COPYRIGHT DOES NOT EXIST

By Linus Walleij, 1998

Translation: Daniel Arnrup (svenskefaen@svenskefaen.no), 2000

TABLE OF CONTENTS

PREFACE

I'm going to start by telling you what it cost me to create this book: lots. Lots of time, and in actuality, lots of money. I'm not complaining. I've had plenty of both. A large part of the book was written during a phase of my studies at a vocational college. It's therefore more or less financed by the public means in the form of student financial aid that I received at the time. In a way, you could propose that due to this fact the book belongs to society. The question is whether society wants to have it.

When you publish a book in a conventional manner, i. e. through a publisher, there is always some kind of quality control. People with many years of experience in the field read the material and ascertain that the content is both well formulated and well motivated. The problem is that they also make sure that the content is, as we say, "politically correct", i. e. that no one will take inordinate offense at it. If a publisher releases obviously inappropriate books, it will suffer from badwill. This is why obviously well-written and even more obviously *portentous* books such as *Mein Kampf* are printed and distributed by smaller publishers that don't have to worry so much about their reputation.

I don't know if any publisher wants to release this book in print, but I leave this as a possibility. [Translator's not: the book If I haven't received an offer within a year or so, I'll release this book under public domain, which means that it will always be free of copyright. Until then, the following applies to this material:

> 1: It will be absolutely free in electronic form. It may be copied and distributed through media such as diskettes, CD-ROMs, through BBSs and the Internet, and through public and private organizations without any prior permission from me. I would, however, be *grateful* for receiving a reference copy in case the book would be mass distributed. **These terms will not be altered if a publisher prints the book.** I do not intend to commit to a contract with anyone who wants the electronic rights to its content.
>
> 2. At the moment it is **not** permissible to mass-distribute the book in printed form without my prior permission. If you want to print a large run of this book I'm sure I wont have a problem with it, but I'm afraid I need to retain control over this process.

Now that you've read this far, you probably realize that I give you free reign in general terms. The distribution of this book is your responsibility too, and the sound of its message is already ringing in your ear. Put it on disks and give it to your friends. Put it on CDs and distribute it with magazines. Print it out on paper if you want to.

With the exception of electronic and personal use, this work is currently (and ironically) copyright-protected. In an earlier version of this preface I came down on the entire capitalist system, and elaborated on how much I hated attempts to treat information as property. I've now settled down a little and realized that if my thoughts are going to have a chance to reach ordinary people through an established publisher, I must be able to give that publisher some competitive advantages.[(1)] I'm not a

utopianist; therefore, I have to make compromises. (And I'll be damned if I'll lose any sleep over it…)

Finally, I will issue the warning that my own values and opinions heavily influence this book. I'm a declared individualist, and I don't mind being called a socialist. At the intersection of these two values there is a little-known ideology called syndicalism or Kropotkin anarchism. Basically, I consider all private property to be equivalent to theft[(2)], but I'm not so bloody stupid that I don't realize that a society without private property is a utopia. My opinions on freedom of speech and of the press are similar to those of the most liberal organizations in Sweden. I have nothing against small and medium-sized companies, but to me, enormous intercontinental corporations are more dangerous factions of power than democratic governments, and as such, corporations must be subject to the same oversight as that for governmental organizations.

I'm now going to tell you about the culture that made me what I am.

---

1. I have now realized that compromises are worthless in this context.
2. Private material property is theft. "Intellectual property" is even worse, possibly armed robbery. Censorship is rape.

COPYRIGHT DOES NOT EXIST

A book about information and power
For everyone and for no one

By Linus Walleij

DEUS EX MACHINA
CARCERES EX NOVUM

This book is about currents of thought in literature, technology, music, film, law and ideology. It was written after I realized that if I didn't write it, somebody else would. It was also written because I wanted all of the nice hackers in Sweden to be aware of, and educated about, their historical and ideological heritage. Finally, the work has been written with an air of popular science, to make it somewhat easier to understand (although the last statement can probably be debated; some chapters are considerably more difficult and technical than others).

Some questions to which you should know the answers before you start reading this book:

Q: *Why should I read this stuff?*
A: To understand new concepts within information society, emerging youth culture, and public debate, and also to give yourself the opportunity to form your own opinions through confronting those of myself and others. The book is focused on cultural phenomena in particular, since they are the strongest indicators of the direction of a society. *Our* society, at the brink of the information society, is called the *post-industrial* society. I will not hide the fact that I will also attempt to make you question that society.

Q: *What is a computer?*
A: A computer is an object that obeys the laws of nature, just like a human being. Like a person, it is neither evil, boring, kind, troublesome, or particularly intelligent. It becomes what it is made to become, just like an individual in society. The difference between a human being and a computer is that the computer has the opportunity to know with certainty who has created it, and it can look like virtually anything. In 1995, most people think that a computer looks like a square box. The computing field distinguishes between *microcomputers* , *minicomputers* , *mainframes* , and *supercomputers* , each being more powerful and cool than the previous. Today, the lines that separate one from the other are so blurry that these labels are a bit antiquated. A microcomputer, for example, is a PC, Mac, or similar home computer. The average person has hardly seen any of the other types.

Q: *What is a computer network?*
A: A computer network consists of two or more independent computers that have been connected by a cable. It is customary to distinguish between LANs (*Local Area Networks*), where computers inside the same building or at most the same block are

connected, MANs (*Metropolitan Area Networks*), which connect computers throughout an entire city, and WANs (*Wide Area Networks*), which connect computers across great distances. The greatest network of them all is the Internet, which links all kinds of computers - and networks - across the entire world. A computer network allows for the transfer of information between different computers, may it be text, images, sounds, or anything that can be entered into a computer. It is similar to telephones or postal transport, but better and faster. Actually, the entire phone network is a computer network, except it connects people instead of computers. Many WANs such as the Internet employ the phone networks instead of laying their own cables. Computers that hold together a computer network are almost exclusively minicomputers or mainframes, i.e. large, refrigerator-looking boxes.

Q: *What is a BBS?*
A: BBS stands for *Bulletin Board System* , which really means an electronic bulletin or poster board. Similar to a regular bulletin board, it is necessary to visit it frequently to see its contents. You can also put up your own "notices" and receive replies to your submissions through other written messages on the board. There are BBSs that are partially connected to the Internet, and some that are stand-alone. Today, you connect to a BBS through the use of a modem, a computer, and a telephone line. In the future, BBSs will probably be replaced by conferencing systems (a type of giant BBS) on the vastly more efficient Internet. Newsgroups are an example of such conferencing systems. Users can also send private electronic mail to each other or mass-distribute computer software through a BBS.

Q: *What is Cyberspace?*
A: Cyberspace is where the money you keep in the bank resides. It is where a telephone conversation takes place and the space through which television programs travel on their way to your receiver. It is an electronic reality consisting of information, and it actually only exists because people have agreed that it works. Physically speaking, it consists of cables, radio waves, pulses of light and large computers with gigantic memory capacities. It is a physical occurrence in the "real" world that we may, with an ounce of faith, consider a universe of its own. It is a reality in which man is God and has created all. It is something of a religion. Most people "believe" in cyberspace, or they wouldn't use an ATM to withdraw currency. The entire economic system of the West exists inside it. Cyberspace was born on March 10, 1876, when Alexander Greham Bell "invented" it. Without electricity, there is no cyberspace. Our civilization is already dependent on cyberspace; if it disappeared, the economy would collapse and the West would perish.

Chapter 2
HACKERS!

HACKER... the word itself has an air of magic, and many connotations. Some associate it with computer crime, intrusion, and espionage. Others imagine a skinny and myopic teenager, whose acned face is constantly illuminated by the glare of a computer screen. Many immediately think of the information officer at work. In recent years, some have even embraced the hacker as a hero. Personally, I see the hacker as a messenger sent by humanity to explore the worlds of information. This mission may seem superficial and self-imposed - perhaps even foolish - but it will make more and more sense the more you read on.

The word originally applied to the people who spent their time crawling under the railroad tracks at the Tech Model Railroad Club's (TMRC) facilities at the Massachusetts Institute of Technology (MIT) in the 1950's, connecting switches and relays with cables. This model railroad was one of the first computer-like structures. A *hack* originally meant a prank of the kind that students and faculty played on their school (or rivaling institutions), such as wrapping the entire roof in tinfoil. A good hack would be very conspicuous, and also prompt the observer to ask him- or herself: *"How in the hell did they do that!?"*. Later, the word became synonymous with a spectacular solution to a technical problem, or an ingenious computer program, or some other generally brilliant design. A *hacker* , therefore, was someone who created and implemented things of this kind.

A hacker, generally speaking, is a person who uses a computer for its own sake because it's fun. An author that uses a word processor all day is not a hacker. Neither is a graphic designer, inventory specialist, or computer instructor. Their professions simply require them to use a computer to simplify or improve the efficiency of some other task. However, a *programmer* that loves his or her work is a hacker. Likewise, an enthusiastic computer technician or microcomputer designer is also a hacker. Last but definitely not least, there are *hobby hackers* , who actually constitute the largest and most overlooked group of computer enthusiasts - probably because they don't use a computer in a professional sense. These amateurs do not have PR directors shouting their cause, nor do they have publishers or trade journals that print their opinions. Some elements of the media focus on this group, but they seldom speak for them; rather, the computer media generally focuses on "bringing up" the amateurs to the standards and norms of the professionals.

In the following section, I will try to summarize a variety of concepts, names, and ideas, all relating to electronic culture and especially the hacker culture. I will also attempt the rather difficult task of classifying these events and ideas from a historical perspective. This can be a risky venture, considering that the time frame is short and it is the type of thing that often generates lots of criticism. Nevertheless, I will proceed; I feel worthy of this task because I have grown up in this culture, and I consider myself to have a very personal relationship to it. I will even suggest that I have some of my information generation's spirit in my blood. Furthermore, I *feel* that it needs to be done

It is a tangled story primarily concerned with young people in the 60's, 70's, 80's, and 90's. It is a history of devotion, computer programs, authority and ingenious scientists. The tale is about hippies, yippies, libertarians, anarchists and classical socialists in one sordid mess, and the ideology that was born out of this mess through a conglomerate of subcultures. We will be thrust between order and chaos, from quiet computer rooms where the only the soft clicking of keyboards can be heard, to high-octane decibels at techno-rave parties in European warehouses.

Let us travel to MIT, sometime in the 60's, for it is where the story begins...

The Cradle of the Hacker Culture

It was no coincidence that the hacker culture was born at MIT. This is where the first large computer networks were created, and the faculty discovered that some of their students were so devoted to their computer studies that the teachers let them work independently. Among the more famous people at this liberal faculty we find **Marvin Minsky** , now a legendary scientist in the field of artificial intelligence. Thus, the first hacker's association was born out of a close-knit group of dedicated students. The work ethic that formed among these early hackers resembled both that of academic study and that of a non-profit organization.

A "Hacker Club" by itself was hardly anything new; like other student groups, both bad and good things came of the association. However, this club became more sectarian and devoted (read: fanatic) as it grew. The mood of the group came to resemble that of the groupof students in the movie *Dead Poets' Society* , and the members increasingly neglected their studies in favor of the exploration of computers and computer technology. In particular, Digital Equipment Corporation's **PDP-1** computer turned out to be incredibly addictive. This machine differed from the mammoth IBM machines that had been used by universities since 1948, in that you could work *directly* with the computer. You could see your program's execution, and you could correct errors (debug) while the program was running. In a flash, the hackers invented a number of new programming tricks and developed, among other things, the first computer game *(Spacewar*) and the first joystick. The accomplishments of these hackers became so notable that they were asked to assist in the development of the **PDP-6** computer, which became a huge hit for Digital. The company currently manufactures behemoths like **VAX** and **DEC** computers, and it owes a great deal of its success to the hackers at MIT.

If these hackers had been treated like other students, they would have been expelled when it turned out that they spent their days (and especially nights) hacking away on the school's computers instead of studying for their finals. That would have been the end of the story. However, by a stroke of luck, the American Department of Defense developed an interest in MIT's resources through ARPA (Advanced Research Projects Agency), which paid MIT to hire developers for a project named **MAC** . MAC stood for Multiple Access Computing and Machine Aided Cognition; the goals of these projects were to have several users sharing a computer, and to make it simple for users to take advantage of the computer's resources.

At MIT, the hackers progressed to developing networks, message systems (one of the worlds first time-sharing systems, which allowed users to share a computer by allowing it to process the requests of one user at a time), and above all *artificial*

intelligence (AI), a research area in which MIT is still a world leader. The hackers speculated about the nature of intelligence, and could not understand what made it so difficult to capture even the simplest operation of intelligence within the circuits of a processor. In the late 70's, a computer science professor by the name of **Douglas Hofstadter** released a book with positively religious undertones called *Gödel, Escher, Bach: an Eternal Golden Braid* , which has served as an articulated statement of the hackers' world view. This work is well-known among hackers, and is also considered a masterpiece by literary experts. Unfortunately, the book is *challenging* (but not hard to read), and it is found in the mathematics section in most libraries, which tends to scare off many potential readers.

Hackers derived a philosophical foundation for their culture from Hofstadter, and speculations about self-referential intelligent systems (self-referential means "learning from mistakes", or simply: learning) figured heavily in this philosophy. Parallels were drawn to such varied subjects as paradoxes among the ancient philosophers, **Bach's** mathematical play with harmonies, **Escher's** mathematically inspired etchings and drawings, and **Benoit Mandelbrot** 's theories of order within chaos (which are physically illustrated by computer-generated chaos images, also known as *fractals*). The arguments in the book eventually lead to an understanding of Gödel's Theorem, which proves that every complete mathematical system, by virtue of its characteristics, contains errors - i.e., there must exist statements that are true, but cannot be proven inside the system.

Hofstadter's book culminates in an argument regarding self-reference and artificial intelligence, which is designed to describe human and machine intelligence as a function of mathematical systems. As mentioned, MIT housed the pioneers in artificial intelligence, and many of its hackers were convinced (and remain convinced) of the possibility of building intelligent machines. However, it is sufficient to establish that this early generation of hackers were very concerned with mathematics, mathematical philosophy, and classical natural sciences. This MIT-born philosophy, centered around intelligent systems, became the mainstay of the hacker generation. It also became important for hackers to display their own cultural identity. According to **Sherry Turkle** , a Harvard sociologist and the author of the book *The Second Self: Computers and the Human Spirit* , the hackers that she has interviewed prefer listening to Bach in particular, and avoid more romantic composers such as Beethoven because of a *lack of order* in these compositions.

