacking broadly refers to attempts to gain access to computers to which one does not possess authorization. The term "hackers" first came into use in the early 1960's when it was applied to a group of pioneering computer aficionados at MIT (Levy, 1984). Through the 1970s, a hacker was viewed as someone obsessed with understanding and mastering computer systems (Levy, 1984). But, in the early 1980's, stimulated by the release of the movie *WarGames* and the much publicized arrest of a "hacker gang" known as "The 414s", hackers were seen as young whiz-kids capable of breaking into corporate and government computer systems (Landreth 1985 :34). The imprecise media definition and the lack of any clear understanding of what it means to be a hacker results in the mis-application of the label to all forms of computer malfeasance.

Despite the inter-relationship between phreaks and hackers, the label of "hacker" is generally reserved for those engaged in computer system trespassing. For CU participants, hacking can mean either attempting to gain access to a computer system, or the more refined goals of exploring in, experimenting with, or testing a computer system. In the first connotation, hacking requires skills to obtain valid user accounts on computer systems that would otherwise be unavailable, and the term connotes the repetitive nature of break-in attempts. Once successful entry is made, the illicit accounts are often shared among associates and described as being "freshly (or newly) hacked".

The second connotation refers to someone possessing the knowledge, ability, and desire to fully explore a

computer system. For elite hackers, the mere act of gaining entry is not enough to warrant the "hacker" label; there must be a desire to master and skill to use the system after access has been achieved :

> It's Sunday night, and I'm in my room, deep into a hack. My eyes are on the monitor, and my hands are on the keyboard, but my mind is really on the operating system of a super-minicomputer a thousand miles away - a super-mini with an operating systems that does a good job of tracking users, and that will show my activities in its user logs, unless I can outwit it in the few hours before the Monday morning staff arrives for work... Eighteen hours ago, I managed to hack a password for the PDP 11/44. Now, I have only an hour or so left to alter the user logs. If I don't the logs will lead the system operators to my secret account, and the hours of work it took me to get this account will be wasted.
> -- Landreth (1985: 57-58)

An elite hacker must experiment with command structures and explore the many files available in order to understand and effectively use the system. This is sometimes called "hacking around" or simply "hacking a system". This distinction is necessary because not all trespassers are necessarily skilled at hacking out passwords, and not all hackers retain interest in a system once the challenge of gaining entry has been surmounted. Further, passwords and accounts are often traded, allowing even an unskilled intruder to erroneously claim the title of "hacker".

Our data indicate that, contrary to their media image, hackers avoid deliberately destroying data or otherwise damaging the system. Doing so would conflict with their instrumental goal of blending in with the average user to conceal their presence and prevent the deletion of the account. After spending what may be a substantial amount of time obtaining a high access account, the hacker places a high priority on not being discovered using it, and hackers share considerable contempt for media stories that portray them as "criminals". The leading CU periodicals (e.g., *Phrack, Pirate*) and several CU "home boards" reprint and disseminate media stories, adding ironic commentary. The perception of media distortion also provides grist for message sections :

> **A1** : I myself hate newspaper reporters who do stories on hackers, piraters, phreaks, etc... because they always make us sound like these incred. [sic] smart people (which isn't too bad) who are the biggest threat to todays community. Shit... the BEST hackers/phreaks/etc will tell you that they only do it to gain information on those systems, etc... (Freedom - That's what they call it...right ?) (grin).
> **A2** : Good point... never met a "real" p/h type yet who was into ripping off. To rip of a line from the Steve Goodman song (loosely), the game's the thing. Even those who allegedly fly the jolly rodger [pirates], the true ones, don't do it for the rip-off, but, like monopoly, to see if they can get Boardwalk and Park Place without losing any railroads. Fun of the latter is to start on a board with a single good game or util [software utility] and see what it can be turned into, so I'm told. Fuck the press.
> -- DS message log, 1989

One elite hacker, a member of a loose-knit organization recently in the national news when some participants were indicted for hacking, responded to media distortions of the group by issueing an underground press release :

> My name is [deleted], but to the computer world, I am [deleted]. I have been a member of the group known as Legion of Doom since its creation, and admittedly I have not been the most legitimate computer user around, but when people start hinting at my supposed Communist-backed actions, and say that I am involved in a worldwide conspiracy to destroy the nation's computer and/or 911 network, I have to speak up and hope that people will take what I have to say seriously... People just can't seem to grasp the fact that a group of 20 year old kids just might know a little more than they do, and rather than make good use of us, they would rather just lock us away and keep on letting things pass by them. I've said this before, you can't stop burglars from robbing you when you leave the doors unlocked and merely bash them in the head with baseball bats when they walk in. You need to lock the door. But when you leave the doors open, but lock up the people who can close them for you another burglar will just walk right in.
> -- "EB", 1990

Although skirting the law, hackers possess an explicit ethic and their primary goal is knowledge acquisition. Levy (1984: 26-36) identifies six "planks" of the original hacker ethic, and these continue to guide modern hackers :

- First, access to computers should be unlimited and total : "Always yield to the Hands-On Imperative !"
- Second, all information should be free.
- Third, mistrust authority and promote decentralization.
- Fourth, hackers should be judged by their prowess as hackers rather than by formal organizational or other irrelevant criteria.
- Fifth, one can create art and beauty on a computer.
- Finally, computers can change lives for the better.

