OUTLAW MENTALITY
Bulletin Board System community
Phrack

Private Sector Damaged/Returning

The Private Sector, which was supposed to have been returned by the 16th of February, 1986 had been damaged in the hands of the authorities. According to them, "one of the cards blew up." They say that this happened before they had the chance to erase the two "illegal" files they found on the hard drive. So now then they had to hold onto it a bit longer. Naturally 2600 Magazine suspected intentional foul play and stepped up the pressure on them to return Private Sector. 2600 suspected the card they authorities were referring to was the hard disk controller. They wouldn't stick another controller from another machine in and they wouldn't let 2600 Magazine even look at the machine. What an outrage!

On Friday, February 28, 2600 Magazine announced the following.

Private Sector has finally been returned, and is in the process of being repaired. It will be back up in the near future at the same number as before; 201-366-4431. Call 2600 Magazine at 516-751-2600 for more details.

At the current writing of this article, Private Sector is up and running. Only time will tell if it will ever be the great bbs it once was.

Information provided by 2600 Magazine

OUTLAWS...?
Phrack Volume One, Issue Five, Phile #10 of 12
Phrack World News Issue 4 Part 1 Compiled by Knight Lightning (April 1986)
Dear Mr. King,
This law firm is counsel to Master Lock Company. Our client has recently been alerted to the dissemination through a Bulletin Board Computer Service located at your address of information potentially damaging to its commercial interests and business relationships. More particularly, we refer to the publication by such computer service of instructions for picking combination locks manufactured by Master Lock Company.

Etc etc....
will take every legal recourse available to it to do so. Under the present circumstances, however, our client would first like to give you the opportunity to take measures to prevent activities that it can only view as malicious both toward itself and toward its customers. … Your compliance with this request is all that is required for an amicable resolution of this matter.

This letter is of course talking about phile #6 of Phrack Issue I, entitled, "How To Pick Master Locks".

Dear Sirs,   4/1/86

My name is Taran King, as you so easily researched, and I used to run Metal Shop, an electronic bulletin board system. I currently run a private line for personal friends of mine, and if asked, I distribute "general files" for them. The fact that I distributed the file is hardly the point. I merely obtained it from the authors of the file and distributed it to other sources, who apparently distributed it other places. If I am responsible for this file, I
believe you should find a number of other authors also.

It is not only this file that you have written me about that the information about the "secret" to picking Master locks is included in, but also
a number of other files that have been circulating for years. It is old information, someone just re-published it.

Although on this topic, I am not well informed, I believe it is legal to print information on such a topic. We do not condone the actions promoted by the files, but merely inform the public on the topic of this. I hate to run on, but I wish to make my point as clearly as possible.
   If I, being one of the people it was passed through, am responsible for the crime rate today of people picking Master, American, or any other company's locks, then I believe anyone who has the file, or has read books should be arrested on this. I believe Paladin Press publishes a number of books on this
topic. I have seen one of the "Picking Master Locks in 3-Easy Steps!" type books and as far as I know, it's still in publication and distribution.
   I hope I'm not sounding disrespectful or condescending, but it annoys me to a great degree when I must be questioned by my father about a letter that has come in the mail from a law firm in New York. Please expect a letter from him inquiring upon the topic that you have written me on.

THICK AS THIEVES

Phrack Volume One, Issue Five, Phile #10 of 12
(April 1986)
Mister Carding Busted

Mister Carding first started in the profession of which his name comes forth in the summer of 1984. Since then he has accumulated roughly $45,000 worth of merchandise.

He was caught once before in the summer of 1985 by Federal agents. However, as the investigation went on, they didn't have enough material and dropped the charges.

Somewhere around the fourth week of February he was caught again, this time by local authorities. Here is how it all started:

"Two months ago, I had tons of stuff coming in and had another guy picking it up. One night two weeks or so ago I had him go out to pick up a 20 meg 3 ½ inch hard drive. It was only the second time I had used that place as a drop spot.

Unfortunately, he walked right into a police stakeout and he was followed, first to my house and then to his own."

The next day the police went to the house of the friend and arrested him. He willingly signed an affidavit stating that Mr. Carding was the mastermind behind the whole operation and that he was just an accomplice.

The court date has not yet been set but his crimes are as follows:
- Fraudulent use of a credit card.
- Possession of stolen merchandise in excessive amounts.
- Computer Invasion (Hacking).

On March 6, 1986:
- The police confiscated his modem. It had been carded.
- He had a meeting with the detectives, in which he had to take a lie detector test. They asked him if he was lying about any part of the case, if he hacked into computers, and if he was using one specific person's card.
- He failed the test.