That the hackers formed a tight core, with their own esthetic and philosophical values, was also a result of their voluntary seclusion. Among all university students, technology majors tend to keep the most to themselves, and an overwhelming majority are male. Among technology majors, computer science students are the most reclusive, and they are even more disproportionately male. If you happen to be a "reject" from the beginning, it is not hard to start re-evaluating your view of society and your environment in general. If you also happen to be Army buddies, this process is almost inevitable. The hackers mostly associated with each other, preferably by computer. In essence, they formed a government-sanctioned subculture.

The original hackers at MIT were, among others, **Alan Kotok, Stewart Nelson, Richard Greenblatt, Tom Knight,** and **Bill Gosper** . They were known to pull thirty-hour shifts in front of the computer and then crash for twelve hours. They found

the machines so fascinating that they forgot about everything else while they were working. At the same time, they nurtured an ideology that held that all information should be free, ate Chinese take-out, and taught themselves how to pick every lock in the computer science building - which they justified with their devotion to putting all available equipment to its best use. Many considered this behavior to be careless and disrespectful, but the hackers considered it necessary to get the job done.

The fact is that the hackers constituted a homogeneous group that should be the envy of any teacher: they were interested in the subject of their studies, and they spent all day and all night solving problems related to their field. The faculty did not try to constrain them.

At this time, the history of networks began. Two computers were connected, then three, then many - and shortly, an entire network was created. Communicating by computer removes a host of irritating particulars present in real life: you don't have to dress up while punching on a keyboard, you can be totally anonymous, nobody will notice you belching or eating with your hands, and no one will know what the color of your skin is. Another user forms his or her opinion of you solely based on your written communication. Social status identifiers are virtually erased, and your opinions are just as valid as anyone else's. Nobody can beat you, fire you, or repress you if you decide to be insolent or speak from your heart. People who communicate by computer tend to be surprisingly honest and forthright, since the discussion is created by everyone and anyone can participate.

MIT, Stanford, Berkeley, and other major American universities were the pillars of the American defense project **ARPAnet** , which became the core of what is today known as the Internet. Through this network, MIT hackers came into contact with hackers at other universities, laying the groundwork for an national hacker culture which would later spread to Europe and, in particular, Sweden. Many of the slang terms that can be found in *The Jargon File* (a widely available file that includes a dictionary of hacker terminology) stem from this period. Some of the most venerable expressions can be traced to the original model railroad club, TMRC. In addition to the dictionary, the file contains anecdotes and observations on the nature of hacking, making it perhaps the most important written work of the original hacker culture.

When hacker culture spread from MIT through ARPAnet, it first reached the other large American universities that performed computer research, including the prominent Stanford and Berkeley schools on the other side of the continent. Thanks to ARPAnet, the hackers were not hindered by geographic distances, and could cooperate and exchange all kinds of information across this vast expanse - a privilege that normal people would not enjoy until the 90's. In San Francisco during the late 60's and early 70's, hackers were influenced by hippie culture, and this influence spread throughout the hacker communities of the entire world through ARPAnet. This was the first interaction between the hacker community and the hippie culture.

The hacker culture first reached Sweden in 1973, when the Linköping School of Technology (LiTH) started specializing in computer technology. The students formed a computer association called **Lysator**, which still claims to be the oldest computer club in Sweden (which is true), and the origin of the true Swedish hacking tradition (which is more questionable). Lysator will play a part in later sections of this book.

Hacker culture not only has its roots in the academic realm; these university hackers only constitute a small part of the digital culture scene. Now and then someone comes along and states that only the hackers that attend college and basically live in the computer labs are "real" hackers. Such a statement is ignorant and stupid. The meaning of a word is, naturally, defined by its users, and anyone who chooses to call him- or herself a hacker has the right to do so.

If we now allow the 60's to roll into the 70's, we will observe a monumental event: the introduction of the high-tech amateurs, who were just as much hackers as Bill Gosper and his MIT buddies.

Chapter 3
THE GRASS-ROOTS OF HACKER CULTURE

The grass-roots of hacker culture consisted of amateur radio and electronics hobbyists, who built their own microcomputers using the very first mail-order kits. Radio amateurs have been around since 1915, and they are organized in several camps. The most puritan insist that the telegraph key and Morse code are still the best tools for international communication. Others prefer radio telephony, i.e. voice transmissions. Still others have tried amateur TV, and some fiddle around with data communication by radio. Radio amateurs are found in any city worth its name, and many have turned to data transfer through the Internet, where they explore yet another means of communication. In a sense, the radio enthusiasts became the first hackers, even before MIT.

The radio amateurs, as opposed to the hackers, seldom attracted young people to any great extent. In Sweden, part of the reason is that you have to be sixteen years old and become certified to use shortwave radios. The average Swedish youth can't afford the courses and testing required for radio certification. Some mess around with radio anyway, and are known as radio pirates. Broadcasting amateur radio without certification is not a big deal, as long as you don't cause problems. You have to be careful to stick to the correct frequencies; broadcasting on bands that are reserved for specific purposes, such as emergency or military channels, carries a risk of being traced and fined. To keep track of what frequencies to use to avoid trouble, radio amateurs soon began cooperating internationally. This became the first *virtual society* , which transcended geographic boundaries but was limited by technology.

Radio amateurs embody a great deal of the culture that would later be adopted by the hackers: a fascination with technology (machines), and a fascination with interpersonal communication. Some are constantly on the lookout for new, cool equipment (gadget freaks). Others only want to find ways to communicate with other people as efficiently as possible, and try to improve existing systems (evolutionists), and some feel that they've mastered an aspect of technology and simply stay with it (these are sometimes called conservatives). Finally, there are those that most amateurs do not want anything to do with: the people that think that broadcasting pirate radio is the most awesome thing in the world, and who use technology as a means of rebelling against society.

The early computer-oriented electronics hobbyists initially gathered around the very first personal computer: the **Altair 8800** , which was introduced as a mail-order kit in 1975. The computer got its name from a planet in a Star Trek episode, and sold in such large quantities that some of the enthusiasts formed their own user groups. They were invariably electronics hobbyists, and often professional engineers. Virtually all of them were adults, but they were struck by the same technical fascination with programming that kept the university hackers awake all night and made them forget everything but the machines. The most active user group was the **Homebrew Computer Club** in San Fransisco. One of its members was **Steve Wozniak** , a dedicated hacker who was to build the **Apple II** computer. His friend **Steve Jobs** successfully marketed it in 1977 as the first real personal computer. Homebrew Computer Club's Swedish counterpart was called **PD68** , which catered to happy

engineers and others who found microcomputers fascinating.

Personal Computers for a Broad Market
In 1978, the Swedish companies Luxor and Scandia Metric contracted with **Data Industrier AB** (DIAB) to build a computer called **ABC80** . DIAB manufactured the chips, while Luxor built the case, monitor, and keyboard. Despite its monochrome display (which required a special monitor), the ABC80 was a quality machine. As with its contemporaries Apple II and Tandy Radio Shack TRS-80, the established American computer industry considered these computers virtually useless. IBM displayed no interest whatsoever. The current trend was toward manufacturing minicomputers such as Digital Equipment's enormous DEC, since the industry giants (spearheaded by IBM and Digital) projected a global need for about 50 large computers in the year 2000. Users would connect to these computers through terminal networks.

It is unclear what prompted Luxor and Scandia Metric to produce a computer for the regular consumer. Most likely, the chief engineers observed personal computing trends in the U.S., where the Apple II and TRS-80 had entered mass-production, and somehow persuaded the management to approve such a venture.

ABC80 became a great success among Sweden's early computer enthusiasts, who had been waiting a long time for a real computer (previous computers had been very expensive and directly imported from the U.S.). Now there was one - and to top it off, it was Swedish! In 1981, it was succeeded by the ABC800. In 1980, electronics hobbyists, engineers, and other enthusiasts formed *ABC-klubben* (the ABC Club) under the leadership of the legendary **Gunnar Tidner** . The ABC Club showed an interest in computer communications from the start, and at the end of that year it opened *Monitorn* (The Monitor), which probably was Sweden's first non-profit BBS. It ran thanks to a program written by Tidner himself. For the rest of the 80's, most new Swedish BBS's were named *X-Monitorn* (such as Örebro-Monitorn, Eskilstuna-Monitorn, etc.) as a tribute to Tidner's breakthrough. The club still has a "monitor" that's used as an internal switchboard for all kinds of things.

The ABC Club grew exponentially as personal computing in Sweden became all the rage it was in the U.S. It became a center for debating the technology of ABC computers as well as data communications in general. In 1985, through a contract with the QZ Computer Center in Stockholm, the ABC club gained access to a DEC-10 computer. On this machine, the members started a central BBS (a "real" conferencing system) with several discussion groups. The BBS, named *Q-Zentralen* (The Q-Zentral) ran on QZ's KOM-system, and resembled past and present networks such as U.S.A.'s Usenet and Prodigy, or England's Compunet.

Many of the pioneers of the future electronic Sweden were found on Q-Zentral's discussion groups: **Sven Wickberg, Anders Franzén, Henrik Schyffert,** and **Jan-Inge Flücht.**

It was not until the early 80's, after the introduction of small, cheap computers, that any real changes in personal computing took place. It was no longer necessary to know how to build your own equipment; therefore, anyone who could afford it could have access to their own computer (albeit not very advanced). Overnight, an array of

personal computers appeared, in the U.S. as well as Europe: Sord, Atari 800, Sol, Texas TI-99A, Vic-20, Spectravideo, etc. Most remained on the market for only a few years before production was halted and/or their manufacturers went bankrupt. In Sweden, only three survived the competition: **Sinclair ZX-80** (thanks to its low price), **ABC-80** (because of its industrial applications and strong support from the ABC-Club), and **Commodore 64** (which will be referred to as the **C64**), simply because it was the most technologically advanced home computer of the time. Even the first PC's hit the market in early 1981, but they commanded such exorbitant prices that no normal person would consider them personal computers. In America, the **Apple II, Atari 800, Commodore PET,** and **C64** were the main survivors. Apple II, in particular, was to the U.S. as the ABC-80 was to Sweden. To this day, there are resilient Apple II-fanatics who still use their late 70's computers, just like Sweden has its resilient ABC-80 users (some of which make up the heart of the ABC80 Club).

Initially, most European hackers were of the same kind as the American ones: old radio amateurs, engineers, or electronics enthusiasts who dreamed of using a *real* computer such as VAX or IBM (those lovely, gray, refrigerator-looking things) instead of simple home computers. The hacker culture from MIT in the 60's, and its extension of the radio amateurs' philosophy, were considered an ideal; a real hacker was a person who wrote programs that did something useful (or appeared to do something useful), or who had mastered electronics and could modify their computer to the amazement of their friends. The most fortunate computer clubs had been able to start their own BBS's on a used minicomputer purchased from some company. The hackers that had gotten started on ABC80, minicomputers, and electronics were generally shocked and somewhat disgusted by the culture that emerged in the mid-80's through the invasion of the C64 (this will be discussed in the chapter 5, *Subculture of the Subcultures*). Many of those hackers have now obtained a PC, and consider writing shareware programs and other real "hacks" to be a noble art.

Hackers of this sort also started the alternative computer network *Fidonet* . In San Francisco, amateurs **Tom Jennings** and **John Madill** devised a system in which different BBS's called each other according to a specific pattern, and through skillful coordination managed to provide coverage as broad as the Internet's. The main difference was that electronic mail had longer delivery times, and there were no permanent connections; the mail was distributed through substations, just like in an old-fashioned postal system. The network also allowed for globally accessible discussion groups. In the beginning of 1985, the Swedish Fidonet was started in Karlstad by **Conny Johnsson** .

Because of the increased affordability of the Internet, many think that Fidonet has become obsolete. Far from everyone agrees - Fidonet is a true amateur creation, while the Internet has mainly been constructed by academicians. However, for a long time there have been bridges connecting the two networks, enabling their respective users to send mail to each other. Personal computing became a public concept, and many teenagers received their first computer in the mid-80's. Most futuristic parents who bought a computer probably hadn't expected their children to spend as much time on the computer as they did, but this was a result of a marketing glitch. Personal computers were marketed as office systems to be used for financial, word processing, and database applications, for all of which they turned out to be quite useless. Apparently, it was simpler to find a recipe in a cookbook than to boot up the computer

and look through some database which took five minutes to load. The only "useful" tasks that the machines could perform efficiently were word processing and simple calculations, which was something that few people were familiar with or could appreciate.

The only adults who really used their computers were almost exclusively technicians or technology fans, who could stay up all night and fight with their ABC80 to make it do one thing or another. Many were electronics hobbyists that modified the computer to suit their own wants and needs. (I belong to the wave of youths who were completely captured by the ABC computers around 13 or 14 years of age; for many in my generation, those machines became a ticket to the electronic world).

It would be until the 90's before the personal computer really got its breakthrough as a popular appliance - but when it came, it came with a vengeance. It is only recently that IBM PC's have become common in the home. If it hadn't been for the Altair 8800, Apple II, Atari 800, and ABC80, it would never even have occurred to IBM to manufacture PC's. The previous trend had been toward building mainframes: mammoth boxes that consumed several kilowatts per hour, and generated so much heat that they needed a separate cooling system to be able to operate. The idea of one computer for each user *was and remains* a hacker's notion, which goes all the way back to MIT, where many late nights were spent working alone on a PDP-1.

Had these microcomputers not emerged, the industry would still be working on their 50 supercomputers that were to provide computing power for the entire world. Without the microcomputer, modern information systems such as the *Client-Server* model (in which a coordinated network of computers distribute tasks and information between them) would never have been invented.

Chapter 4
UNDERGROUND HACKERS

As a product of the home computing trend and the futuristic spirit that followed the space race (which culminated in the moon landing in 1969), several technology-oriented subcultures formed. Some were perfectly normal associations of science-fiction enthusiasts and amateur radio hobbyists. Others were... *peculiar.* It was these organizations that drew a stigma on hacker culture, and are responsible for the fact that hackers are frequently thought of as criminals. How many of you - raise your right hand - have ever pondered what it would be like to have control of technology? To have the power to decide what radio and television programs will be broadcast? Imagine having these enormous electronic systems under your control. Imagine being able to fill all TV screens with white noise when that guy you hate shows up, or knock out all the telephones in the nation when you know that your beloved is chatting sweetly with his/her ex-lover. Imagine being the *master* of the information systems of society...

Phreakers
A collection of electronics fanatics in the 60's and 70's, called **Phone Phreaks** , were among the first to study the emerging computer technologies. These "phreakers" specialized in fooling the phone companies' switches into connecting free calls all over the continent, through a technique called *Blue Boxing* (which refers to a small blue box containing electronic components that produced the tones which manipulated the switches).

Some of the phreakers were university students. As the hackers had been mesmerized by computer technology, others had found it fascinating to try different number sequences on the school's telephones to see how far you could get connected. Some succeeded in connecting to the public telephone networks and call for free, since the school's local telephone network was a complimentary service.