Phrack, recognized as the "official" p/hacker newsletter, expanded on this creed with a rationale that can be summarized in three principles ("Doctor Crash", 1986). First, hackers reject the notion that "businesses" are the only groups entitled to access and use of modern technology. Second, hacking is a major weapon in the fight against encroaching computer technology. Finally, the high cost of equipment is beyond the means of most hackers, which results in the perception that hacking and phreaking are the only recourse to spreading computer literacy to the masses :

> Hacking. It is a full time hobby, taking countless hours per week to learn, experiment, and execute the art of penetrating multi-user computers : why do hackers spend a good portion of their time hacking ? Some might say it is scientific curiosity, others that it is for mental stimulation. But the true roots of hacker motives run much deeper than that. In this file I will describe the underlying motives of the aware hackers, make known the connections between Hacking, Phreaking, Carding, and Anarchy, and make known the "techno-revolution" which is laying seeds in the mind of every hacker... If you need a tutorial on how to perform any of the above stated methods [of hacking], please read a [*Phrack*] file on it. 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.
> -- "Doctor Crash", 1986

Computer software, such as auto-dialers popularized in the film *WarGames*, provides a means for inexperienced hackers to search out other computers. Auto-dialers randomly dial numbers and save the "hits" for manual testing later. Some users self-identify has hackers simply on the basis of successfully collecting computer numbers or passwords, but these users are considered "lamerz", because they do not possess sufficient

knowledge to obtain access or move about in the system once access is obtained. Lamerz are readily identified by their message content :

> **Sub ->numbers From ->(#538) To ->all Date ->02/21/xx 06:10:00 PM** Does anyone know any numbers for hotels, schools, businesses, etc..and passwords if you do please leave a bulletin with the number and the password and/or logon id.
> **Sub ->phun From ->(#138) To ->all Date ->02/22/xx 12:21:00 AM** Anyone out there got some good 800 dial up that are fairly safe to hack ? If so could ya leave me em in e-mail or post em with the formats... any help would be appreciated... thanx
> **Sub ->NUMBERS From ->(#538) To ->ALL Date ->02/24/xx 03:12:00 PM** Does anyone have any 1-800 numbers with id, logon and passwords ?
> **Sub ->Credit Card's for Codez From ->(#134) To ->All Date ->01/26/xx 07:43:00 AM** Tell ya what. I will exchange any amount of credit cards for a code or two. You name the credit limit you want on the credit card and I will get it for you. I do this cause I to janitorial work at night INSIDE the bank when no one is there... hehehehehehe
> **Sub ->Codes.. From ->(#660) To ->All Date ->01/31/xx 01:29:00 AM** Well, instead of leaving codes, could you leave us "uninformed" people with a few 800 dialups and formats ? I don't need codes, I just want dialups ! Is that so much to ask ? I would be willing to trade CC's [credit cards] for dialups. Lemme know..
> **Sub ->0266 Codez From ->(#134) To ->All Date ->01/31/xx 06:56:00 AM** Anyone, What is the full dial up for 0266 codez ?

Such requests are considered amateurish, rarely generate the requested information, and elicit predictable "flamez" (severe criticism) or even potentially dangerous pseudo-assistance :

> **Sub ->Reply to: 0266 Codez From ->(#124) To ->C-Poo Date ->01/31/xx 09:02:00 AM** Okay, here's the full info, Chris : Dial 1-900-(pause)-[xxx]-REAL. When it answers, hit #*9876321233456534323545766764 Got it ? Okay, here's a 800 number to try : 1-800-426-[xxxx]. Give the operator your zip, and fake it from there ! Enjoy, you hackmeister, you !
> **Sub ->Reply to: 0266 Codez From ->(#448) To ->#38 Date ->01/31/xx 03:43:00 PM** What the fuck kind of question is that ? Are you that stupid ? what is the full dial up for an 0266 ? Give me a break ! Call back when you learn not when you want to leech !
> **Sub ->CC-ING From ->(#393) To ->#38 Date ->02/05/xx 01:41:00 AM** WHAT THE HELL ARE YOU ? PROBABLY A NARC, AREN'T YA ! NO ONE IN HIS RIGHT MIND ASKS FOR CARDS. (AND NARCS AREN'T IN THEIR RIGHT MINDS) AND GIVE OUT CARDS, WHAT DO YOU THINK WE ARE, SHLONGS ?! PERSONALLY I GET MY OWN ON THE JOB, PUMPING GAS PAYS A LOT MORE THAN YOU THINK, THEREFORE I DON'T NEED ANY. THINK ABOUT IT, IF YOU ARE A GOOD HACKER, WHICH I CAN SEE YOU'RE NOT, THEN YOU CAN HACK OUT YOUR OWN CODEZ. PEOPLE WHO NEED CCS CAN CALL CC-VMBS. I HAVE ONE, BUT DON'T ASK FOR IT. IF YOU DON'T KNOW MY CC-VMB LINE THEN YOU'RE NOT TO WELL KNOWN. A LOT OF KNOWN HACKERS KNOW MY CC-VMB LINE. WELL, IF YOU'RE A NARC, YOU'VE JUST BEEN FOUND OUT, IF NOT YOU MIGHT WANT TO GET A JOB AS ONE CUZ YOU ACT JUST LIKE ONE [In BBS protocol, upper case letters indicate emphasis, anger, or shouting].