The police believe he hacked into the computer of a bank in New Jersey, Mr. carding denies all of it. However it is the truth.
Most people didn't know it but Mr. Carding was one of the better hackers around and should be remembered.

He is pleading innocent to all charges and has signed a reverse affidavit stating that the other guy was the mastermind.

He, as of this writing, has not been arrested but expects to have full charges brought on him within the next week.

Information provided by Mister Carding

Anarchist Politics:
THE TECHNO-REVOLUTION

Phrack Volume One, Issue Six, Phile 3 of 13
Article By Doctor Crash

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.

To fully explain the true motives behind hacking, we must first take a quick look into the past. In the 1960's, a group of MIT student 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.

Hackers realize that the businesses aren't the only ones who are entitled to modern technology. They tap into online systems and use them to their own advantage. Of course, the government doesn't want the monopoly of technology broken, so they have outlawed hacking and arrest anyone who is caught.

Even worse than the government is the security departments of businesses and companies. They act as their own "private armies" and their ruthless tactics are overlooked by the government, as it also serves their needs.

Hacking is a major facet of the fight against the computer monopoly. One of the ways hackers accomplish their means has developed into an art in itself:
Phone Phreaking. It is essential that every Hacker also be a Phreak, because it is necessary to utilize the technology of the phone company to access computers far from where they live. 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 inexorbitantly 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.

There is one last method of this war against computer abusers. This is a less subtle, less electronic method, but much more direct and gets the message across. I am speaking of what is called Anarchy. Anarchy as we know it does not refer to the true meaning of the word (no ruling body), but to the process
of physically destroying buildings and governmental establishments. This is a
very drastic, yet vital part of this "techno-revolution."

Hacking must continue. We must train newcomers to the art of hacking. We must also increase computer Crashing. I know that crashing a computer seems a waste, but when there is no other way to subvert a business, their system must be shut down.

As I stated above, this is only on the motives. If you need a tutorial on how to perform any of the above stated methods, please read a 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.

NB: George Woodcock's famous "Anarchist Reader" – a guide to 19th and 20th century writers and activists, first published in a small edition in 1977, was republished in a new edition in 1986, by Fontana.

This book featured, among others, the story of Bakunin, the Russian activist who battled Karl Marx for control of the Socialist International, the body which co-ordinated the European socialist movement. Marx won, and redefined socialism with his concept of the People's State – until then a paradox as far as socialist thought was concerned. Old-style socialists, who could not countenance any State at all, renamed their movement Anarchism.

The book also introduced Proudhon, author of "The Conquest of Bread", which lays out the philosophy of anarchism.

The Conscience of a Hacker

Phrack Volume One, Issue 7, Phile 3 of 10

By The Mentor

Written on January 8, 1986

The following was written shortly after my arrest...

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

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...

Or feels threatened by me... Or thinks I'm a smart ass... Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

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 the 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...
Damn kid. Tying up the phone line again. They're all alike...
You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless.

We've been dominated by sadists, or
ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.
This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us
and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.
I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

NOVICE'S GUIDE TO HACKING 1989edition

Phrack Volume Two, Issue 22, File 4 of 12
by The Mentor
Legion of Doom/Legion of Hackers
Part 1: What is Hacking, A Hacker's Code of Ethics, Basic Hacking Safety

Part One: The Basics
~~~~~~~~~~~~~~~~~~~~~~

As long as there have been computers, there have been hackers. In the 50's at the Massachusets Institute of Technology (MIT), students devoted much time and energy to ingenious exploration of the computers. Rules and the law were isregarded in their pursuit for the 'hack.' Just as they were enthralled with
their pursuit of information, so are we. The thrill of the hack is not in breaking the law, it's in the pursuit and capture of knowledge.

To this end, let me contribute my suggestions for guidelines to follow to ensure that not only you stay out of trouble, but you pursue your craft without damaging the computers you hack into or the companies who own them.

I. Do not intentionally damage *any* system.
II. Do not alter any system files other than ones needed to ensure your escape from detection and your future access (Trojan Horses, Altering Logs, and the like are all necessary to your survival for as long as possible).
~~~~~~~~~~~~~~~~~~~~~~