A young man by the name of **Mark Bernay** (a. k. a. **The Midnight Skulker**) had in-depth knowledge of the phone system. He went up and down the American West Coast and put up notices in phone booths with party-line numbers that he had established, and in this manner created a small network of technology-oriented youths. However, these youngsters did not turn phreaking into the considerable criminal operation it is today.

Instead, a man called **Joe Engressia** created (without knowing it) the underground movement of telephone manipulators at the end of the 60's. Even though the telephone company (then called Bell) had traced and prosecuted the first phreakers back in 1961, few of them had been members of an organized movement: most were businessmen, some were general laborers or students, and one was even a millionaire. The reason for this wave of phreaking was that Bell had made publicly available the information that anyone needed to build a blue box.

Joe Engressia was blind, but he had been compensated by the fascinating gift of perfect pitch. He could recall a note he had heard, and perfectly reproduce it by whistling. At age eight, he had already discovered that he could manipulate the system

of telephone switches by whistling certain tones. These systems were called *multi-frequency systems* (MF), and it was information about these systems that Bell made the mistake of publishing in 1960. Joe was arrested after connecting free calls for some friends by simply whistling into the receiver. Thanks to the publicity surrounding the incident, Joe and other telephone enthusiasts formed a rapidly growing underground network mainly consisting of blind people. A few knew how to whistle the tones, while others employed early keyboards and synthesizers to produce the necessary sounds. Through Joe, phreaking grew into a major youth movement. He was arrested again in 1971, and was given a suspended sentence in exchange for promising never to manipulate telephones again. Later, he was hired by a small Tennessee company as a telephone repairman.

Allow me to make an observation at this point. Frequently, I hear of people that claim to know someone who can "whistle" their way through the telephone system and call for free. The person telling the story is never the one that knows how to do this, and upon closer inspection it turns out that it was really a friend of a friend... etc. Stories about "whistlers" should be treated as common myths, just like many other stories about phreakers and hackers. Please note that "whistling" *requires* perfect pitch, which is a talent that few people possess. It is also necessary to know (and have listened to) the tones that are required. Therefore, there is a diminishing number of people who would be able to do the trick - perhaps only a handful in any given country. Finally, this technique is useless against modern telephone systems such as the AXE-system (*translator's note* : AXE is an acronym for Automatic Cross-Connection Equipment).

Joe and his buddies used keyboards to make calls. Other methods to produce the necessary tones were even more common. **John T. Draper** , a. k. a. **Cap'n Crunch** , used a toy whistle from boxes of the cereal brand with the same name. By covering one of the holes and blowing through the whistle, he produced a tone with the frequency of exactly 2600 Hz (which roughly corresponds to an E in the five-times-accented octave - not a very pleasant tone). This happened to be the exact note that AT&T and other long-distance companies used to indicate that long-distance lines were available. If either party to a call emitted this tone, the switch performing the call would be fooled into thinking that the call had ended (because that was how the switches signaled that the line was free), and therefore all billing for the call stopped. The whistle enabled people to call for free.

Draper was a very active phreaker. He initiated big party-line calls where he came into contact with many of the blind people, and disseminated his knowledge among other phreakers. He kept a list of contacts and directed the exchange of ideas between phreakers. Like some of them, he was an electronics fanatic, and himself built the tone generators that allowed total control of the entire telephone system. These generators were called MF-boxes (or, as mentioned earlier, Blue Boxes), and gave their owners complete access to national and international telephone traffic - totally free. It wasn't very difficult to construct these boxes, since all information concerning the MF-system had been made public. As it is not exactly cheap to replace an entire telephone system, there are still countries whose systems can be manipulated by blue boxes.

Many were (like Drapner) completely spellbound by the blue boxes' power to hook up calls across the world through cables and satellites; they inspired a feeling of

unlimited power over the telephone system. One of Draper's more known tricks was to connect back to himself around the globe through seven countries, simply for the incredible satisfaction of hearing his own voice with a 20-second delay.

In 1971, the media caught wind of the phreaking phenomenon. One journalist, **John Rosenbaum** , wrote an article about the movement, and Draper was arrested and imprisoned shortly after its publication. He was approached by the Mafia (who wanted to exploit his skills), and severely beaten after he refused. Upon his release, an old friend (Steve Wozniak, who developed the Apple II computer) came to his aid and made him quit phreaking in favor of programming. After a few modem-related incidents on the Apple II (the modems in question were rather computerized blue boxes), he wrote the word processing program *Easy Writer* , which was sold by IBM with their PCs. He made more than a million dollars off the project.

In the same year (1971), the hippies discovered the possibility of making free calls. A militant faction of the hippie movement, known as *yippies* , started a magazine called *Youth International Party Line* (the name both referred to the political nature of the movement and to its obvious telephonic emphasis). The paper's mission was to teach methods of telephone fraud. Yippies are a kind of tough hippies that do not hesitate to use violence and terrorism to obliterate (as far as possible) American society. They also advocate the use of hallucinogens. Yippies consist of people that have become so sick of American society and its system that they only see one solution to the problem - total destruction. As opposed to classical anarchists, they were not opposed to technology; rather, they exploited all knowledge and resources available to them. One of the most frightening aspects of the yippie movement was that many of its members were quite *intelligent* . The yippies represented fundamentally different values and norms, which rocked the foundation of American culture. This political force would later sow the seeds of the ideology that is today known as *cyberpunk* , to which I will return in a separate chapter. Prominent yippie leaders include **Abbie Hoffman** and **Jerry Rubin.**

In 1973, a faction of technology fanatics broke away from the yippie movement and formed an expressly anti-social and anarchistic organization around the paper (now known as *TAP* , or *Technical Assistance Program*) . In this new version, the magazine provided instruction in subjects far beyond simple telephone scams: it contained formulas for explosives, blueprints for electronic sabotage, information on credit card fraud, etc. Much of this content was naturally "exciting" for teenagers and slightly immature young men, and the periodical was widely copied and transmitted across the globe. Within a short period of time, there was a global network of phreakers. The basic philosophy of the paper is still the same as that of the yippie party (Youth International Party).

In TAP, peculiar forms of writing were introduced, such as substituting "z" for "s", 0 (zero) for o, and spelling the word freak "phreak". These trends have remained. In the early 90's, a character named **B1FF** showed up on the Usenet computer network and took this abuse of the written word to the limits of the absurd, writing words the way they were pronounced rather than the way they were spelled. B1FF combined this practice with an artificial habit of typing 1 for I, 4 for A, + for T, 3 (a reversed E) for E, etc. B1FF's typographical antics drove some people totally nuts, but the hackers thought the practice was super-cool and started writing like B1FF, to annoy generally

anal-retentive people and to put an anarchistic stamp on the otherwise disciplined Usenet. They have even gone so far as to randomly mix lower- and upercase letters, resulting in text that is almost *painful* to read.

In Sweden, a sister publication to TAP surfaced. It was called *Rolig Teknik* ("Fun With Technology"), and aroused some attention in the dailies. Rolig Teknik was started by **Nils Johan Alsätra,** a legendary figure in Swedish underground culture. He was inspired by TAP, and published several articles between 1984 and 1993, all based on the same social philosophy as that of its American counterpart. The publication described how to make fake hundred-crown notes to fool gas station machines (*translator's note* : In Sweden, the *crown* is the official unit of currency, and most gas stations have automatic gasoline dispensers that are used outside the station's business hours), how to fool electric meters, and (naturally) different methods for making free calls. Nils started the magazine after being fined for building and selling *Black Boxes* (or, as he himself termed them, *unit-eaters*), which enabled owners to make free calls after connecting the boxes to their telephone jacks. Before he started selling them, he gave the phone company the opportunity to purchase the device for three million crowns (about $450,000). The phone company never replied.

Rolig Teknik expired after a raid in Gothenburg, Sweden, in 1993. The raid was precipitated by the event that Alsätra had begun to publish anonymous classifieds where the advertisers could offer goods, using the paper as a middle-man, without having to display their name and address. For every transaction where the payment was handled by the publication, Rolig Teknik received SEK 10 (SEK=Swedish crowns, SEK 10 = about $1.50). Since the content of many of these ads was rather questionable, this practice was considered equivalent to fencing and arms dealing. After the police obtained permission from the executive branch of the government (for the first time in Swedish history), they raided the editorial offices of the paper. Since then, not a peep has been heard about the paper or Alsätra himself. The possibility of using the "unit-eaters" that Alsätra invented disappeared with the modern AXE telephone system, but many of the other tricks remain effective to this day.

For the modern hacker, magazines such as *Phrack* or *Phun* are the hottest items. In Sweden, there is also a newfangled print magazine (in the spirit of Rolig Teknik) called *Alias* [1] . Phrack is probably the most popular, since it has received a great deal of publicity. It is free to individuals, while organizations and governmental institutions have to pay $100 per year for a subscription. In this way, the authorities actually help finance the publication of the magazine, since they have to keep up with underground trends and developments [2] . As the telephone companies have started to fix the glitches in their systems, phreakers have learned to use exceptionally sophisticated methods to make free calls. One technique involves actually reprogramming phone company switches. Another consists of using stolen or artificial credit card numbers to bill the call to some other (sometimes non-existent) person or company. Ideally, the bill should be sent to international conglomerates such as Coca-Cola, McDonald's, or the phone companies themselves.

The point of using credit cards is that by calling through a specific 800 number, you should be able to bill the call to the card in question, no matter which private or public phone you are calling from. Since you can't show the card to an operator (human or

computerized), you enter the card number and PIN (*Private Identification Number* , a personal code associated with the card number) that are necessary for credit purchases over the phone.

Another free-call method is to use a **PBX** (*Private Branch eXchange)* , which is usually a corporation's internal switchboard. Using a PBX frequently involves dialing an 800 number associated with an automated switchboard, entering a code, and then dialing the number of the desired target. The call will be billed to the company that owns (or employs) the switchboard. The procedure is a simplified and automated version of the debit/credit card payment system, which means that a human operator is not required to verify and record numbers and codes. In the beginning, PIN codes were not even used; it was simply a matter of calling the correct toll-free number and then dialing the desired phone number. It was believed that keeping the toll-free number secret would offer enough protection. Since phreakers are known to systematically dial extensive series of 800 numbers, they soon discovered that it was possible to dial other locations from some of these numbers, and before long the phone companies introduced PINs. For reasons which I will soon explain, PBX codes are constantly circulating outside the spheres of their proper owners.

The phreakers, then, more or less randomly dial toll-free numbers in their search for PBXs, computers, phone company switches, and other interesting telecommunications devices, a practice commonly referred to as *war-dialling* (from the movie *War Games*) or simply *scanning* (this practice is by no means illegal; the point of having a telephone is to be able to call the numbers you want, and as many as you want). During these treks across the phone networks, phreakers often run into all kinds of intriguing things, such as the phone companies' private service lines and *voice mail boxes* (VMBs). Through voice mail boxes, you can send messages to each other if nothing else works (read: in case the phone company has blocked all other means of communicating for free). Voice mail is usually employed by large corporations with many employees on the go, such as consulting or sales and marketing companies, as a more efficient alternative to written communication. Voice mail boxes use private codes just like an ATM machine, and the codes are just as easy to crack (simple codes like 1234, 0001, or the same number as that of the box itself are common). Some voice mail boxes also allow for further connections, which means that it's possible to call long-distance from such a box.

Most phreakers learn of technical methods and stolen or faked codes from other phreakers. Information of this kind is often disseminated by private BBSs and confidential relationships. Most people involved with phreaking know nothing about actually getting these codes or what the technical instructions they receive actually mean. They simply follow the instructions and advice they receive from others, punch in a few numbers and Presto! - they're hooked up with the other side of the world!

However, there are also people like John Draper, who really know what they're doing. The most zealous ones are often youngsters less than 20 years old, who nevertheless possess enough knowledge to match a degree in electrical engineering, or *beyond* . Naturally, this is considered a very dangerous situation in a society where *knowledge is power.* Of course, the phone companies' systems are idiot-proof. Not even all the idiots in the world would be able to re-program a telephone switch to give them free calls. The problem is the smart criminals.

Bright, inquisitive youths, who want to know how the phone networks function, usually begin by reading standard, college-level telecommunications literature. Many of the more accomplished ones could easily pass professional exams with a flourish. They master the jargon of communications technicians, and are able to recite obvious acronyms such as DCE, OSI, V.24, MUX, NCC, or PAD in their sleep. They seem to have a sort of fetish for the telephone network.

Not all (but a great majority) of the technical information regarding the telephone systems is public. The missing details are usually discovered through a method called "trashing", which entails going to the dumpsters outside a major telecommunications company and digging through the trash for useful documentation (that should have been run through a paper shredder, since it is not at all appropriate literature for teenage technology geniuses). In this manner, phreakers find out about functions, system commands, and secret phone numbers that are meant for internal use. Sometimes it's worse - the hackers actually have access to a person on the inside, who intentionally reveal company secrets to them. Today, these security leaks have been virtually eradicated, despite the fact that the number of people that must have access to this information is great. Trashing is also performed to retrieve obsolete or discarded equipment, which is not really a criminal practice. It is also not very common, especially in Sweden.

The art of "social engineering" is more widespread (and often more effective). The technique is based on attacking the weakest link in the entire phone and banking system: the human being. The expression comes from the telemarketing field, where it is part of the telemarketer's job to dissimulate him- or herself and focus on the customer's weaknesses, to build trust while still remaining concise and effective. The following is an example of social engineering by a phreaker, loosely based on a case published in a highly improper hacker periodical (WARNING: use this example to protect yourself and others from becoming victims of this type of crime, not to commit the same type of crime yourself. If you abuse this information, I will be sorely disappointed!).

P = Phreaker
V = Innocent victim
T = The victim's telephone

T : Ring!
V : Hello!
P: Hello, is this Mr. X?
V: Yes... who's calling?
P : Good morning, this is Noam Chomsky at the Accounts Security Division of the Chase Manhattan Bank. How are you doing this morning?
V : Er... just fine. What's the problem?
P : We have a situation here right now involving our databases. Your Chase Visa card is currently unusable due to the loss of a large portion of our customer files. If you would give me your card number and PIN, we can restore your account immediately.
V : Just a minute, who did you say you were?

P : My name is Noam Chomsky, and I'm with the Accounts Security Division of Chase Manhattan Bank. There's a situation here... (repeats what he just said)
V : (Suspicious) I wasn't aware of this. Is there a number I can call you back on?
P : Sure, no problem. I appreciate your carefulness. Give me a call back at 800-555-5555, (fake number that connects to a phone booth or that has been programmed into the phone company switches by P himself, which he can remove at will without trace. Naturally, it's not his home phone number).
V : Thanks! Talk to you in a moment.
T : Click. Silence. Buzz...
P : Chase Manhattan Bank, Accounts Security Division, Noam Chomsky speaking. How can I help you?
V : Great! This is Mr. X. I was afraid you were a scammer. OK, my Visa card number is XXXX... and my PIN is XXXX.
P : (Pauses, writing). Thank you. We will restore your account as soon as possible. Please refrain from using your card during the next 24 hours. Goodbye, and thank you for your cooperation.
V : Goodbye.
T : Click.