Although hackers freely acknowledge that their activities may be occasionally illegal, considerable emphasis is placed on limiting violations only to those required to obtain access and learn a system, and they display

hostility toward those who transgress beyond these limits. Most experienced CU members are suspicious of young novices who are often entranced with what they perceive to be the "romance" of hacking. Elite hackers complain continuously that novices are at an increased risk of apprehension and also can "trash" accounts on which experienced hackers have gained and hidden their access. Nonetheless, experienced hackers take pride in their ethic of mentoring promising newcomers, both through their BBSs and newsletters :

> As [my] reputation grew, answering such requests [from novice hackers wanting help] became a matter of pride. No matter how difficult the question happened to be, I would sit at the terminal for five, ten, twenty hours at a time, until I had the answer.
> -- Landreth (1985: 16)

The nation's top elite p/hacker board was particularly nurturing of promising novices before it voluntarily closed in early 1990, and its sysop's handle means "teacher". *Phrack*, begun in 1985, normally contained 10-12 educational articles (or "philes"), most of which provided explicit sophisticated technical information about computer networks and telecommunications systems (5). Boundary socialization occurs in message bases and newsletters that either discourage such activity or provide guidelines for concealing access once obtained :

> Welcome to the world of hacking ! We, the people who live outside of the normal rules, and have been scorned and even arrested by those from the "civilized world", are becoming scarcer every day. This is due to the greater fear of what a good hacker (skill wise, no moral judgements here) can do nowadays, thus causing anti-hacker sentiment in the masses. Also, few hackers seem to actually know about the computer systems they hack, or what equipment they will run into on the front end, or what they could do wrong on a system to alert the "higher" authorities who monitor the system. This article is intended to tell you about some things not to do, even before you get on the system. We will tell you about the new wave of front end security devices that are beginning to be used on computers. We will attempt to instill in you a second identity, to be brought up at time of great need, to pull you out of trouble.
> -- P/hacker newsletter, 1987

Elite hacking requires highly sophisticated technical skills to enter the maze of protective barriers, recognize the computer type, and move about at the highest system levels. As a consequence, information sharing becomes the sine qua non of the hacker culture. "Main message" sections are generally open to all users, but only general information, gossip, and casual commentary is posted. Elite users, those with higher security privileges and access to the "backstage" regions, share technical information and problems, of which the following is typical :

> 89 Mar 11 From ** > Help ! Anyone familiar with a system that responds : A2 : SELECT : DISPLAY : 1=TRUNK,2=SXS;INPUT :3=TRUNK,4=SXS,5=DELETE;7=MSG and then it gives you a prompt If you chose 1... ENTER OLD#,(R=RETURN) At this point I know you can enter 7 digits, the 8th will give you an INVALID ENTRY type message. Some numbers don't work however. (1,2,7,8 I know will) Anybody ?
> 89 Mar 10 From *** > I was hacking around on telenet (415 area code) and got a few things that I am stuck-o on if ya can help, I'd be greatly happy. First of all, I got one that is called RCC PALO ALTO and I can't figure it out. Second (and this looks pretty fun) is the ESPRIT COMMAIL and I know that a user name is SYSTEM because it asked for a password on ONLY that account (pretty obvious eh ?) a few primnet and geonet nodes and a bunch of TELENET ASYYNC to 3270

> SERVICE. It asks for TERMINAL TYPE, my LU NUMBER and on numbers higher than 0 and lower that 22 it asks for a password. Is it an outdial ? What are some common passwords ? then I got a sushi-primnet system. And a dELUT system. And at 206174 there is JUST a: prompt. help !
> -- P/h message log, 1988

Rebelliousness also permeates the hacker culture and is reflected in actions, messages, and symbolic identities. Like other CU participants, hackers employ handles (aliases) intended to display an aspect of one's personality and interests, and a handle can often reveal whether its owner is a "lamer" (an incompetent) or sophisticated. Hackers take pride in their assumed names, and one of the greatest taboos is to use the handle of another or to use multiple handles. Handles are borrowed liberally from the anti-heros of science fiction, adventure fantasy, and heavy metal rock lyrics, particularly among younger users, and from word plays on technology, nihilism, and violence. The CU handle reflects a stylistic identity heavily influenced by metaphors reflecting color (especially red and black), supernatural power (e.g., "Ultimate Warrior, "Dragon Lord"), and chaos ("Death Stalker", "Black Avenger"), or ironic twists on technology, fantasy, or symbols of mass culture (e.g., Epeios, Phelix the Hack, Ellis Dea, Rambo Pacifist, Hitch Hacker).