III. Do not leave your (or anyone else's) real name, real handle, or real phone number on any system that you access illegally. They *can* and will track you down from your handle!
IV. Be careful who you share information with. Feds are getting trickier. Generally, if you don't know their voice phone number, name, and occupation or haven't spoken with them voice on non-info trading conversations, be wary.
V. Do not leave your real phone number to anyone you don't know. This includes logging on boards, no matter how k-rad they seem. If you don't know the sysop, leave a note telling some trustworthy people that will validate you.
VI. Do not hack government computers. Yes, there are government systems that are safe to hack, but they are few and far between. And the government has inifitely more time and resources to track you down than a company who has to make a profit and justify expenses.
VII. Don't use codes unless there is *NO* way around it (you don't have a local telenet or tymnet outdial and can't connect to anything 800). You use codes long enough, you will get caught. Period.
VIII. Don't be afraid to be paranoid. Remember, you *are* breaking the law. It doesn't hurt to store everything encrypted on your hard disk, or keep your notes buried in the backyard or in the trunk of your car. You may feel a little funny, but you'll feel a lot funnier when you when you meet Bruno, your transvestite cellmate who axed his family to death.
IX. Watch what you post on boards. Most of the really great hackers in the country post *nothing* about the system they're currently working except in the broadest sense (I'm working on a UNIX, or a COSMOS, or something generic. Not "I'm hacking into General Electric's Voice Mail System" or something inane and revealing like that).
X. Don't be afraid to ask questions. That's what more experienced hackers are for. Don't expect *everything* you ask to be answered, though. There are some things (LMOS, for instance) that a begining hacker shouldn't mess with. You'll either get caught, or screw it up for others, or both.
XI. Finally, you have to actually hack. You can hang out on boards all you want, and you can read all the text files in the world, but until you actually start doing it, you'll never know what it's all about. There's no thrill quite the same as getting into your first system (well, ok, I can think save a couple of biggers thrills, but you get the picture).

One of the safest places to start your hacking career is on a computer system belonging to a college. University computers have notoriously lax security, and are more used to hackers, as every college computer department has one or two, so are less likely to press charges if you should be detected. But the
odds of them detecting you and having the personel to committ to tracking you down are slim as long as you aren't destructive.

If you are already a college student, this is ideal, as you can legally explore your computer system to your heart's desire, then go out and look for similar systems that you can penetrate with confidence, as you're already
familar with them.

So if you just want to get your feet wet, call your local college. Many of them will provide accounts for local residents at a nominal (under $20) charge. Finally, if you

get caught, stay quiet until you get a lawyer. Don't volunteer any information, no matter what kind of 'deals' they offer you. Nothing is
binding unless you make the deal through your lawyer, so you might as well shut up and wait.

A Report On The InterNet Worm

Phrack Volume Two, Issue 22, File 8 of 12
By Bob Page
University of Lowell
Computer Science Department
November 7, 1988

Here's the truth about the "Internet Worm." Actually it's not a virus - a virus is a piece of code that adds itself to other programs, including operating systems. It cannot run independently, but rather requires that its
"host" program be run to activate it. As such, it has a clear analog to biologic viruses -- those viruses are not considered live, but they invade host cells and take them over, making them produce new viruses.

A worm is a program that can run by itself and can propagate a fully working version of itself to other machines. As such, what was loosed on the Internet was clearly a worm.

……………

If you haven't read or watched the news, various log files have named the responsible person as Robert Morris Jr., a 23-year old doctoral student at Cornell. His father is head of the National Computer Security Center, the
NSA's public effort in computer security, and has lectured widely on security aspects of UNIX.

Associates of the student claim the worm was a 'mistake' - that he intended to unleash it but it was not supposed to move so quickly or spread so much. His goal was to have a program 'live' within the Internet. If the reports that he intended it to spread slowly are true, then it's possible that the bytes sent to ernie.berkeley.edu were intended to monitor the spread of the worm. Some news reports mentioned that he panicked when, via some "monitoring mechanism" he saw how fast it had propagated.

Cf. Tony Blair’s son Euan being picked up for drunkenness in Leicester Square, Jack Straw’s son being arrested for dealing cannabis, etc etc
Morris: the archetypal teenage rebel………..

Excerpt from
The History of The Legion Of Doom

Phrack Volume Three, Issue Thirty-one, Phile #5 of 10

The Legion of Doom has been called everything from "Organized Crime" to "a Communist threat to national security" to "an international conspiracy of computer terrorists bent on destroying the nation's 911 service." Nothing comes closer to the actual truth than "bored adolescents with too much spare time."
LOD members may have entered into systems numbering in the tens of thousands, they may have peeped into credit histories, they may
have monitored telephone calls, they may have snooped into files and buffered interesting text, they may still have total control over
entire computer networks; but, what damage have they done? None, with the exception of unpaid use of CPU time and network access charges. What personal gains have any members made? None, with the exception of three instances of credit fraud that were instigated by three separate greedy individuals, without group knowledge.