If you fall for this type of con, the consequences could be devastating. Normally, the credit card companies will absorb the loss if you can prove that it wasn't you that used the card, but if you can't... ouch! It is not only consumer credit accounts that are victimized; company accounts are also relentlessly exploited in this manner. Other methods of obtaining card numbers include trashing (see above) or simply searching through mail boxes for letters from banks that might contain cards or PINs.

Credit card numbers are also used by phreakers to purchase merchandise, such as computers and peripherals, synthesizers, stereo equipment, and other capital goods. The criminal orders the merchandise for general delivery or gives the address of an abandoned building, which makes it impossible to trace the perpetrator. This method is known as "carding" among phreakers and hackers. A fair number of Swedes have been arrested and sentenced for these crimes. A *considerably* greater number have (as usual) gotten away with it.

Phreakers are social people, who love to use their skills to talk for *hours* about basically nothing and everything. Naturally, conversation tends to focus on methods, codes, and other things that are essential to phreaking. Sometimes international party conferences lasting up to eight hours are created. Some talk, others simply listen, someone hangs up and someone else dials in. The conversation lasts as long as the moderator can maintain it, or until the phone company catches on and disconnects it. A very famous conference was the **2111-conference** , which took place on the 2111 number in Vancouver (a test number for telex transmissions). Phreakers as well as sympathizing operators (!) used to call this number to chat away a few hours.

Clearly, these practices are illegal and terribly immoral, etc. However, I am sure that some readers would agree that it is rather amusing to see a few bright teenagers using the conferencing systems of multi-national corporations to set up global party lines, simply in order to *shoot the bull* for a while! The phreakers consider this gross exploitation to be harmless, at least in those cases where they just snatch bandwidth by using technical tricks. They are of the opinion that since the cables are already there, why not use them? Where's the harm in that? Does it damage the phone network? Hardly, unless you don't know what you're doing. Does it hurt any individuals? Not as long as you stay away from hospital and military lines. Do the phone companies lose money? Not at all, since none of the phreakers would have made these calls if they had to pay for them. Does it overload the phone network, forcing the companies to expand? No it doesn't, since international connections have a fairly high ceiling.

The real crime committed by phreakers is that of interfering with the social order. What if everyone started doing this? Everything would go straight to hell! International lines would break down, and chaos and anarchy would ensue. It's not a question of theft; more appropriately, it is a question of *order* . Stealing credit card numbers and using them, on the other hand, is fraud. These arguments are completely irrelevant to a true yippie, since he/she is only out to destroy society. In contrast, many phreakers are fairly average and law-abiding members of the middle and working classes. However, they have taken **Nietzsche** to heart and consider themselves a type of elite (or even superhuman) with the natural right to take advantage of the system. They would never suggest that *everyone* should exploit these systems in this manner, and claim that they also want to help the phone companies discover their security gaps by pointing out existing flaws. Therefore, they contend that actions can not be defined as good or evil solely on a legal basis, just like Zarathustra through Nietzsche had to reject the concepts of *right* and *wrong* . This has nothing to do with fascism; it's a theory of the improvement of systems through individual transcendence.

The phreaker magazine TAP has been followed by other publications such as *2600: The Hacker Quarterly* (the name is derived from the 2600-Hz tone that was discussed earlier), *Iron Feather Journal*, and a cornucopia of electronic magazines that are too numerous to list.

Telia (*translator's note:* Telia is the largest telephone company in Sweden, and is a governmentally supported corporation. Before deregulation a few years ago, it was a state agency that had a monopoly on telecommunications traffic in Sweden) is reluctant to acknowledge that phreakers exist, and it would be safe to assume that a number of phreaking cases are kept in the dark (most likely to avoid consumer complaints such as: "Why do *they* get to call for free when *I* have to pay?", "Why doesn't somebody *do* something about this?", " *I'm* by God an honest taxpayer, and I *demand* ...", etc. etc.).

In Sweden, phreakers have actually succeeded in manufacturing fake phone cards, re-programming mobile phones to bill to someone else's number, using Telia's own access codes, using blue boxes to fool Telia's switches, and (most frequently) using foreign credit card numbers to make international calls [3] . Additionally, the oldest form of phreaking (known as *gray-boxing*) still plays a part. Gray boxes

(predecessors to the blue ones) are the boxes found attached to telephone poles or beside the electric company's fuse boxes. By hooking into a gray box, you can physically connect yourself to someone else's phone line and make calls in their name.

There are no reports on the extent of these crimes, and Telia would rather have it that way. To put the spotlight on security breaches would be fatal in the current market, where Telia competes with private telephone companies and has to be concerned with its image. Therefore, incidents of fraud are frequently covered up.

The situation is even worse in the United States, where many phreakers have studied corporate public relations in depth in order to use social engineering to set up fake credit cards or telephone service. They exploit the corporations' strong emphasis on customer service to pit the telephone companies against each other. For example, if a phreaker encounters problems in setting up a fake 800 number, he or she will say something like "well, if that's the way it's going to be, I might as well call X or Y or Z (competitors)". This serves to discourage phone company sales reps from asking too many questions or asking for too many details.

These problems point to shortcomings in a society where social interaction between businesses and people has become neglected, due to the extreme *size* of modern corporations. The social aspect of a business has been separated from its sphere of productivity in the struggle toward increased efficiency, which has created an anonymous society. According to conversations I have had with phreakers, the large companies are the easiest to deceive: they can't tell who's fake and who's for real since they've never encountered either one in person. The only available means of separating the wheat from the chaff is by observing what the individual *sounds like* and the quality of his/her vocabulary and verbal communication. The phone companies have turned into anonymous logotypes toward their customers, and as long as the business world works this way, phreakers will find ways to call for free.

Network hackers

Let us now leave the telephone networks and take a look at computer networks. As technology fanatics, the phreakers soon discovered computer technology. There were plenty of phreakers similar to Cap'n Crunch, who initially engaged in phreaking because they didn't have access to computers. Together with renegade college students and other less savory characters, they created small hacker groups that engaged in downright intrusive activities. In addition to being experts at tweaking telco switches, many of these hackers attained great proficiency in manipulating the large computer systems (VAX, IBM etc.) that governed the nodes of the Internet, which had become virtually global by the late 80's. These systems were usually **UNIX systems** (synonyms include *machine* , *site* , *host* , *mainframe* , etc.). Others specialized in VAX systems, which used the VMS operating system instead of UNIX. VMS became somewhat more popular among hackers, since it was easier to penetrate than UNIX.

The first hackers to become publicly known were **Ronald Mark Austin** and the members of his hacking group **414-gang** , based in Milwaukee. 414-gang started "hacking" remote computers as early as 1980, and it was the 1983 discovery (just after the opening of the movie *War Games*) of these hackers that sparked the entire debate of hackers and computer security. The 414-gang had entered the computer system of a

cancer hospital in New York. While the group was removing the traces of the intrusion (after an interview in the New York Times, which included a demonstration of possible entry methods), they accidentally erased the contents of a certain file in an incorrect manner, with resulting in the destruction of the entire file. The mere *notion* of the possibility of this file containing important research results, or a patient journal, was terrifying. Prior to 1983, few people knew what hackers were. Now, everyone talked about them. It was probably this early debate that imbued the word with its negative connotations.

Personally, I use the term *network hacker* (they are also known as *crackers* or *netrunners*) to define this type of hacker. Most of the first-generation network hackers used Apple II computers, for which there were several phreaker magazines such as *Bootlegger* . These magazines would become the predecessors of the future multitude of hacking and phreaking publications. When network hackers came to Europe, they primarily used C64 computers, and had no papers or magazines since such a tradition hadn't emerged among European hackers. This lack of forums greatly limited European hackers' activities. As they didn't have access to American Apple II's, they couldn't read the American hacking publications to learn to hack better. Network hacking has *never* been as extensive on this (the European) side of the Atlantic.

A funny detail is that after the 414-gang became famous, most hacker groups developed a penchant for putting equally incomprehensible numbers before or after their proper names. 414-gang derived its number from the Milwaukee area code.

It can be difficult to immediately understand what it means to "gain entry" to a computer system. To "crack" or "break into" a system simply entails convincing a remote computer to do things it isn't supposed to do (for you, at least). It could be referred to as instigation or fraud in more common terms. Let me illustrate it through the following dialogue:

"Hello", the computer says.
"Hi," says the hacker, *"I would like some information."*
"Hold on a minute", the computer responds. *"Who do you think you are?"*
"I'm the system administrator", the hacker says (or something like that).
"Oh well, then it's OK", says the computer and gives the hacker the desired information.

Naturally, it doesn't look like this in real life, but the principle is the same. Hacking into a system involves a form of social engineering applied to electronic individuals. Since computers aren't that smart to begin with, one can't call them stupid for not being able to tell the difference between a system administrator or a hacker. Therefore, many think that the hacker is not playing fair by tricking the computer in this way (similar to stealing candy from a baby). To enable the computer to distinguish between a hacker and the system administrator, it has been given special identifying strings that the user must repeat, together with his or her username, when access is needed. These are called *passwords* , and the idea is that hackers shouldn't know about them. Sometimes, hackers find out what the password(s) is/are anyway, or in some other manner convince the computer to think that they are the system administrator or someone else who has the right to access the computer. An

functioning username-password pair is called a *NUI* (Network User Identification, or user identity). A hacker sometimes refers to security systems as *ICE* (Intrusion Countermeasure Electronics). The on-screen exchange between a hacker and a computer can look something like this:

***** WELCOME TO LEKSAND KOMMUNDATA ICE *****

UserID: QSECOFR (the hacker enters a name)
Password : ******* (the hacker enters a password, which is normally not echoed to the screen)
SECURITY OFFICER LOGGED IN AT 19.07 . (The userID and password together constitute a valid user identity named "Security Officer").
ENTER COMMAND> GO MAIN (the hacker has "gained access" to the system). [4]

The usual methods for finding passwords are not that spectacular. The simplest is to glance over an authorized user's shoulder, or actually recording the log-in keystrokes on video (since they rarely appear on the screen). Other "tricks" include searching for notes under desktop pads, or guessing different combinations of initials, birthdates, or other words and numbers that relate to the person whose user identity the hacker wants to take over. It is especially common for users to use their spouse's maiden name as a password. If the target identity is that of a system officer, the hacker tries different computing terms. All of this falls under the definition of social engineering, which I mentioned in relation to phreaking. A surprisingly effective method is simply calling the system operator and saying that you are an employee who's forgotten his/her password. "Trashing" and collecting loose pieces of paper at computing conventions are other common techniques.

The most sophisticated methods bypass the entire security system by exploiting gaps in the *system programs* (*operating systems* , *drivers* , or *communications protocols*) running the computer in question. To be usable, a computer must have system software running on it. Since VAX/VMS systems are fairly rare, it is mostly UNIX systems that are attacked using this approach. It is especially common to use glitches in the commands and protocols that bear mysterious names such as FTP, finger, NIS, sendmail, TFTP, or UUCP.

Methods such as the above are becoming less and less viable, since the security gaps are usually closed as soon as they are discovered. The "filling" of the gaps is accomplished as the system administrator receives (or in a worst-case scenario, *should have received*) disks containing updated system software, which is then installed on the system. The programs are usually called *fixes, patches,* or *updates.* However, many systems officers fail to completely update the system programs, with the result that many of the security gaps remain for quite some time. Others neglect parts of the security system because it creates a hassle for authorized users. For example, many system administrators remove the function which requires users to change their password frequently, or which prevents the usage of passwords that are too common. Some computers (in 1995) still have security holes that were cautioned against in 1987. Swedish computers are no exception.

When a hacker has gained entry to a system, he or she can (often) easily obtain more passwords and usernames through manipulating system software. Sometimes, they

read through electronic mail stored on the computer, in search of passwords. Imagine one such message: *"Bob, I won't be at work on Friday, but if you need access to my numbers, the password is 'platypus'."*

Most of these hackers never caused (and still don't cause) any damage to computer systems. Mainly, the intruders are driven by curiosity and a desire to see "if they can do it". It's about the same type of thrill that comes from wandering subway tunnels, or crawling through underground sewers, i.e. an exciting form of "forbidden" exploration. In fact, hackers in general follow an unwritten rule which states that one should **never** steal and **never** destroy anything on purpose. Those who break this rule are called *dark side hackers* (from the movie *Star Wars*). In **Clifford Stoll's** book *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* , one can follow the chase of such a hacker.

The hacker that Stoll had problems with obviously belonged to the dark side: he tried to systematically retrieve classified military information, and had ties to the KGB (the events took place during the height of the Cold War). He had the assistance of one of the most feared hacker groups: **Chaos Computer Club** , an organization with a political agenda, founded in 1984 by **Hewart Holland-Moritz** . They purported to fight for individual rights in the information society, and were known for killing the project for a German information system called *Bildschirmtext* , by exposing its lack of security and reliability at a press conference.

In 1989, the case of the spying hacker made worldwide headlines, and Stoll wrote his book shortly thereafter. The case has spurred its own mythology: one of the players, who called himself **Hagbard** , was found burned to death in a forest, and many speculated that the death was KGB's doing. This is probably not true; the hacker in question was named **Karl Koch** , and had severe psychological and drug problems even before he started hacking, and it was most likely (as the police suspected) a matter of suicide. Among other things, Koch believed that the world was ultimately controlled by the *Illuminati* , a fictional Islamic mafia that has supposedly infiltrated governments and organizations since the 13th century, an idea he had gotten from the books by the same name. He was also fond of psychedelic drugs, which didn't help much. Upon closer examination, it is easy to reach the conclusion that Koch was a raging paranoid, but the headline *"Hacker Assassinated by the KGB?"* obviously sells more papers than *"Hacker Committed Suicide?"*.

Koch, together with **Pengo** (Hans Hübner) and **Markus Hess** , were members f the hacker group **Leitstelle 511** , which had a clear political profile and a taste for long nights of hacking and drug orgies. They had obtained classified information and software through the Internet, with Markus as a UNIX expert and Pengo masterminding the intrusions. The project, which consisted of systematically exploring American defense installations, was code named *Project Equalizer* . The name was derived from the hackers' slightly naive idea that their espionage would even the odds between East and West in the Cold War. This was more properly an excuse to spy for their own gain than an expression of real political intentions. Markus and Pengo, as the two most talented hackers of the group, mostly hacked for their own pleasure, and did not receive any considerable financial gains. All of the involved, after being caught, were sentenced to between one and two years imprisonment, but

the sentences were suspended. Pengo was not charged, since he had fully cooperated with the police.