This anti-establishment ethos also provides an ideological unity for collective action. Hackers have been known to use their collective skills in retaliation for acts against the culture that the perceive as unfair by, for example, changing credit data or "revoking" driver's licenses (Sandza, 1984b; "Yes, you Sound very Sexy", 1989). Following a bust of a national hacker group, the message section of the "home board" contained a lively debate on the desireability of a retaliatory response, and the moderates prevailed. Influenced especially by such science fantasy as William Gibson's *Neuromancer* (1984), John Brunner's *The Shockwave Rider* (1975), and cyberpunk, which is a fusion of elements of electronic communication technology and the "punk" subculture, the hacker ethic promotes resistance to the very forms that create it. Suggestive of Frazer's (1922) *The Golden Bough*, power is challenged and supplanted by rituals combining both destruction and rejuvenation. From this emerges a shared ethos of opposition against perceived Orwellian domination by an information-controlling elite :

> (Hackers will) always be necessary, especially in the technological oppression of the future. Just imagine an information system that systematically filters out certain obscene words. Then it will move on to phrases, and then entire ideas will be replaced by computers ! Anyway, there will always be people tripping out on paper and trying to keep it to themselves, and it's up to us to at least loosen their grasp.
> P.A. message log, 1988

Another hacker summarized the near-anarchist ethic characterized the CU style :

> Lookit, we're here as criminal hobbyists, peeping toms, and looters. I am in it for the fun. Not providing the public what it has a right to know, or keeping big brother in check. I couldn't care less. I am sick of the old journalistic hackers nonsense about or (oops ! OUR) computerized ego... I make no attempt to justify what I am doing. Because it doesn't matter. As long as we live in this goddamn welfare state I might as well have some fun taking what isn't mine, and I am better off than those welfare-assholes who justify their stealing. At least I am smart enough to know that the free lunch can't go on forever.
> U.U. message log, 1988

In sum, the hacker style reflects well-defined goals, communication networks, values, and an ethos of resistance

to authority. Because hacking requires a broader range of knowledge than does phreaking, and because such knowledge can be acquired only through experience, hackers tend to be both older and more knowledgeable than phreaks. In addition, despite some overlap, the goals of the two are somewhat dissimilar. As a consequence, each group constitutes a separate analytic category.

Phreaks

> Running numbers is not only fun; it's a moral imperative !
> -- Phreak credo

Phreaking broadly refers to the practice of using either technology or telephone credit card numbers (called "codez") to avoid long distance charges. Phreaking attained public visibility with the revelation of the exploits of John "Cap'n Crunch" Draper, the "father of phreaking" (Rosenbaum, 1971). Although phreaking and hacking each require different skills, phreaks and hackers tend to associate on same boards. Unlike hackers, who attempt to master a computer system and its command and security structure, phreaks struggle to master telecom (tele-communications) technology :

> The phone system is the most interesting, fascinating thing that I know of. There is so much to know. Even phreaks have their own areas of knowledge. There is so much to know that one phreak could know something fairly important and the next phreak not. The next phreak might know 10 things that the first phreak doesn't though. It all depends upon where and how they get their info. I myself would like to work for the telco, doing something interesting, like programming a switch. Something that isn't slave labor bullshit. Something that you enjoy, but have to take risks in order to participate unless you are lucky enough to work for Bell / AT&T / any telco. To have legal access to telco things, manuals, etc. would be great.
> -- Message log, 1988

Early phreaking methods involved electro-mechanical devices that generated key tones or altered phone line voltages to trick the mechanical switches of the phone company into connecting calls without charging, but the advent of computerized telephone-switching systems largely made these devices obsolete. In order to continue their practice, phreaks have had to learn hacking skills in order to obtain access to telephone company computers and software.

Access to telecom information takes several forms, and the possesion of numbers for "loops" and "bridges", while lying in a grey area of law, further enhances the reputation and status of a phreak. P/hackers can utilize "loop lines" to limit the number of eavesdroppers on their conversations. Unlike bridges, which connect an unlimited number of callers simultaneously, loops are limited to just two people at a time (6). A "bridge" is a technical name for what is commonly known as a "chat line" or "conference system". Bridges are familiar to the public as the pay-per-minute group conversation systems advertised on late night television. Many bridge systems are owned by large corporations that maintain them for business use during the day. While the numbers to these systems are not public knowledge, many of them have been discovered by phreaks who then utilize the systems at night. Phreaks are skilled at arranging for a temporary, private bridge to be created via ATT's conference calling facilities. This provides a helpful information sharing technique among a self-selected group of phreak/hackers :

> Bridges can be extremely useful means of distributing information as long as the [phone] number is not known, and you don't have a bunch of children online testing out their DTMF. The last great discussion I participated with over a bridge occurred about 2 months ago on an AT&T Quorum where all we did was engineer 3/way [calls] and restrict ourselves to purely technical information. We could have convinced the Quorum operators that we were AT&T technicians had the need occurred. Don't let the kids ruin all the fun and convenience of bridges. Lameness is one thing, practicality is another.
> -- DC, message log, 1988

Phreaks recognize their precarious legal position, but see no other way to "play the game" :

> Phreaking involves having the dedication to commit yourself to learning as much about the phone system/network as possible. Since most of this information is not made public, phreaks have to resort to legally questionable means to obtain the knowledge they want.
> -- TP2, message log, 1988

Little sympathy exists among experienced phreaks for "teleco ripoff". "Carding", or the use of fraudulent credit cards, is anathema to phreaks, and not only violates the phreaking ethic, but is simply not the goal of phreaking :

> Credit card fraud truly gives hacking a bad name. Snooping around a VAX is just electronic voyeurism... carding a new modem is just flat out blue-collar crime. It's just as bad as breaking into a house or kicking a puppy ! [This phreak] does everything he can (even up to turning off a number) to get credit information taken off a BBS. [This phreak] also tries to remove codes from BBSes. He doesn't see code abuse in the same light as credit card fraud, (although the law does), but posted codes are the quickest way to get your board busted, and your computer confiscated. People should just find a local outdial to wherever they want to call and use that. If you only make local calls from an outdial, it will never die, you will keep out of trouble, and everyone will be happy.
> -- *Phrack*, 3(28) : Phile 2