Profile of Chris Goggans

Phrack Volume Three, Issue Thirty-five, File 3 of 13
by S. Leonard Spitz
Associate Publisher, INFOSecurity Product News

Malicious hackers, even though most operate undercover, are often notorious for the colorful pseudonyms they travel under. Reformed hackers, however, prefer a low profile so as to shed their image of perceived criminality. Kevin Mitnick, infamous for the DEC caper, is one of the foremost advocates of this strategy.
Now comes Chris Goggans, trailing his former "Legion of Doom" moniker, Erik Bloodaxe, behind him, to try it his way. Goggans insists that where once he may have bent the rules, he is now ready to give something back to society. And coming across with a high degree of sincerity, he affirms his intention to try. Are he and his colleagues, wearing their newly acquired information security consultants hats, tilting at windmills, or does their embryonic, cracker-breaking start-up, Comsec Data Security Co., stand a fighting chance? We thought we would ask him.

Chris Goggans: There certainly was activity going on within the group that could be considered illegal. But most of this was taking place when members of the group were all between the ages of 14 and 17. While I don't want to blame immaturity, that's certainly a factor to be considered.

We never said "This is a computer and this is how to break into it."

Colorful names and words used to describe groups also add to notoriety. If we had been the "Legion of Flower Pickers," the "Legion of Good Guys," or the "SuperFriends," there probably wouldn't be this dark cloud hanging over the group.

NB The Legion of Doom was the name chosen by the group's founder, whose handle was Lex Luthor. In the Superman Stories, Lex is involved in a group of the same name.

ISPNews: What is your definition of a hacker?

CG: A Hacker is someone who wants to find out everything that there is to know about the workings of a particular computer system, and will exhaust every means within his ability to do so.

ISPNews: Would you also comment on the ethics of hacking?

CG: There is an unwritten code of ethics that most people tend to adhere to. It holds that: no one would ever cause damage to anything; and
no one would use any information found for personal gain of any kind. For the most part, the only personal gain that I have ever seen from any sort of hacking activity is the moderate fame from letting others know about a particular deed. And even in these cases, the total audience has been limited to just a few hundred.

ISPNews: Are you unaware of hackers who have in fact accessed information, then sold it or massaged it for money?

CG: No, certainly not. I am just acknowledging and defining a code of ethics. We of the Legion of Doom tried to adhere to that code of ethics. For example, members of the original nine who acted unethically were removed from the group.

ISPNews: Do you believe that penetrating a computer system without either making changes or removing information is ethical, or a least is not unethical?

CG: At one time in the past I may have held that belief, but now I certainly must not, because the whole idea of being involved in the formation of my new company, Comsec Data Security, would show otherwise.

ISPNews: So today, you believe that unauthorized entry is unethical.

CG: Exactly. As a hacker, I didn't particularly hold that. But as things such as invasion of privacy, even though I never caused any damage, and breach of trust became more apparent to me, I was able to step back, see the picture, and realize it was wrong.

ISPNews: What are your views on the ownership of information?

CG: I feel that proprietary information, national-security-related information, information that could be considered a trade secret, all definitely have ownership, and access should be restricted. In the past, I felt that information that affected me or had some relevance to my life should be available to me. I felt that information should be available to the people it affected, whether that be phone company information, credit bureau information, banking information, or computer system information in general. I am saying this in the past tense. In the present tense, I feel that the public is entitled only to information in the public domain. Information not available legally through normal channels is just going to have to be left at that.

ISPNews: Do you believe that software should always be in the public domain.?
CG: No, I do not. If I wrote something as wonderful as Lotus, or any of the Microsoft programs, or Windows, I would want people to pay for them.

COMPUTER UNDERGROUND DIGEST

Volume 1, Issue #1.00 (March 28, 1990)
Introduction

Over the past few years I've often been asked to justify the use of "computer underground" when referring to the realm of hackers, phreakers, and pirates. Certainly the "computer" part is easy to justify, or at least accept as valid. No, it's the "underground" that has been criticized. Now I certainly don't claim to have invented the term, in fact it is taken from the vocabulary of the p/hackers themselves. However "underground" does imply, at least in common usage, some characteristics that are not necessarily accurate. Some of these are organization, criminality (or at lest marginality), unity, and purposiveness.