This is one of the few known cases of network hackers making money off their "hobby". Generally, people engage in this type of hacking for the intellectual challenge, or for the social aspects of data communications. **Kevin Mitnick** is another hacker to become more or less legendary. Originally, he was a phreaker who developed a hitherto unsurpassed skill in manipulating people as well as computers and telephone switches. Mitnick is the archetypal dark side hacker: He stole the source code (*source code* is the version of a computer program that can be read, written, and modified by humans. After a process known as *compilation* , the program is readable only to computers - and hackers) for **Digital** 's operating system *VMS 5.0* by breaking into their software development division through phone and computer networks. He was very vindictive, and punished police and companies that crossed him by giving them outrageous telephone bills or spreading lies about them through phones and fax machines. When police tried to trace his calls, he was instantly alerted and could abort the call, since he had hacked into the phone company **Pacific Bell** 's surveillance systems. When he was arrested, he was just about to steal the source code for the not entirely unknown computer game *Doom*.

After his arrest in December 1988, he was sentenced to one year's imprisonment and six months of rehabilitation. He was treated together with alcoholics and drug addicts for his almost pathological obsession with hacking. Recently, he was again apprehended after being pursued by a security expert by the name of **Tsutomu Shimomura** , and a journalist named **John Markoff** (who had earlier written a book about Mitnick).

Much of the publicity surrounding Mitnick was hyped to the point of witch hunting. Many were of the opinion that he wasn't as dangerous as Markoff portrayed him to be. Nevertheless, Kevin has become a symbol for the "dangerous" hacker: cold, anti-social, vindictive, and extraordinarily proficient in manipulating people and phone switches. On the other hand, he was never a master of computer hacking - a field in which he has many superiors. It is worth noting that Kevin never sold the information he captured to any third parties. He only wanted the VMS operating system to be able to improve his hacking skills, and he never cooperated with organized criminals.

This type of illegal break-in has been glorified in films such as *War Games, Sneakers* (1992), and the TV series *Whiz Kids* , and as a result, many (completely erroneously) think that hackers in general primarily engage in this criminal form of hacking. Even in the Swedish film *Drömmen om Rita* (*Dreaming of Rita* , 1992), a romanticized hacker has one of the cameo roles. He is a symbol for the young, the new, the wild; a modern Jack Kerouac who drifts through the streets with his computer. The hacker is portrayed as a modern-day beatnik. An interesting detail is that the hacker in this movie goes by the name **Erik XIV** , which is the same pseudonym used by a real hacker in a few interviews with *Aktuellt* (a Swedish news program) and *Z-Magazine* in 1989, where he explained how to trick credit card companies into paying for international calls and merchandise ordered from abroad (crimes for which he was later convicted and sentenced).

Actually, very few youths interested in computers take to criminal activities. Nevertheless, computer crime is frequent, but the real problem is that computer systems do not have adequate protection; no hacker would be able to force a sufficiently protected system, even if theoretically possible. No one can fool a computer that is smart enough. Most security breaches are probably kept in the dark for PR reasons. As far as I know, no bank has *officially* lost money because of dark side hackers; on the other hand, if I were a bank and some hacker transferred a few million dollars to his or her own account, would I want to prosecute the hacker so that all of my customers would realize how insecure my computer system was? Swedes may remember the publicity surrounding the software bug in Sparbanken's (a large Swedish bank) computer system in 1994...

Companies with poor security would probably find it embarrassing if the public found out that teenage hackers could read their secrets or transfer money from their accounts. In those cases, it's PR-correct to put a lid on the incident, which is exactly what has happened in many instances.

The distinction between network hackers and phreakers is blurred. It is customary to say that a *phreaker* explores computer systems for social reasons, primarily to be able to call their friends long-distance for free, while an intrusion-prone *hacker* explores the systems for their own sake and for the thrill of outwitting technology. The anarchistic yippie attitude and the urge to break down systems stem from the phreakers.

Many have rightfully questioned society's negative view of hacking, i.e. "hobby intrusions". Hackers have been compared to cave explorers, searching for new realms out of curiosity and a desire for challenge rather than greed. Since the networks are so complex that there is no comprehensive map, hackers are of the opinion that cyberspace is the uncharted territory where electronic discussions take place, a universe which they curiously explore. To compare hacking to burglary is insipid. During a burglary, there is physical damage to doors and locks, and real objects are stolen. A typical hacker never damages anything during an intrusion (very few hackers are vandals[5]), and to the extent that he/she "steals" information, it is only copied, not removed. Essentially, the only "theft" that takes place is a few cent's worth of electricity and some minimal wear on the machine being used, but considering the high rate of depreciation of computer equipment, this can hardly be considered a loss. Furthermore, any computer connected to the Internet *allows* outsiders to use it to search for and distribute information.

I suspect that the main reason that the establishment fears hackers is that hackers assume the role of someone else - that they present themselves as system operators or other authorized users, and enjoy the privileges associated with their assumed status. The worst part is that they seem to be able to do this with ease, thus publicly embarrassing the computer experts that the corporations pay dearly for. This tends to be aggravating, especially since the business world in general and (to an even higher degree) the corporate world depend on a system of fundamental status symbols, where every person is at the top of their own little hierarchy. To act like someone or something that you are not is considered a cardinal sin (remember Refaat El-Sayed's fake doctoral degree!) (*translator's note* : In the 80's, Refaat El-Sayed was the CEO

of Fermenta, a large Swedish pharmaceutical company, who was ousted following a scandal involving purchased credentials).

The condemnation of hackers is disproportionate to their criminal acts, and sentences are way too severe. This is grounded in an almost paranoid fear of what the hacker accomplishes, and the code of ethics that he or she subscribes to. The hacker is (like most people) *definitely* not evil by nature, nor a hardened criminal, but an individual that listens to his/her own heart. The hacker is not a psychopath, nor interested in hurting or stealing from other people in a traditional sense. Possibly, the hacker wants to steal secrets, which frightens many. Later, we will go deeper into hacker ethics and ideology.

Swedish network hackers appeared at a later stage than the ones in the U.S., partially because of Televerket's (*translator's note* : Televerket was the government authority that later became Telia - the name literally translates into "The Telephone Service") monopoly on the modems that are needed to connect to a computer across the phone networks. The first case that I know of happened in 1980, when a student at Chalmers School of Technology (at Gothenburg University) was fined for manipulating the billing system at Gothenburg's computer center in order to use the system for free. The first case to attract media attention occurred when a journalist from *Aftonbladet* (a major Swedish daily), **Lars Ohlson** , hired a couple of 17-year-olds, a few modems, and a few computers, and tried to break into Stockholm's **QZ** computer center (after seeing the movie *War Games)* . The QZ operators noticed what they were doing, which led to Ohlson's arrest and subsequent fining, under loud protests from (among others) *Dagens Nyheter* (one of Sweden's largest, oldest, and most respected newspapers). The three never succeeded in breaking into QZ, and the original purpose had been to test its security, which turned out to be very good... in 1983.

In the first 1984 issue of the paper *Allt om Hemdatorer* ("All About Personal Computers"), there was a report of a considerably more successful intrusion attempt. With the help of an imported Apple II, two youths (17 and 19 years old, respectively) managed to get into **DAFA-Spar** , the government's individual address database. Even though the information contained in the database was far from classified, it is easy to imagine the consequences if, for example, a foreign power could retrieve information about every Swedish citizen. DAFA-Spar themselves were surprised and shocked by the incident. The youths, inspired by *War Games* , had also succeeded in entering Gothenburg's Computer Center, Medicin-Data and the computers at Livsmedelsverket (the Swedish equivalent to the U.S. Food and Drug Administration) The hackers claimed to have performed the break-ins to point out security deficiencies.

Like their American counterparts, most Swedish network hackers seem to have worked alone, i.e., without forming groups. Reportedly, many of the first Swedish hackers were inspired by the BBS *Tungelstamonitorn* , which was run on an ABC806 computer by **Jan-Inge Flücht** in Haninge (a Stockholm suburb) in 1986-87. The BBS later changed its name to *Jinges TCL* and became known as one of the most outspoken and insolent Swedish boards through the amateur network Fidonet. In 1987, **SHA** (the *Swedish Hackers Association*) was formed, which (curiously enough) is most famous for irritating freelance journalist and security consultant

Mikael Winterkvist , after he attempted to chart the transmission of computer viruses in Sweden.

The SHA itself claimed to be Sweden's largest and most well-organized hackers group. Others see them as boastful people from Stockholm with a strong need for self-assertion, which is a rather empty sentiment considering that nearly all underground hackers have an enormous need to assert themselves (*translator's note:* and people from Stockholm are often considered to be boastful and arrogant by other Swedes *not* from Stockholm). One of their most successful hacks involved an SHA member gaining access to Swedish Radio's computers, and becoming so familiar with the system that he could change the programming schedules at will. Just for fun, he changed Pontus Enhörning's (a famous Swedish radio personality) password and emailed him to tell him about it, which generated some publicity.

SHA succeeded, during its heydays, in entering several computer systems around Sweden: among others, **SICS, KTH/NADA, ASEA, Dimension AB, S-E Banken, SMHI, OPIAB, DATEMA,** and - last but not least - **FOA** (*translator's note:* FOA stands for Försvarets Forskningsanstalt, or Sweden's Defense Research Facility). None of the victimized companies or authorities have shown any great desire to talk about the intrusions. Swedish security experts shrug and sigh when SHA is mentioned. The police, as well as many companies' own security teams, know exactly who the SHA is, but they can't prove anything. Mostly, the SHA is given free reins, since the authorities feel that they have the group "under control". They're not afraid of the SHA, and they have no reason to be, since the group consists of relatively benign hackers who are not out to destroy or corrupt anything. For the most part, all that they want is some system time and open telephone lines. If you shut them out, they respect it, but if you act in an arrogant and authoritarian manner toward the SHA, they tend to get pissed off and threaten with horrendous retaliation.

Sweden has also been subject to hacker attacks from abroad. Perhaps the most well-known incident occurred when a couple of UK hackers, **Neil Woods** and **Karl Strickland** (known under pseudonyms as **PAD** and **Gandalf** , collectively as **8LGM** , which stood for *8 Little Green Men* or *the 8-Legged Groove Machine*), broke into the Swedish Datapak and Decnet networks during Christmas of 1990. Using a computer program, they searched through 22,000 subscribers looking for computers to access, and established contact in 380 cases. The two 20-year-olds were sentenced to six months imprisonment on the 4th of June, 1993, for computer violations in fifteen countries (they were the first to be sentenced under the new UK computer security regulations). Before one passes judgment on Pad and Gandalf, one should know that they were the ones that hacked into one of the EU's computers and helped expose **Jacques Delors** ' (a French EU representative) exorbitant expense accounts.

Virus Hackers

Computer viruses are constantly a hot item. This exciting area is still fertile ground for publicity in magazines and periodicals. The **Michelangelo** virus, discovered around March 6, 1992, attracted lots of attention. The virus was believed to cause great damage to data and computers around the world. These fears turned out to be greatly exaggerated; basically, the virus didn't do anything. This was taken to indicate that media warnings had been effective, and the theory, so to speak, proved itself. The question is whether the Michelangelo virus ever constituted a threat.

Computer viruses are small programs, and like all other programs, they are created by people. Hackers who engage in virus programming are made out to be the worst villains among hackers, and are thought to only be interested in screwing things up for other people. At the time of this writing, legislation is underway that would make the manufacture as well as distribution of computer viruses a criminal offense. The first modern viruses (such as the Michelangelo virus), the *link* and *boot viruses* , surfaced in the beginning of the 80's. Many of the first ones came from *Bulgaria* of all places, and it was in this country that the first BBS dedicated only to virus exchange and discussion appeared: the *Virus Exchange* . Supposedly, the reason for Bulgaria's central position in the virus industry was that the East Bloc, during some phase of the Cold War, decided to manufacture viruses for electronic warfare. Bulgaria is known for its high-class computer scientists, and so it was a natural choice for construction of these "weapons". Thus, many Bulgarian students came into contact with government-financed virus programming and later continued to develop viruses as a hobby. The most prominent of these students is **Dark Avenger** , who has attained cult status among today's virus hackers.

Individual link and boot viruses possess different attributes, but share the ability to *propagate* efficiently. Most are written by hackers, and not all viruses are destructive. Computer viruses have been classified as electronic life by researchers as prominent as **Stephen B. Hawking** . If so, then it is the first life form to be created by humans. Some virus hackers are just regular hobby hackers who have developed an interest in viruses, while others are network hackers. The electronic magazine **40hex** (named after an MS-DOS function) is a forum for American virus builders, and primarily provides code for virus programs and explores virus techniques, but also reports on political and economic aspects of viruses. The magazine is published by the virus hacker groups *Phalcon* and *SKISM* (Smart Kids Into Sick Methods). (Notice the pun?).

It's a shame to say that virus builders are only concerned with destruction. Mostly, it is just another manifestation of the *graffiti phenomenon* , which is a desire to see one's name on as many screens as possible, and to read in the papers about the effects of the virus one wrote. It's a question of becoming someone. In addition, constructing a virus is an intellectual challenge that requires a relatively high degree of programming knowledge. The virus hackers are probably the most intellectual hackers next to the university hackers. In the case of destructive viruses, it is usually a manifestation of the phreakers' old yippie attitudes. The virus hacker is the fascinating person produced when you cross a yippie anarchist with a disciplined programmer. A related fact is that viruses are exclusively written in assembly language, which is the hardest and most complicated programming language to learn. No virus hacker that I've heard of has ever made money from making a virus.

The virus hackers have a sort of love-hate relationship to **John McAfee** and his company, which makes the virus-removing program **VirusScan** . Before he started working on computer viruses, he supported himself by selling membership cards for an association which simply guaranteed their members to be AIDS-free, so it is fair to say that he has had experience with viruses. It has been implied that his company supports virus production, since it is vital to its continued existence that new viruses or new versions of viruses are constantly appearing. The company's main source of income comes from *program updates* , i.e. selling new versions of the software that

can neutralize and protect against the newest viruses. McAfee worked under a similar system selling AIDS-certificates. He was accused of bolstering the public fear of the Michelangelo virus in 1992.

Computer viruses can also be considered an art form. A virus is a computer program just like any other, and according to copyright laws, every creative computer program contains an artistic element. It is obvious that the creation of a virus requires determination, effort, and imagination. Imagine that while systems analysts and administrators are breaking their backs to get their systems to work in an orderly and coordinated fashion, there are little hoodlums out there trying to accomplish the *exact opposite* , i.e. chaos, disorder, and ruin. It doesn't take a lot of inside knowledge to see the humor in the situation. The virus builders are taunting the nearly pathological fixation on order within corporations and governmental agencies. It can very well be viewed as a protest against a nearly *fascistic* desire for control, order, and structure.