Experienced phreaks become easily angered at novices and "lamerz" who engage in fraud or are interested only in "leeching" (obtaining something for nothing) :

> **Sub ->Carding From ->JB (#208) To ->ALL Date ->02/10/xx 02:22:00 PM** What do you people think about using a parents card number for carding ? For instance, if I had a friend order and receive via next day air on my parents card, and receive it at my parents house while we were on vacation. Do you think that would work ? Cuz then, all that we have to do is to leave the note, and have the bud pick up the packages, and when the bill came for over $1500, then we just say... "Fuck you ! We were on vacation ! Look at our airline tickets !" I hope it does... Its such a great plan !
> **Sub ->Reply to: Carding From ->(xxx) To ->X Date ->02/11/xx 03:16:00 AM** NO IT'S NOT A GREAT IDEA ! WHERE'S YOUR SENSE OF RESPONSIBILITY TO YOUR FAMILY ? ARE THEY ALL IN AGREEMENT WITH YOU ? WOULD YOU WANT ANYONE TO USE YOUR PRIVATE STUFF IN ILLEGAL (AND IMMORAL) ACTIVITIES WITHOUT YOUR KNOWLEDGE ? DIDJA EVER HEAR ABOUT TRUST BETWEEN FAMILY MEMBERS ? IF

YOU'RE GOING TO BE A THIEF (AND THAT'S NOT NEAT LIKE JAMES BOND IN THE MOVIES), TAKE THE RISKS ONLY UPON YOURSELF !

Sub ->Carding From ->(#208) To ->(#47) Date ->02/12/xx 11:18:00 AM Why not ? We have a law that says that we have the right to refuse payment to credit cards if there are fraudulent charges. All we do and it is settled... what is so bad about it ? I'm going for it !

Sub ->Reply to: Carding From ->(xxx) To ->J.B. Date ->02/13/xx 02:08:00 AM APPARENTLY YOU MISSED THE MAIN POINTS I TRIED TO MAKE TO YOU... YOU'RE A THIEF AND A LIAR, AND ARE BETRAYING THE TRUST OF YOUR FAMILY AS WELL AS INVOLVING THEM IN YOUR RISK WITHOUT THEIR KNOWLEDGE. THAT MEANS YOU ARE A FAIRLY SCUMMY INDIVIDUAL IF YOU GO THROUGH WITH IT ! NOW AS TO YOUR "DEFENCE" ABOUT $50 MAXIMUMS AND ERRONEOUS BILLINGS.. LAW MAKES A CLEAR DISTINCTION ABOUT THEFT BY FRAUD (OF WHICH YOU WOULD BE GUILTY). AND IN A LARGER SENSE, YOUR THEFT JUST MAKES IT MORE COSTLY FOR YOU YOU AND EVERYBODY ELSE TO GET CREDIT, AND DO BUSINESS WITH CREDIT CARDS. YOU'RE GOING TO DO WHATEVER YOU DO ANYWAY... DON'T LOOK FOR ANY APPROVAL IN THIS DIRECTION.

Ironically, experienced phreaks are not only offended by such disregard of law, but also feel that "rip-off artists" have no information to share and only increase the risk for the "techno-junkies". Message boards reflect hostility toward apprehended "lamerz" with such comments as "I hope they burn him", or "the lamer probably narked [turned informant] to the pheds [law enforcement agents]". Experienced phreaks also post continual reminders that some actions, because of their illegality, are simply unacceptable :

It should be pointed out however, that should any of you crack any WATS EXTENDER access codes and attempt to use them, you are guilty of Theft of communications services from the company who owns it, and Bell is very willing and able to help nail you ! WATS EXTENDERS can get you in every bit as much trouble as a Blue Box should you be caught.

Ex-phreaks, especially those who are no longer defined by law as juveniles, often attempt to caution younger phreaks from pursuing phreaking :

ZA1 : One thing to consider, also, is that the phone compagny knows where the junction box is for all of the lines that you are messing with and if they get enough complaints about the bills, they may start to check things out (I hope your work is neat). I would guess that the odds are probably against this from happening though, because when each of the people call to complain, they'll probably get a different person from the others. This means that someone at Ma Bell has to notice that all of the complaints are coming from the same area... I don't think anybody there really cares that much about their job to really start noticing things like that... anyway, enjoy !!! My guess is that you're under-age. Anyway, so if they catch you, they won't do anything to you anyway.

ZB1 : Yeah I am a minor (17 years old) I just hope that they don't cause I would like to not have a criminal or juvenile record when I apply to college. Also if they do come as I said in the other message if there are no wires they can't prove shit. Also as I said I only hook up after 6 p.m. The phone company doesn't service people after 6 p.m. Just recently (today) I hooked up to an empty line. No wires were leading from the two plugs to somebody house but I got a dial tone. How great. Don't have to worry about billing somebody else. But I still have to disconnect cause the phone bills should be coming to the other people pretty soon. HEHEHEHE.