Does the CU display these characteristics? Discussing each would take much more room than I intend to use today. My M.A. thesis of August 1989 addressed the issues of organization and unity, from a sociological viewpoint. The articles included in this issue of the Digest address all of the a fore mentioned issues from another viewpoint, one formed largely by cultural outsiders. The issue that faces us now is who gets to define what the CU is all about? Do we rely on the Federal Justice department to identify and label the intent, organization, and purpose of the CU as conspirical? Do we rely on the media to define the CU as reckless and unlawful? Do we, as citizens, trust those in power to make decisions that will forever impact the way our societal institutions of control approach those whose application of technology has out paced our conceptions of private property and crime?

Am I an advocate _for_ the computer underground? No, I'm not "one of them" and I don't speak for "them". However I do think it is in the best interest of all if the "problem" of the CU is approached from the new perspective it deserves. If our society is to ultimately decide that CU activity is every bit as terrible as puppy-whipping then that decision should be made, not forced upon us by lawmakers (and others) who are assuming, from the very beginning, that CU activity is threatening and criminal.

Hackers and Left Politics

by L. Proyect Columbia University
http://www.columbia.edu/~lnp3/mydocs/computers/hackers.htm

Some of the key pioneers in the personal computing revolution were not driven by entrepeneurial greed. For example, the Community Memory project in Berkeley, California was launched in 1973 by Lee Felsenstein. The project allowed remote public access to a time-shared XDS mainframe in order to provide "a communication system which allows people to make contact with each other on the basis of mutually expressed interests, without having to cede judgement to third parties." The Community Memory project served as a kind of bulletin board where people could post notes, information, etc., sort of like an embryonic version of the Internet. Felsenstein, born in 1945, was the son of a CP district organizer and got involved in civil rights struggles in the 1950's. Eventually, he hooked up with the Free Speech Movement at Berkeley and became a committed radical. Lee's other passion was electronics and he entered the UC as an electrical engineering major.

Felsenstein then hooked up with another left-of-center computer hacker by the name of Bob Halbrecht and the two went on to form a tabloid called PCC "People's Computer Company". Among the people drawn to the journal was Ted Nelson, a programmer who had bounced from one corporate job to another throughout the 60's but who was always repelled by "the incredible bleakness of the place in these corridors."

Nelson was the author of "Computer Lib" and announced in its pages that "I want to see computers useful to individuals, and the sooner the better, without unnecessary complication or human servility being required." Community Memory flourished for a year and a half until the XDS started breaking down too often The group disbanded in 1975.
The PCC continued, however, and played a key role in publicizing the earliest personal computers. One of the machines that Felsenstein and Halbrecht got their hands on was an Altair 8800, the first genuine personal computer for sale to the public.
So enamored of the idea of personal computing were Felsentsein and Halbrecht that they then launched something called the Homebrew Computer Club. The club drew together the initial corps of engineers and programmers who would launch the personal computer revolution. Among the participants were a couple of adolescents named Steven Jobs and Steve Wozniak who went on to form the Apple Corporation.

The hacker ethic which prevailed at the Homebrew Computer Club was decidedly anticapitalist, but not consciously pro-socialist. Software was freely exchanged at the club and the idea of proprietary software was anathema to the club members. There were 2 hackers who didn't share these altruistic beliefs, namely Paul Allen and Bill Gates. When Allen and Gates discovered that their version of Basic which was written for the Altair was being distributed freely at the club, they rose hell. The 19 year old Gates stated in a letter to the club that "Who can afford to do professional work for nothing?"

Another interesting example of the anticapitalist hacker ethic is personified in one Richard Stallman. Stallman worked at the MIT Artificial Intelligence Lab in the early 1970's and, no doubt influenced by the spirit of the age, came to see the lab as the embodiment of a philosophy which "does not mean advocating a dog-eat-dog jungle. American society is already a dog-eat-dog jungle, and its rules maintain it that way. We hackers wish to replace those rules with a concern for constructive cooperation."

Stallman developed EMACS, the most widely used Unix text editor, and went on to form the GNU foundation which distributes EMACS and other free software. When you press ctrl-x, ctrl-w upon entering EMACS, you can read a statement of the GNU foundation which includes the following words "If you distribute copies of a program, whether gratis or for a fee, you must give the recipients all the rights you have. You must make sure that they, too, receive or get the source code." Can one imagine Microsoft Inc. issuing a statement such as this?