"To some, we are demons; to others, angels...
... Blessed is the one who expects nothing, for he will not be disappointed."

(Excerpt from the source code of the virus *Dark Avenger*, by the Bulgarian virus hacker of the same name. *Translator's note:* one does notice a mere whiff of inspiration from *Hellraiser*...).

The most notorious Swedish virus hacker is known as **Tormentor** . In 1992, he formed a loosely connected network of Swedish virus hackers by the name **Demoralized Youth** . Tormentor belonged to the relatively small group of hackers that became interested in virus building, and established contact with similarly interested Swedish youths. Among others, he got to know a 13-year-old who had collected over a hundred viruses, and downloaded new ones from the Bulgarian *Virus Exchange* BBS. During the late fall of that year, Tormentor distributed a virus of his own creation to different BBS's in Gothenburg, and could observe it spreading like a wave across Sweden. Intense Fidonet discussions ensued.

Someone discovered an "antidote" to Tormentor's virus, and he modified it and distributed it again, only to have it trounced by another anti-virus technique. This process was repeated five times before Tormentor got sick of constantly updating and distributing the virus. Afterwards, Tormentor concluded that the virus contained several errors. To start with, he had only tested it against McAfee's VirusScan; additionally, it was afflicted by several programming errors, and - worst of all - it was *not* destructive! Those are the words of a true anarchist. Tormentor embodies the virus hacker in a nutshell, and he is probably an eternal Swedish legend in the field. He was in contact with the SHA from the beginning, and is still involved in a feud with Mikael Winterkvist at the company Computer Security Center/Virus Help Center.

Among other well-known viruses we also find the so-called *Trojan Horse* **AIDS** (Trojan horses are viruses that *infiltrate* remote computers or networks). AIDS was a program that was distributed free-of-charge to companies across the world, following an international AIDS conference in London, and it purports to contain information about AIDS. When the program is run, it locks up the computer's hard drive and the user is prompted to deposit a certain amount in a an account in Panama (talk about electronic extortion). However, this virus has nothing to do with hackers; it was

created by a man named **Joseph Papp** , who was not considered mentally fit to stand trial.

Another famous virus is *RTM* , a.k.a. *The Internet Worm* . This was a *worm virus* , which copied itself across computer networks. The program was written by the student and hacker **Robert Tappan Morris** (hence the name 'RTM'), and his idea was to write a program that traversed the Internet on its own, finding out how many systems it could get into. It was then supposed to report back to its author with a list of its destinations. Unfortunately, Morris had made a programming error which caused an overload of the entire Internet. For this little trick, he was sentenced to fines and probation. The worm virus idea originated at the Xerox Research Center in Palo Alto, California, where they were used to maximize the use of machine resources (for example, by having some programs run only at night, when no one else was using the computers).

Cable and Satellite Hackers

It is uncertain whether satellite and cable hackers should be referred to as hackers, and it is even more uncertain whether I have the right to call them "illegal hackers". First, what these hackers do is seldom illegal. Second, they are closer to radio amateurs and electronics freaks than computer users. On the other hand, phreakers and computer constructors are often considered to be hackers, and furthermore, neither radio amateurs nor electronics hobbyists want anything to do with them. Plus, they also subscribe to the fundamental hacker principle that holds that information should be free... so I guess they're hackers.

If you flip to the last pages of an evening newspaper, right after the sports pages, where you find all the ads for porno movies and Rogaine, you will also find ads offering cable TV decoder kits. These kits are built by this type of hacker. The entire Swedish branch of this underground operation can be traced to the close-knit circle of Rolig Teknik (which was mentioned earlier) readers. It is hardly possible to find a decoder builder that has *not* read Rolig Teknik.

The absolutely most famous hack that has been performed by this kind of hacker was witnessed by HBO viewers on April 27, 1987. In the middle of the movie *The Falcon And The Snowman* , the broadcast was interrupted by a blank screen on which the following text appeared: *"Good Evening HBO from Captain Midnight. $12.95 a month? No Way! (Showtime/Movie Channel, Beware!)".*

The basis for this message was HBO's plans to encrypt their broadcasts so that whoever wanted to see their programs would have to purchase a decoder. **Captain Midnight** , whose real name turned out to be **John MacDougall** , had interrupted HBO's broadcast by reprogramming the satellite that transmitted on that channel.

The transmission was interesting because it showed how vulnerable the technological society is. What if Captain Midnight had instead decided to alter the satellite's trajectory, and thus sabotaged millions of dollars worth of equipment? Perhaps worst of all, the hacker penetrated every television viewers consciousness and distributed the unequivocal political message which stated that TV, as a form of information, shouldn't cost anything.

On this subject, I would also like to mention some other electronics hackers like the Uppsala-based Atari enthusiast by the name of **Marvin** (an assumed name), who together with some friends constructed their own telephone cards - "eternal" cards that never ran out.... After a lengthy process, these Uppsala hackers were given suspended sentences and fines, while Telia never received a cent in reimbursement (which was partially due to the fact that Telia itself had made orders for these cards, as they were mighty curious about the invention). Many engineering students across Sweden became so impressed by Marvin's cards that they made copies, and soon there was a considerably greater number of copies than originals. Marvin himself never manufactured very many cards. Mainly he wanted to prove that it was possible, since Telia had boasted of the superior security features of these cards.

A similar case involved the Amiga hacker **Wolf** , a resident of Helsingborg (located in southern Sweden), who managed to acquire a card reader of the type that was used for public transit (bus) cards. Wolf was an unusually crafty young man, who was familiar with all types of electronic equipment, and also very mechanically talented. He had a two-year gymnasium degree (*translator's note: in Sweden, like many other European countries, the gymnasium offers an intermediate level of schooling somewhere between High School and university, and in some cases offers degrees)* in electronics and telecommunications, but he was more dedicated than most university engineers. He had already had a run-in with the justice system for moonshining. Without any major difficulty, he managed to hook up the card reader to his Amiga and write a program that could control it. Initially, he probably only wanted to test the system to see if he could program the cards himself, but as time passed it turned into an enterprise. Eventually, it became an operation in which hundreds, perhaps thousands, of cards were forged. Due to a solid and secure database system, the regional transit authority was able to trace and block the forged cards. During a search of Wolf's residence, authorities found (among other things) Marvin's extensive description of Telia's phone cards.

The need for proper legislation for these types of crimes is pressing. There are operations that border the illegal, but that cannot be outright criminalized. It is *not* illegal to own a card reader or to manufacture fake cards. Electronic "identity documents", such as phone cards or decoders, are not considered identity documents by virtue of the fact that they are electronic, and therefore it is not illegal to possess them. Swedish legislation has simply not yet been adapted to electronic documents. However, *using* fake documents is clearly illegal. Only commercial manufacture and sales of pirate decoders is illegal - not private possession or distribution. Presumably, legislation has been limited so as not to infringe upon the freedoms of radio amateurs, which means that mail-order kits or other tools for amateur use are permitted. It would be totally legal to put up ads for phone card kits, just as decoder kits are being sold.

The solution to this controversy is, of course, not prohibition, but building systems that are so safe that they cannot be penetrated even if the attacker knows *everything* about their inner workings, which is possible through crypto-technology. The question is whether this solution is really that good. In a society that is based on electronic currency, this would serve to prevent *all* types of fraud and forgery. I will return to this subject in a later section.

Anarchists

The "hackers" that call themselves anarchists are hardly hackers in the traditional sense. Neither are they anarchists. More accurately, they're teenagers with a general interest in bombs, poisons, weapons, and drugs. Since relevant information cannot be found in most libraries, these teenagers find their way to that electronic computer culture in which all information is cross-distributed to other youths who do not themselves have children, and therefore do not feel any sort of responsibility for the information being distributed. For obvious reasons, the youths see themselves as equals, and consider the whole thing a rebellion against adult values and norms. Childish? Perhaps. As a protest against Big Brotherism, it can hardly be considered childish. In any case, there are plenty of adult "anarchists".

Anarchists distinguish themselves by distributing blueprints for weapons and bombs, drug recipes, and instructions on how to efficiently kill another person, etc., with inexhaustible interest. Some hackers become angry when they find their BBS's swamped with such material (which is often totally erroneous, dangerous, and useless); others let the anarchists carry on. The most controversial anarchist publication in Sweden is *The Terrorist's Handbook* [6] . Much of the information in the book has to do with basic pyrotechnics, and has nothing to do with terrorism (sometimes I wonder if one of my student neighbors has developed an obsession with this book, as he with inexhaustible energy detonates home-built fireworks every evening. Apparently, many chemistry students have learned a lot about pyrotechnics by studying this type of material).

Some people seem to collect similar blueprints and books in the same manner that others collect rocks or stamps. It is only recently that so-called *ASCII-traders* (ASCII stands for American Standard Code for Information Interchange, which is really a method of coding text) have surfaced; these people are information collectors who dial into different BBS's and look for exciting and somewhat *suspicious* information. Don't ask me why they do this. Collecting non-living objects is something that one engages in for no reason whatsoever. The digital information collector's obsession is obviously as strong as that of a collector of physical items.

---

[1] Alias Publications is one of the publishers that have offered to print this book. The editor-in-chief, Mikael Borg, wanted me to write more about Alias in this book, which I can understand. Alias is an excellent magazine for those who are interested in this type of material, but who don't have access to BBS's and the Internet, or the energy to dig out the electronic documents that describe hacking techniques. Alias has a shortage of good contributing writers, but they do the best they can, and the paper is interesting to read. Wicked voices claim that Alias is just out to make a quick buck, but as far as I can tell, this claim is not true. Most of the material seems to be thoroughly edited, and the design is far above underground standards.
Update : At present, Alias Publications has ceased doing business, and Mikael Borg has gone underground by moving to Thailand.
[2] After writing this, one of my articles was accepted by Phrack (see Phrack #48, article 17): a historical summary of Swedish hacking culture, based on the research I did for this book.
[3] The current method is manufacturing your own home-made cards that the new

public phones accept as real credit cards.

[4] An experienced hacker will instantly note that I've chosen a totally boring system: the AS-400.

[5] Security experts constantly emphasize that there *are* destructive hackers out there. Remember that this threatening image provides the reason for their existence.

[6] Pay attention to our definition of "anarchist" (see the first paragraph). Do not confuse hacker-anarchists with political anarchists. The Terrorist's Handbook was published in Sweden by a company that also published quite a bit of Nazi propaganda.

Chapter 5
SUBCULTURE OF THE SUBCULTURES

The phenomenon that started at MIT, becoming global through personal computers and networks, has reached us in a subtle way. It is hard to recognize it as the same thing that drove American youth to spend their days and nights hacking. Few parents had any idea that their sons (and in some cases, daughters) could be influenced by a culture rooted in American universities simply by spending a few hours in front of a computer screen. The screen in question would be hooked up to a **Commodore 64**, for (in Sweden) it is with this machine that it all began.

The high-tech (1984) C64 had gone into full bloom; hundreds of thousands of youngsters in Europe, the U.S., and Australia sat hunched over their breadbox-looking machine, fascinated by its possibilities. The C64, like the Apple II and Atari 800, was built around MOS's 6502 microprocessor (which is still in use, including in Nintendo's entertainment system), and therefore many Apple and Atari owners saw the transition to C64 as a natural progression. At first, most programs (primarily games) for the C64 were quite primitive, with poor graphics and sound reminiscent of those produced by a PC internal speaker - that is, beeps and screeches. At some point, however, the market broke through a magic barrier and so many C64's were sold that it became profitable to start companies producing software solely for this computer. This had occurred with the Apple II and Atari in the U.S., but since the C64 was first real European home computer, these companies were completely new phenomena on the east side of the Atlantic. The first companies started in the UK, which was the country that had first started importing the C64, and which became the leading edge for European computer culture.

It was the games, with their (for the time) advanced graphics and sound, that would be copied and distributed through the so-called Scene. The Scene, a kind of virtual society, started in the U.S. around 1979, when Apple II and Atari games were hot stuff. The software companies were angry, and called the Sceners pirates and criminals. Pirate BBSs for personal computers (usually consisting of an Apple II and the program *ASCII Express Professional*) had mushroomed and mixed their own values and electronic magazines into the underground hacker/phreaker movement. The most notorious BBS **was Pirate's Harbour** , which had such prominent users as the well-known crackers **Mr. Xerox** and **Krakowicz** .

Just before the C64's arrival in Sweden, and parallel with The ABC Club growing into a representative and presentable computer club, a small and tight group of Apple II enthusiasts had created an underground network. This network included **Captain Kidd** , **Mr. Big** , **Mr. Sweden** , **TAD** , **TMC** (The Mad Computerfreak), and others. Since there was no Swedish market for Apple II software, the group had imported games to crack and share. They even had contact with the infamous American Apple II underground and its BBSs. Most of the group's members advanced to a C64, and it was through them that the Swedish Scene originated. [(1)]

The concept of a "scene" is the same as in a theater or music stage. A scene is the location of a performance, where the purpose is to show off one's abilities, not to

make money or dominate other people. Scenes (or stages) are found in almost all cultural spheres, and, fascinatingly, also in techno-cultural ones such as those of radio amateurs, model airplane hobbyists, and hackers. What separates the personal computer scene from other scenes is that it ran against commercial interests, and therefore it came to be considered a dangerous and criminal subculture.

The *Scene* (capital S) is thus a label for the large group of users that exchange programs (primarily games) and also so-called demos. The thinking was straightforward: why buy a game for 25 bucks if I can copy it for free from my neighbor? This practice was, of course, illegal (which most people realized); however, it was a crime comparable to copying the neighbor's records to a cassette tape, with the exception that the copy did not suffer a loss of quality and could be infinitely reproduced. A copy of a copy of a copy would be identical to the original.

The Swedish prosecuting pioneer **Christer Ström** (from Kristianstad) and his colleagues around the world have, to an extent, been successful in curbing the commercial mass-distribution of pirated copies. However, private distribution is still alive and well, even though it is currently somewhat hampered by the fact that modern games are usually delivered on CD-ROMs, and not very easy to copy (if they are copied, they usually have to be transferred to around 50 diskettes, which makes the practice rather unwieldy and expensive). One buys the original rather than spending hours copying it [(2)] (more on this subject will follow later).

Starting January 1, 1993, all reproduction and distribution of copyrighted software (even to friends) is against Swedish law, although no individual has been sentenced for giving copies of programs to his/her friends. The crime is, as previously stated, comparable to copying records or videos, or not using your turn signal when making a turn. You can relax as long as you don't mass-distribute pirated software. Perhaps I shouldn't have said that - it is a terribly politically incorrect statement.