ZX1

: Be cool on that, especially if you're calling other boards. Easiest way for telecom security to catch you is match the number called to the time called, call the board, look at users log or messages for hints of identity, then work from there. If you do it too much to a pirate board, they can (and have successfully) pressured the sysop to reveal the identity under threat of prosecution. They may or may not be able to always trace it back, but remember : yesterday's phreaks are today's telecom security folk. AND : IT'S NOT COOL TO PHREAK TO A PIRATE BOARD... draws attention to that board and screws it up for everybody. So, be cool phreaking... there's safer ways.
ZC2 : Be cool, Wormburger. They can use all sorts of stuff for evidence. Here's what they'd do in Ill. If they suspected you, they'd flag the phone lines, send somebody out during the time you're on (or they suspect you're on) and nail you. Don't want to squelch a budding phreak, but you're really taking an unnecessary chance. Most of us have been doing stuff for some time, and just don't want to see you get nailed for something. There's some good boards with tips on how to phreak, and if you want the numbers, let me know. We've survived to warn you because we know the dangers. If you don't know what ESS is, best do some quick research.
-- P/h message log, 1988

In sum, the attraction of phreaking and its attendant lifestyle appear to center on three fundamental characteristics : the quest for knowledge, the belief in a higher ideological purpose of opposition to potentially dangerous technological control, and the enjoyment of risk-taking. In a sense, CU participants consciously create dissonance as a means of creating social meaning in what is perceived as an increasingly meaningless world (Milovanovic and Thomas, 1989). Together, phreaks and hackers have created an overlapping culture that, whatever the legality, is seen by participants as a legitimate enterprise in the new "techno-society".

Conclusion

The transition to an information-oriented society dependent on computer technology brings with it new symbolic metaphors and behaviors. Baudrillard (1987: 15) observed that our private sphere now ceases to be the stage where the drama of subjects at odds with their objects and with their image is played out, and we no longer exist as playwrites or actors, but as terminals of multiple networks. The public space of the social arena is reduced to the private space of the computer desk, which in turn creates a new semi-public, but restricted, public realm to which dissonance seekers retreat. To participate in the computer underground is to engage in what Baudrillard (1987: 15) describes as private telematics, in which individuals, to extend Baudrillard's fantasy metaphor, are transported from their mundane computer system to the controls of a hypothetical machine, isolated in a position of perfect sovereignty, at an infinite distance from the original universe. There, identity is created through symbolic strategies and collective beliefs (Bordieu, cited in Wacquant, 1989: 35).

We have argued that the symbolic identity of the computer underground creates a rich and diverse culture comprised of justifications, highly specialized skills, information-sharing networks, norms, status hierarchies, language, and unifying symbolic meanings. The stylistic elements of CU identity and activity serve what Denzin (1988: 471) sees as the primary characteristic of postmodern behavior, which is to make fun of the past while keeping it alive and the search for new ways to present the unpresentable in order to break down the barriers that keep the profane out of the everyday.

The risks entailed by acting on the fringes of legality and substituting definitions of acceptable behavior with their own, the playful parodying of mass culture, and the challenge to authority constitute an exploration of the limits of techno-culture while resisting the legal meanings that would control such actions. The celebration of

anti-heros, re-enacted through forays into the world of computer programs and software, reflects the stylistic promiscuity, eclecticism and code-mixing that typifies the postmodern experience (Featherstone, 1988: 202). Rather than attempt to fit within modern culture and adapt to values and definitions imposed on them, CU participants mediate it by mixing art, science, and resistance to create a culture with an alternative meaning both to the dominant one and to those that observers would impose on them and on their enterprise.

Pfuhl (1987) cogently argued that criminalization of computer abuse tends to polarize definitions of behavior. As a consequence, to view the CU as simply another form of deviance, or as little more than "high-tech street gangs" obscures the ironic, mythic, and subversive element, the Nieztschean "will to power", reflected in the attempt to master technology while challenging those forces that control it. The "new society" spawned by computer technology is in its infancy, and, as Sennet (1970 : xvii) observed, the passage of societies through adolescence to maturity requires acceptance of disorder and painful dislocation.

Instead of embracing the dominant culture, the CU has created an irreducible cultural alternative, one that cannot be understood without locating its place within the dialectic of social change. Especially in counter-cultures, as Hebdige (1983: 3) observes, "objects are made to mean and mean again", often ending :

> In the construction of a style, in a gesture of defiance or contempt, in a smile or a sneer. It signals a Refusal. I would like to think that this Reusal is worth making, that these gestures have a meaning, that the smiles and the sneers have some subversive value...
> -- Hebdige (1982: 3)

Footnotes

1. Participants in the computer underground engage in considerable word play that includes juxtaposition of letters. For example, commonly used words beginning with "f" are customarily spelled with a "ph". The CU spelling conventions are retained throughout this paper.

2. Conly and McEwen (1990: 3) classify "software piracy" in the same category as theft of computers and trade secrets, and grossly confuse both the concept and definition of computer crime by conflating any illicit activity involving computers under a definition so broad that embezzlement and bulletin boards all fall within it. However, the label of "computer criminal" should be reserved for those who manipulate computerized records in order to defraud or damage, a point implied by Bequai (1978: 4) and Parker (1983: 106).

3. One author has been active in the computer underground since 1984 and participated in Summercon-88 in St. Louis, a national conference of elite hackers. The other began researching p/hackers and pirates in 1988. Both authors have had sysop experience with national CU boards. As do virtually all CU participants, we used pseudonyms but, as we became more fully immersed in the culture, our true identities were sometimes revealed.