I have gone on at length without discussing the Internet. Suffice it to say that the hacker ethic infuses the entire project know as the Internet. What threatens it the most is the mindset best exemplified by Bill Gates who would make every last thing proprietary.

In general, we should resist the temptation to put an equal sign between the so-called free-market and technological advances. There is much evidence that the kind of breakthrough that personal computing represents is to a large degree attributable to the selfless, generous and anticorporate motives of the early hackers.

The Cult of the Dead Cow (cDc)

Douglas Thomas, Hacker Culture pp95-104

The Cult of the Dead Cow are very media aware.
With software such as Linux, it has become possible to completely dissociate hacking from criminality. On the other hand, media representations have come to focus almost exclusively on criminal aspects of hacking.

Oxblood Ruffin speaks:
If there is one general theme that resonates with politics and hacking I would say that most people in the computer underground are varying shades of libertarian, but from my experience that doesn't really translate into group action. I know some people to be somewhat active politically, but I believe they act as individuals and not as part of a hacker group. I personally got involved with cDc because I've been politically active, or working in political circles for a lot of my professional life. I saw the opportunity of using civil disobedience online – sort of another tool in the arsenal – but I don't believe what we're doing is common, or even duplicated anywhere else.

What makes the cDc's statement distinct from most hacker commentary is that it is positioned in terms of politics (for example, Reagan and "mourning in America"), and it uses a merger of discontent and technology to enact dissent ("these malcontents speak of their disillusion with The American Way and their obsession with their new computers")….[that] connects technology to politics not in a metanarrative of control or change but in terms of a narrative of disruption.

[The cDc thus become] the first hacker group dedicated to a kind of political action based on principles of civil disobedience and visibility, and…. the first group to connect hacker identity with the notion of political action.

Hackers vs Microsoft

Douglas Thomas pp95-104
[cDc released "Back Orifice" – the hack of Microsoft's "Back Office", which enables hackers to enter your Windows 95 and 98 OS from across the internet.]
As the name indicates, the product was designed to rudely confront Microsoft and to force it to take notice of the program and the cDc itself.

The point that Microsoft failed to acknowledge was that Back Orifice was not designed to exploit bugs in the system but rather was intended to expose Microsoft's complete lack of concern about security issues. As one member of the cDc explained "The holes that Back Orifice exposes aren't even really bugs, but more fundamental design flaws. Of course, Microsoft calls them Features."

It is essentially an exploitation of social relations, between the expert and the end-user, that makes such hacking possible. It is also the place where cDc takes aim at Microsoft…."Microsoft seeks to buffer the user from the actual workings of the computer. They give you a nice little gui [graphical user interface], integrated web-browser and all the bells and whistles. But why is there this file with all my passwords cached in plain text? Isn't that bad? ….The problem is that if Microsoft wants to buffer their customers from the workings of the computer, then they have to do a hell of a lot better job of protecting them from OTHER people who DO understand the workings of their computer.

The conflict is the same one that has been rehearsed ever since Bill Gates released his memo accusing the Homebrew Computer Club members of being thieves. Hackers see Gates and Microsoft as producing an inferior product, selling it for too much money, and taking advantage of a market of end-users that they were fundamental in creating. At a practical level, Microsoft is creating problems for hackers interested in securing their own networks, but at a philosophical level, Microsoft is violating the most basic tenets of computer culture. Most segments of computer culture, including the computer industry, have always been able to operate within the general confines of an ethic. This ethic was driven, for the most part, by the concept of a social conscience, a dedication the principle that computers could make people's lives better….[not always, but] there has always been a genuine belief among hackers and industry that technology was doing more good than harm. [Hackers remained politically neutral for the same reason.] Microsoft changed all that by embracing corporate policy that violated much of what hackers (and even industry) considered to be for the social good.

Whatever arguments one might have with Sun, Apple, or Intel, there was always something else to redeem them. With Microsoft, the situation was different. Microsoft, from the very beginning, had operated in opposition to the ethic that animated hacker culture. When Microsoft challenged hackers on the grounds of their own ethics, however, a movement in the hacker underground was created that recognised politics as an essential part of a newly constituted hacker ethic.

[Responding to Microsoft, which accused cDc of being unethical for releasing its Back Orifice software, the cDc accused Gates of having no morals, for happily supporting the Chinese leaders in 1996 – despite human rights violations – and opening up new markets and access to "even more money" – as cDc member Blondie Wong puts it: "one of the reasons that human rights in China are not further ahead is because they have been de-linked from American trade-policy" In effect, "businessmen started dictating foreign policy."]