Anyway, back to 1984. The people that removed the (often virtually nonexistent) copy protection from the games, the so-called crackers, came up with the excellent idea of displaying their name or pseudonym (handle) on the start-up screen of a cracked program. The phenomenon is, together with many other phenomena in the hacking world, related to graffiti. If we take into account that such a copy could reach tens of thousands of people (many more than would read something sprayed on a concrete wall), it is not hard to understand how the practice became so popular. Hackers with handles such as **Mr. Z** , TMC (The Mercenary Hacker), **WASP** (We Against Software Protection), **Radwar** , **Dynamic Duo** , or **CCS** (Computerbrains Cracking Service) figured heavily on screens everywhere. Sometimes individual hackers hid behind these pseudonyms, sometimes loosely connected groups. In the U.S., there were already firmly established and well-organized cracking groups, but in Sweden and Europe, the phenomenon was completely new. The underground hacker movement started to grow from scratch, especially in the larger cities, where there were plenty of hackers that would meet at different computer clubs and exchange knowledge and programs.

The personal computer had incredible penetration as a medium, and several hacker groups soon formed, spending all their time removing copy protections from games, and then compressing and distributing the products (known as wares or warez).

Among the first groups was the American **Elite Circle** , which had its roots in both phreaker and hacker culture, and had already managed pirate BBSs for Apple II and Atari software. The notion of cracking and distributing games came from the USA, where it had started with an Apple II program called *Locksmith* . It could remove copy protections from programs using certain parameters. In the beginning, it was enough to simply change the parameters for this program to crack a piece of software, but later it became necessary to spend more work on the actual cracking, and the cracker him/herself would have to be a programmer.

The hackers cracked programs because they were pissed off at the software companies for putting in copy protection routines that prevented them from looking around inside the programs and copying them for their friends. They wanted information to be free. This was the true reason, even though many gave justifications such as "The programs are too expensive, I only copy programs I couldn't afford to buy anyway, I want to test it before I buy it", etc., which were only partially true. The fundamental belief was that information was not property, and that they did not want to be part of any software industry.

One of the first programs to be pirated, and perhaps the first ever, was *Altair BASIC* . It was delivered on a punch card for the computer with the same name. BASIC stands for Beginner's All-purpose Symbolic Instruction Code, and Altair BASIC was written by none less than Bill Gates himself. Behind the reproduction was one of the members of **Homebrew Computer Club** in Silicon Valley, a hacker (**Dan Sokol**) who would later be known as **Nightstalker** . He wrote a program that copied the punch card pattern and thus became the world's first cracker. The 19-year-old Gates was up in arms: he wrote an angry letter to the user groups in which he claimed that copying a program was theft and would ruin the industry. Most thought little Bill was an idiot; no one had ever tried to sell computer programs before, and the norm was for everyone to share everything. For the large computer systems, the software came with the machine, and nobody really cared if it was copied. With personal computers came software piracy, simply because there were software companies that wanted to profit from this new hobby. The hobbyists themselves never asked for any software companies.

Here, it is necessary to make a crucial distinction: hackers distinguish between regular distribution of a program to friends and the activities of pirates. Pirates are not friends but people who try to profit from reproducing and distributing software. Pirates are parasites that prey on personal computer users, who just want software, as well as the computer industry in general. Both hackers and members of the software industry think that pirates are scum. The software companies hate them for stealing their income, and hackers hate them because they try create a new dependency relationship that is no better than the old one. Hackers, in general, firmly believe that copying should be done on a friendly basis and for free. Only in a few exceptional cases have hackers cooperated with pirates to get original games (nowadays known under the more cryptic term "licenses") for cracking purposes. Sweden's greatest pirate of all time, **Jerker** (fictitious name), was a retired father of two, in his forties, and hated by the industry as well as the hackers (with the possible exception of the **Xakk** group, which depended on him for their originals). Rumor has it that he's not given up piracy, and still makes his living selling illegal copies. Jerker says that he is not really

interested in computers, and it seems to be true. Personally, I think that he has a considerably greater interest in money.

The Scene in 1986: as hackers developed their programming expertise, the introductory screens displayed at the beginning of cracked games became more advanced and grew into several dimensions. Hackers were inspired by title screens and sequences from games, and the introductory screens went from comprising mainly vertically scrolling text to advanced graphics with animation, sound, and sophisticated technical tricks that made the show more cool. A new art form, the *Intro* , was born, and it was practiced solely by programmers. Although the art of demo writing had existed (in a simple form) in the time of the Apple II, the C64 and its advanced technology permitted it to bloom. Groups like **Eagle Soft** , **Hotline** , **Comics Group** , **FAC** (Federation Against Copyright), **Triad** , and **Fairlight** flooded the Scene in the last half of the 80's.

Some of these groups started their own BBS's where ideas were exchanged and programs distributed. The word *elite* was adopted as a term for the groups that were the most productive and had the most distribution channels (especially to the USA). The European part of the Scene had an obsession with distributing their cracked games to the United States as quickly as possible. It was probably due to a form of "sibling rivalry", since the Scene itself started with the American Apple II computers, and the most experienced hackers were from the U.S. It was important to impress "big brother" with your cracked games. In the European Scene, more ties to the USA meant higher elite status.

The demand for open communication channels led to the hackers attacking the Internet (among other things), and cooperating with European and American phreakers to open more channels to the West. The phreakers and network hackers called these newcomers from the world of personal computing *Warez d00ds* , since they were always bringing "wares" in the form of pirated or cracked games. They referred to themselves as traders, or, more expressly, modem traders, since they used modems to connect to different BBSs. At first it was Americans skilled in the fine art of phreaking who contacted different European cracking groups, and later the Europeans themselves started calling the U.S., hacking Internet computers, etc.

Eventually, the Europeans' inferiority complex with respect to the "big brother of the west" had the result that the European home computer hackers, in their struggle to excel, developed programming and cracking skills totally superior to their American counterparts. During 1987-88, American computer game companies began adding copy protection to software exported to Europe, but not to the games sold within the U.S. They feared the European cracking groups, and Sweden in particular was considered an unusually dangerous country. The computer gaming industry suggested that much of the pirated software that circulated through the U.S. and Europe originated in Sweden, which is actually true. Most of these games came from an imports store in Göteborg (Gothenburg), which was visited once a week by a Swedish hacker who was supposedly "reviewing" new games. Without the storekeepers' knowledge, he copied the games and distributed them to various Swedish crackers.

It didn't take long for someone to come up with the idea of separating the intros from the games, letting them stand for themselves; the intro would even be allowed to

occupy all of the computer's memory. This resulted in the birth of demo programs (or *demos*), which were dedicated to graphical and musical performances and extraordinary technical tricks. The first demos were collections of musical themes from various games, usually accompanied by a simple text screen. For the most part, it was the same groups that had previously done cracking and intros that migrated to demo creation, but "pure" demo groups also surfaced, such as **1001 Crew** , **The Judges** , **Scoop** , and **Ash & Dave** . A distinct jargon and theory of beauty developed, mainly through the exchange of programs and knowledge on England's **Compunet** , which was an enormous conferencing system dedicated solely to personal computer fans. Compunet became the hard core of the demo groups, but most of the software exchange still took place through disk trading and BBSs. Later, and especially during 1988, the underground magazine *Illegal* became a sort of cultural nexus for this rapidly growing society.

Norms for telling the bad from the good evolved quickly, and the widespread expression *lamer* was introduced as a term for people who didn't want to program, and instead used presentation software to produce demos. Probably, the term originates in skater slang. The word lamer spread far outside hackers' circles, and soon applied to any computer-illiterate person. Many similar slang terms have been derived from the Scene, but these relationships are not expressed in the Jargon File; rather, the document serves to perpetuate the negative view of subcultural hackers (to whom it invariably refers to as warez d00ds). This view is both erroneous and prejudiced.

From an American perspective, it is understandable that the academic hackers from MIT, Berkeley, Stanford etc. considered the personal computer hackers amateurs of little value; in the U.S., virtually all teenagers with a personal computer were exclusively interested in games. American demos and intros were primitive, and nowhere near the level of sophistication of the European ones. On the whole, the American part of the Scene had a less developed culture than the European side. The American hackers were heavily influenced by the phreaker culture, and as a result usually insolent and aggressive. The feelings of contempt were mutual.

An unfortunate consequence of this animosity is that European hackers searching for their identity are easily attracted by American hacker ideals, and thus assume a slightly scornful attitude towards personal computer enthusiasts. It is worth noting that the cultural foundation of European hackers consisted of personal computer hobbyists, and not of phreakers, network hackers, or small academic clubs at universities. The European hacker identity was built around Commodore's and Atari's personal computers, and this is where the European hacker should seek his/her roots. In addition, there are (of course) values and traditions inherited from the American universities. However, one thing is fairly certain: the European personal computer hackers developed the art of computing in a way that never occurred in the U.S. The aggregate of European teenage hackers created a beautiful and amateur-based art form of a kind that MIT and Stanford never witnessed.

The Art Form of the Demo

A demo is somewhat difficult to define; it really has to be experienced. Even the first hackers at MIT created (around 1961) simple demos in the form of small mathematical patterns that were displayed on a simple screen. These were called *Tri-*

pos or *Minskytron* -patterns (after the professor of the same name). The demos were beautiful, but lacked practical applications.

Sine curves, scrolling text, and mobile blocks of graphics coupled with music constituted the first personal computer intros. As time has progressed, the products have come to resemble motion pictures or corporate demonstrations, known as *trackmos* . The name is derived from the fact that new data has to be loaded continuously from disk to keep the demo running (a disk is subdivided into tracks, hence trackmo). Since MIT, demo programmers have had a passion for weaving mathematical image patterns into their creations.

As the demos appeared, this new cultural expression began spreading from the C64 to other computer platforms. First, it migrated to the Atari ST (1984) with groups such as **TCB** (The Care Bears) and **Omega** , and later (1986) to the Commodore Amiga, where (among others) **Defjam** , **Top Swap** , **Northstar** and **TCC/Red Sector** , and later **Skid Row** and **Paradox** , became well-known. In 1988-89, demos started to appear even for the IBM PC, from (among others) the Swedish pioneers **TDT** (The Dream Team) and **Space Pigs** . (The Macintosh has, to my knowledge, never nurtured any significant demo activity, but this may change as the Mac has become more of a "personal computer"). The transfer of games, intros, and demos was completely dependent on a network of postal mail and a great number of individuals and BBS's that called cross-nationally and cross-continentally to distribute the programs. During the 80's, the demo groups couldn't afford to connect to the Internet; only a few university hackers had that opportunity, and most of the Commodore hackers were in secondary school. Most of the university hackers were of the "old-fashioned" kind, and completely ignored personal computers in favor of minicomputers (which were the coolest things around in their opinion).

Since computer programs are often copied through several generations (copies distributed and then copied and distributed.... etc.), they offer an exceptional opportunity for the distribution of names and addresses to help expand the trading market. Fairly quickly, the early hacking groups recruited members whose only purpose was to copy and trade demos with others of similar mind, primarily in order to spread their own group's creations. These members were known as *swappers* , and a diligent swapper could have around a hundred contacts. Since it wasn't very economical to send dozens of letters a month, many (to the chagrin of the postal service) started spraying liquid Band-Aid on the postage stamps so that they would "last longer".

Pure swappers soon discovered that it was possible to trade merchandise other than disks, and two new subcultures emerged: film-swappers and tape-swappers. The former engaged in the exchange of videos of all types, although primarily movies that were banned by some government, or that were exciting for some other reason. The tape-swappers exchanged music cassettes.

Disk swaps among hackers have been extremely important as a contact surface for these subcultures. The word disk-swapper is never used in writing by the hackers, since the word (in its pure form) simply indicates the exchange of disks. Film-swappers in particular are connected to the hacker culture, since the breakthrough of the VCR coincided with the personal computer boom in the mid-80's. Frequently, a

swapper trades disks, cassettes, video tapes, or any other media that can be duplicated. The difference between a swapper and a regular pen-pal is that the content of the swap (the disk, cassette, or whatever) is more important than anything else. If you don't feel like writing a letter, you just send a disk labeled with your own name so that the recipient will know who sent it. Disk swapping is, however, a phenomenon associated with the European personal computer hackers of the 80's. For the IBM PC of the 90's, this procedure is relatively uncommon - the standard nowadays is to get the programs you want from a BBS or even the Internet. Swapping has given way to trading, that is, the exchange of information has gone from disks to modems.

In the beginning, hacker groups consisted of just programmers and swappers, or individuals that were a combination of the two. The most successful groups of this kind have always been those who enjoyed geographic proximity, enabling their members to exchange ideas and knowledge without expensive and troublesome telephone connections. After some time, a need for more specialized hackers arose, and categories like musicians, graphics experts, the previously mentioned crackers, and coders emerged. The difference between a cracker and a coder was that the former specialized in removing copy protection (i.e. modifying existing programs), while the latter was concerned with pure programming (or coding).

To destroy copy protection routines is not illegal in itself (actually, you pretty much have the right to do whatever you want to with a product that you have purchased). On the other hand, widespread distribution of the "cracked" program, which the swappers frequently engaged in, is highly illegal (although I should point out that many of the swappers only traded demos, and stayed away from distributing copyrighted software). However, we again run into the similar act of copying music CD's, which is just as illegal. No law enforcement agency in its right mind would ever get the urge to strike against a hobby hacker who copied software for his or her friends, as long as it wasn't not done in a commercial capacity. The crackers and traders did not know this, which made the practice more exciting and "forbidden" (remember that the average hacker was in his or her teens, and that it is very important to rebel against society at that age).

In the U.S., there was another category of hackers called fixers. The fixers modified the code generating the signals for European PAL television systems to fit the American NTSC standard. (These hackers did not exist among the PC hackers, because all PC's have their own video systems intended for monitors rather than TVs). Some hackers also had suppliers, who acquired the original programs that the crackers stripped of copy protection routines. It was not unusual for these suppliers to work in software retail stores or even at software companies.

For social reasons, so-called copy-parties were held, as early as 1984, at which many hackers from different groups got together (in some city) to interact and trade knowledge and experiences. Possibly, the hackers drew inspiration from *The Whole Earth Catalog's* first hacker conference in that year. The event is reminiscent of role-playing conventions in that it is a rather narrow group of interested parties that gather, but it is different in that the mood is rather tumultuous and unrestrained, more like a big party than a regular convention. The term copy-party stems from the fact that a great deal of copying took place at these parties, both legal and illegal. Nowadays, salience has been reduced by calling the events demo-parties or simply parties. A

famous series of recurring copy- parties were held during the 80's in the small Dutch town of Venlo. The Party (capital P) is probably Europe's (or even the world's) largest and most frequented copy party. Since 1991, it is held annually during December 27-30 in Herning Messecenter, Denmark, and attracted close to 2000 people in 1994.