4. Although we consider software pirates an integral part of the computer underground, we have excluded them from this analysis both for parsimony and because their actions are sufficiently different to warrant separate analysis (Thomas and Meyer, 1990). We also have excluded anarchist boards, which tend to be utilized by teenagers who use BBSs to exchange information relating to social disruption, such as making homemade explosives, sabotaging equipment, and other less dramatic pranks. These boards are largely

symbolic, and despite the name, are devoid of political intent. However, our data suggest that many hackers began their careers because of the anarchist influence.

5. In January, 1990, the co-editor of the magazine was indicted for allegedly "transporting" stolen property across state lines. According to the Secret Service agent in charge of the case in Atlanta (personal communication), the offender was apprehended for receiving copies of E911 ("enhanced" 911 emergency system) documents by electronic mail, but added that there was no evidence that those involved were motivated by, or received, material gain.

6. "Loop lines" are telephone company test lines installed for two separate telephone numbers that connect only to each other. Each end has a separate phone number, and when each person calls one end, they are connected to each other automatically. A loop consists of "Dual Tone Multi-Frequency", which is the touch tone sounds used to dial phone numbers. These test lines are discovered by phreaks and hackers by programming their home computer to dial numbers at random and "listen" for the distinctive tone that an answering loop makes, by asking sympathetic telephone company employees, or through information contained on internal company computers.

Bibliography

Allman, William F. 1990. "Computer Hacking goes on Trial". U.S. News and World Report, January 22: 25.

Altheide, David L. 1985. *Media Power*. Beverly Hills : SAGE.

Baudrillard, Jean. 1987. *The Ecstasy of Communication*. New York : Semiotext(e).

Bell, 1976. *The Cultural Contradictions of Capitalism*. New York : Basic Books.

Bequai, August. 1987. *Technocrimes*. Lexington (Mass.) : Lexington. 1978. *Computer Crime*. Lexington (Mass.) : Lexington.

Bloombecker, Jay. 1988. Interview, Hour Magazine. NBC television, November 23.

Bordieu, Pierre. 1989. "Social Space and Symbolic Power". Sociological Theory, 7 (Spring) : 14-25.

Brunner, John. 1989. *The Shockwave Rider*. New York : Ballantine. Callinicos, Alex. 1985. "Posmodernism, Post-Structuralism, Post-Marxism ?" Theory, Culture and Society, 2(3) : 85-101.

Camper, John. 1989. "Woman Indicted as Computer Hacker Mastermind". Chicago Tribune, June 21 : II-4. "Civil Liberties Hacked to Pieces: Jolyon Jenkins Refuses to Panic over Computer Crime". New Statesman & Society, February 9: 27. "Computer Expert's Son Cited as Virus Creator". 1988. Chicago Tribune, November 5: 1, 2. "Computer Hacker Ring with a Bay Area Link". 1990. San Francisco Chronicle, May 9 : A-30. "Computer Saboteur gets Probation". 1988. Chicago Tribune, Oct. 22: 4.

Conly, Catherine H. 1989. *Organizing for Computer Crime Investigation and Prosecution*.

Conly, Catherine H. and J. Thomas McEwen. 1990. "Computer Crime". NIJ Reports, 218 (January/February) : 2-7.

Cooley, Ronald B. 1984. "RICO: Modern Weaponry against Software Pirates". Computer Law-Journal, 5 (Fall) : 143-162.

Denzin, Norman K. 1988. "Blue Velvet: Postmodern Contradictions". Theory, Culture and Society. 5 (June) : 461-473.

"Doctor Crash". 1986. "The Techno-Revolution". *Phrack*, 1(6) : Phile 3.

"EB" [anonymous computerphile]. 1990. *Phrack*, 3(31) : File 6.

Featherstone, Mike. 1988. "In Pursuit of the Postmodern: An Introduction". Theory, Culture and Society, 2-3 (June) : 195-215.

Harper's Forum. 1990. "Is Computer Hacking a Crime ? A Debate from the Electronic Underground". Harper's, 280 (March) : 45-57.

Frazer, James G. 1922. *The Golden Bough*. New York : MacMillan.

Geertz, Clifford. 1973. *The Interpretion of Cultures*. New York : Basic Books. 1973.

Gibson, William. 1984. *Neuromancer*. New York : Ace.

Glaser, Barney G. and Anselm L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago : Aldine.

Goodenough, Ward. 1981. *Culture, Language, and Society*. Menlo Park (Calif.) : Benjamin/Cummings.

"Hacker, 18, Gets Prison for Fraud". 1989. Chicago Tribune, February 15 : III-1.

Hebdige, Dick. 1982. *Subculture: The Meaning of Style*. New York : Metheun.

Hollinger, Richard C. and Lonn Lanza-Kaduce. 1988. "The Process of Criminalization: The Case of Computer Crime Laws". Criminology, 26 (February) : 101-126.

Kane, Pamela. 1989. *V.I.R.U.S. Protection: Vital Information Resources under Siege*. New York : Bantam.

Landreth, Bill. 1985. *Out of the Inner Circle: A Hacker's Guide to Computer Security*. Belleview (Wash.) : Microsoft Press.

Lash, Scott. 1988. "Discourse or Figure ? Postmodernism as 'Regime of Signification'". Theory, Culture and Society, 5 (June) :311-336.

Latimer, Dan. 1984. "Jameson on Post-Modernism". New Left Review, 148 (November/December) : 116-128.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. Garden City : Doubleday.

Lyotard, Jean-Francois. 1988. *The Postmodern Condition: A Report on Knowledge*. Minneapolis : University of Minnesota Press.

Manning, Peter K. (forthcoming). "Strands in the Postmodernist Rope: Ethnographic Themes". in N. Denzin (ed.), Studies in Symbolic Interaction (Vol. 13). Greenwich (Conn.) : JAI.

Markoff, John. 1990a. "3 Arrests Show Global Threat to Computers". New York Times, April 4, A1, A11. 1990b. "Drive to Counter Computer Crime Aims at Invaders". The New York Times, June 3: 1, 21.

Marx, Gary T. 1988a. *Undercover: Police Surveillance in America*. Berkeley : University of California Press. 1988b. "The Maximum Security Society". Deviance et Societe, 12(2) : 147-166.

Marx, Gary T., and Nancy Reichman. 1985. "Routinizing the Discovery of Secrets: Computers as Informants". Software Law Journal, 1 (Fall) : 95-121.

McEwen, J. Thomas. 1989. *Dedicated Computer Crime Units*. Washington D.C. : National Institute of Justice.

Meyer, Gordon R. 1989a. *The Social Organization of the computer underground*. Unpublished Masters Thesis, Northern Illinois University. 1989b. "Hackers, Phreakers, and Pirates: The Semantics of the Computer Age". Pp. 74-82 in P. Kane, *V.I.R.U.S. Protection: Vital Information Resources under Siege*. New York : Bantam.

Meyer, Gordon R. and Jim Thomas. 1989. "Role Differentiation in the computer underground". Paper presented at the Society for the Study of Social Problems annual meetings, Berkeley, August.

Michalowski, Raymond J. and Erdwin H. Pfuhl. 1990 (forthcoming). "Technology, Property, and Law: The Case of Computer Crime". Contemporary Crisis.

Milovanovic, Dragan, and Jim Thomas. 1989. "Overcoming the Absurd: Prisoner Litigation as Primitive Rebellion". Social Problems 36 (February) : 48-60.

Newman, Charles. 1985. *The Post-Modern Aura: The Act of Fiction in an age of Inflation*. Evanston (Ill.) : Northwestern University Press.

Parker, Donn B. 1983. *Fighting Computer Crime*. New York : Charles Scribner's Sons.

Pfuhl, Erdwin H. 1987. "Computer Abuse: Problems of Instrumental Control". Deviant Behavior, 8(2) : 113-130.

Rosenbaum, Ron. 1971. "Secrets of the Little Blue Box". Esquire, 76 (October) : 116-1125, 222-226.

Rosenblatt, Kenneth. 1990. "Deterring Computer Crime". Technology Review, 93 (February/March) : 34-40.

Sandza, Richard. 1984a. "The Night of the Hackers". Newsweek, 104 (November 12) : 17-18. 1984b. "Revenge of the Hackers". Newsweek, 104 (December 10) : 25.

Schwartz, Eddie. 1988. "Special on 'Computer Hacking'". WGN Radio, Sept 27.

Schwartz, John. 1990. "The Hacker Dragnet: The Feds Put a Tail on Computer Crooks -- and Sideswipe a few Innocent Bystanders". Newsweek, April 30: 50.

Sennett, Richard. 1979. *The Uses of Disorder: Personal Identity and City Life*. New York : Vintage Books.

Stoll, Clifford. 1989. *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. New York : Doubleday.

Thomas, Jim and James B. Marquart. 1988. "Dirty Knowledge and Clean Conscience: The Dilemmas of Ethnographic Research". Pp. 81-96 in D. Maines and C. Couch (eds.), *Information, Communication and Social Structure*. Springfield, Ill. : Charles C. Thomas.

Thomas, Jim and Gordon R. Meyer. (Forthcoming). "(Witch)Hunting for the Computer Underground: Joe McCarthy in a Leisure Suit". The Criticial Criminologist.

Tompkins, Joseph B., Jr., and Linda A. Mar. 1986. "The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem". Computer-Law Journal, 6 (Winter) : 459-481.

Van, John. 1989. "Oddballs no More, Hackers are now a Threat". Chicago Tribune, March 5, IV : 4.

Van Maanen, John, and Stephen Barley. 1985. "Cultural Organization: Fragments of a Theory". Pp. 31-53 in P.J. Frost, et al., (eds.), Organizational Culture. Beverly Hills : Sage.

Wacquant, Loic J.D. 1989. "Towards a Reflexive Sociology: A Workshop with Pierre Bordieu". Sociological Theory, 7 (Spring) : 26-63.

Winter, Christine. 1988. "Virus Infects Huge Computer Network". Chicago Tribune, November 4, 1, 18. "Yes, You Sound very Sexy, but I Really Need a Probation Officer". 1989. Chicago Tribune, June 13, 10.

WMAQ Evening News. 1990. (Channel 5, Chicago), February 6.

Zablit, Jocelyne. 1989. "Fraud Sweep Nabs 2 Michigan Teens in Computer Ring". Detroit Free Press, 25 May : 1, 18.