Not even hackers always get along: confrontations between groups or individuals often escalated into "gang wars", mostly involving psychological warfare. The objective was to ostracize a person or group by refusing to exchange disks, and encouraging friends to join in the boycott. In this manner, an individual or a group could be "excommunicated" from the community. To reach this goal, lengthy text files containing pointed truths or pure lies were distributed, whereupon the accused retaliated using the same technique. The wars basically never produced any tangible outcomes, and copy-party melees were extremely rare. Conducting psychological warfare against other hackers should be regarded as rather harmless, even though the participants were often fervently committed to the battle. It should be assumed that these schisms taught teenage hackers a great deal about the true nature of war: it rages for a while, then dissipates, only to flare up elsewhere. Some leave the Scene (or die in a real war), but most remain, and some day another disagreement occurs.

I would like to take the opportunity to mention that among the phreakers, these wars ended much more quickly: you simply reported your enemy to the police. This was the only way to practically interfere with a phreaker's life. Among both the phreakers and hackers, however, friendship dominated over strife. Through the occasional wars between hacker groups, yet another aspect of human behavior was transferred to cyberspace. Abstractions of war as an advanced chess game in the form of confrontations on the Scene as well as in many different role-playing games, or tangibly as in the movie War Games, have given many hackers a cynical view of human nature.

Those who are (and were) active on the Scene participate because they have a relationship with the computer that is different from that of any previous generation. Where one person only sees a box, a machine with a screen and keyboard, the hobby hacker sees an entire world, filled with its own secrets and social mores. It is these hidden secrets that spellbind and beckon the hacker, and makes him or her forget everything else. The search for more knowledge accelerates toward a critical mass, a sustained level of intensive productivity. This is the state in which a hacker produces a demo in two weeks or cracks one game per day. All social interaction outside the realm of the computer and its users becomes insignificant.

Eventually, most reach a limit at which they grow weary of the Scene and the eternal quest for something newer, bigger, and better. They simply quit. One hacker that I know well once told me: "The only real way to quit is dragging the computer to a swamp and dumping it". This serves to illustrate the weariness following exaggerated participation on the Scene. Others keep their hacking to moderate levels, and lead normal lives apart from their hobby. These moderates tend to stay on the Scene the longest (personally I've been on the Scene since 1986 and I remain there today, albeit as a somewhat sporadically active member).

The Scene reveals a great deal about the true nature of hacking culture; it is a roof under which to gather. Hacking is about the exploration of computers, computer

systems, and networks, but also an inquiry into the workings of society, and the creation of new and personal things through experimenting with subcultures. That is why hackers break into systems to which they are not authorized, spray fixative on postage stamps, and blatantly disregard any form of copyright. They want to explore and see how things work. Perhaps subconsciously, they want to prepare for the future. The hacker culture emphasizes exploration, not cold-blooded theft, and hackers are not egocentric criminals that only seek destruction [(3)].

The actual motivation for real hackers is simply exploration, while someone who hacks with theft or sabotage as a motive is a computer criminal and not a hacker. Jörgen Nissens has written a fascinating thesis called Pojkarna Vid Datorn (The Boys at the Computer), which makes it clear how special the hacker culture surrounding personal computing really is. He has interviewed some of the hackers in the groups Fairlight and TCB, and points out how strange it is to hear members speaking of market shares of the Scene, and how the groups are run under something similar to corporate principles, even though they lack a profit motive. He also emphasizes that hackers behave more like bored consumers than criminals or classical youth gangs; they are members of what Douglas Coupland refers to as Generation X.

The personal computer groups are typical of Generation X. They abhor politically correct messages, they run everything like a business, and they are sick of the enormous market. Instead of consuming, they started producing. Instead of manipulating money to achieve status and enjoy the admiration of others, they have created a market where they trade creativity for admiration without any material layers in between. No CD's, promotion tours, or marketing schemes are necessary. There is only a need for pure information products in the form of demos and cracked games, which are traded for pure information in the form of respect and admiration.

The only subcultural hackers to receive any great media attention were those who crossed the line to network hacking or phreaking and got busted. In 1989, parts of the circle surrounding the demo group *Agile* were arrested after one of their members, **Erik XIV** (fictitious name), went to the media and exposed how vulnerable credit card transactions really were. At the same time, another of their members, **Erlang** (also a fictitious name), ordered video editing equipment for a quarter of a million crowns (about $35,000) to his own home address using fake credit card numbers. Driven by their slightly elitist attitude from the demo culture, they wanted to be alone in their mastery of credit card technology, and tested the limits of what was possible using artificial codes.

When the police arrested Erlang after he had ordered the editing equipment, he started telling them everything with an almost pathological obsession with detail. Phreakers and hackers often do this; it seems as if they believe the police will be impressed by their feats. The people involved in the Agile case were all given suspended sentences, high fines, and probation. All of them, save Erlang, now work in the computer industry (surprise?).

Attitudes

The first hackers at MIT always made use of all the technological resources they could lay their hands on. It wasn't always the case that the "authorities", the professors and custodians responsible for the equipment, approved of this behavior. Most

teachers thought that instruction in computer science should be of the classical authoritarian kind, where the professor stood at the lectern and lectured. If the students were to have access to the computers it should be through explicit assignments to be turned in for grading, not through the learning by doing that the hackers practiced. They loved the computers, and couldn't for the life of them imagine why they would be kept away from the machines. They sneaked in at night and used the machines unbeknownst to the instructors.

After several personal confrontations with computer professors, and especially after having worked as a computer instructor myself, I have realized that this classical emphasis on utility is all too common among Swedish computer teachers. It is simply not possible to get people to think that "computers are fun" if you at the same time force them to adhere to rules for what they are allowed and not allowed to do with the computer. Many computer instructors throw a fit when they discover that the students have installed their own programs on the computers, or have programmed something that wasn't the subject of an assignment. Common reasons for this behavior are a paranoid fear of viruses, the view that computer games are just a waste of time, and so on. One teacher at my old gymnasium (secondary school), which we will call X, installed a program on his computers which triggered a screeching alarm as soon as someone tried to change any of the machines' configurations (the machine configuration, in this case, is a couple of files with information that allows the computer to use different accessories). Of course, an exploring hacker will feel like changing the configurations, and the school's own binary geniuses naturally ignored the large posters all over the computer room proclaiming that this activity was absolutely prohibited. Central to this story is the fact that the teacher was a foreign language instructor, who could not under any circumstances accept that "his" computers would be used for anything else than language programs, word processing, or other authorized activities. Some students that triggered the alarm were banned from the linguistics computer lab, while the more skillful students (who knew how to change the configuration without setting off the alarm) were still permitted in the computer room, despite having changed the configuration many times.

These students, who possessed some of the true hacker mentality that says that you shouldn't accept a monopoly on knowledge or computing power, wrote an amusing little program. Besides completely circumventing X's little security system, the program also randomly displayed a requester, a small text window which said: X IS A MORON. Below this text was an "OK"-button that had to be pressed in order to proceed. The program was a classical hack: it wasn't very useful, but it didn't do any real harm, and it was funny. The first hackers at MIT would surely have appreciated this prank (personally, I find it exquisite!). It was completely impossible for the teacher in question to find and remove the program. In the end, he had to format all the hard drives on the computers and reinstall all the software from scratch. To face the music and ask the hacking students to remove the program, or even apologize to them, never occurred to him. Doing this would not only mean recognizing the students' right to use the computers, it would also mean confessing the truth - that some of the students were more adept in computer science than himself.

The fact is: the parents of these students had paid taxes to enable their children to use computers at school. The students, like hackers in general, were therefore of the opinion that the natural thing would be to let them use the computers to do whatever

they wanted, and as much as they wanted (outside regular class hours, of course). This obvious right has been known since the time of the MIT hackers as the hands-on imperative.

Computer instructors frequently do not understand hackers. They think that if the hackers have to mess around with the computers all the time, why can't they do something useful and authorized, such as figuring out a repayment plan, or writing a summary of African history, or something along those lines? The predominant attitude seems to be that the students should only use the machines, not explore them, and definitely not hack them. The machine should only be a tool, and the user should preferably know as little as possible about the processes that take place behind the screen. The hacker is the one who, in spite of these authoritarian attitudes, actually wants to know.

Hackers don't want to do "useful" things. They want to do fun things, like exploring the computer's operating system, installing their own programs, and trying out different technological features. This is what makes it fun to use a computer. I have tried to mention this to several computer instructors of my acquaintance, but alas, mostly with no results. I personally believe that this kind of exploration is beneficial, and wouldn't for the life of me want to prohibit students from engaging in it. It is the foundation for the enthusiasm that makes some people think that "computers are so much fun". If a student, after all, manages to screw up the computer, I consider it my responsibility as a teacher to restore the machine to full functionality again. If I can't do this, I'm incompetent. If I don't have time to do this, the school is short-staffed. I have never had any significant problems with my own students; in fact, I have invariably had positive experiences with them. The fact is that I encourage my students to explore the operating system even if it is not the subject matter of the course. If the computers I'm responsible for are infected by viruses or crash, then it is my problem rather than the students'.

At MIT in 1960, the possibilities that opened up when students were allowed to freely access the equipment were quickly discovered. Professor Marvin Minsky would walk into the computer room, put down some electronic device and then let the students try to develop a control program for it on their own. This was not instruction - it was high-level research, and it was the students, the hackers, that conducted it. If it hadn't been for this attitude towards learning, computers would never have become what they are today. After MIT became the first computer school in the world to allow the students unlimited access to the computers, this new pedagogy spread to all universities that were engaged in computer research, including the Swedish ones. No self-respecting university today bans their students from the computer rooms. They often have their own keys or keycards, and can come and go as they please. The Swedish primary and secondary schools have a lot to learn from the universities in this respect.

The fact is that the network hackers' mayhem in the university computers divide the computer staff into two camps: those who fly off the handle when they discover that someone has hacked their computer, and those who find it interesting and exciting if someone hacks their computer. The latter group, however, is not nearly as vocal as the first, which has led to the popular view that all computer professors or information officers hate hackers. This is far from the truth. The hacker is engaged in exploration.

Not just of single computers, but also of computer systems, computer networks, the telephone network, or anything electronic. They condemn and/or ignore the authority that wants to prevent them from exploring. They are not motivated by theft. Period.

Mentality

What keeps hackers going from a psychological perspective is a sensitive subject. MIT's hackers could stay up and work a 30-hour shift, then crash for about 12 hours, only to get up and complete another 30-hour shift. Sometimes, hackers neglect everything but the computer, including nutrition, hygiene, and normal social interaction. We see this as unhealthy, although we may accept it among persons working on corporate boards, committees, or other professions with a high degree of responsibility. It should be made clear that virtually every hacker goes through such a period of intense concentration at some point in his/her career, and it would be hasty to condemn such behavior in general.

In some cases, the computer is actually a means of escape from an intolerable existence. A youth in the ages of 14 to 19 is subject to many harsh demands from his or her environment. It is demanded that they should be able to handle school, socialize with their friends, and (implicitly) connect with the opposite sex. At the same time, one should not forget that hacking is often conducted in a group environment, and it is based on a friendship that goes far beyond the limited area of computing (For the uninitiated: friendship is the phenomenon that makes someone get the idea of lending a room to someone else for a few days, copy a computer program, share knowledge, etc., without demanding payment).

The computer offers a convenient escape from the demands of growing up. In earlier stages of history, many men (and some women) have distanced themselves from difficult emotions by whole-heartedly dedicating themselves to some science, and becoming so totally wrapped up in their research that they "forget" their troublesome social "duties" such as friends, marriage, and all that the entail. Computing, in our time, is a largely unexplored territory. Everyone with access to a computer is instantly drawn into a world in which much is strange and unknown, but which at the same time possesses an underlying logic. A computer begs to be explored. In this way, the computer can almost become a drug that replaces a more "natural" urge to explore social behavior patterns. The excursions into the computer do not become a substitute for sexual relations; it becomes something that you occupy yourself with so you don't have to think about sexual relations. This is why so many so-called "nerds" spend most of their time with computers. Society has given them a thankless role from the beginning, and instead of playing along with it, they escape it.

Many hackers are fully aware of this escape. At the same time, they see the hard life, ruled by the laws of the jungle, lurking outside cyberspace, and they finally make a conscious decision to either change everything or stay where they are. Some old hackers have, through the years, developed an incredible cynicism because of this. They condemn the real world and are committed to creating a world in which they can rule for themselves, inside the computers. They observe technological advances in virtual reality and artificial intelligence with excitement, and tell themselves that *one day ...*

If they could go into the computer forever, they would. They already hate the "real" world in which they have to feel restrained by their physical or social disabilities, and where their fate as losers has already been determined. The human sexual identity consists of a social as well as physical side, and if you lack one or the other, you're destined to be a loser. It happens that hackers become aware of this, and instead say: "We don't want to be part of it", and then retreat to cyberspace. There is nothing we can do about this, except possibly tone down our social attitudes towards those who are different, if even that would help. Maybe it is undesirable to have hackers adjust to a "normal" life. Maybe we want them where they are, where they feed their brains with so many practical problems that they don't have to think about social dilemmas, so that we can keep track of them and keep them under control. They are contained in a subculture where the weird is normal. Their condition can, at worst, develop into mild or severe escapism, i. e. escaping from reality. This condition is usually called computer sickness.

In addition, we can observe that illegal hackers possess a somewhat different pattern of behavior compared to the subcultural hackers, depending on which way they have entered the culture. Some phreakers come from an environment consisting of party lines, amateur societies, etc. They are driven by a desire to communicate, rather than exploration through the formation of groups and internal competition. They are often considerably more arrogant and practice phreaking simply because they are bored, and have nothing better to do (it's the same motivational factor as for people who dial various party lines on 900-numbers). They don't take hacking to be a deadly serious business, and often make fun of hackers, since deep down they think the hackers are complete geeks.

Hackers, who would rather spend time with computers than with telephones, generally identify with their group and possess more group loyalty. A pure phreaker, of the kind I just discussed, would have no problem at all turning his/her friends in to the police if he/she got busted, while a real hacker would never turn in even his/her enemies.

Network hackers, as well as phreakers, virus hackers, and some crackers, suffer from a hopelessly negative self-image. They see themselves as mean, cruel, and dominant badasses. They have assumed a role in which they identify themselves with a desire for destruction, hate of society, anarchism and general mischief, mainly to feel a sense of belonging. For most, this is only a temporary stage. If they have assumed yippie ideals, however, it is not temporary.

The most dangerous hackers (from the perspective of society at large) are invariably bitter. They consider themselves misunderstood and misjudged by the educational system. They think that the schools have been unsuccessful in harnessing their intelligence and talent, and consider themselves to have a right to exact revenge on a society that shut them out of a world of knowledge, simply because they didn't act the right way, and lacked the proper social code. They have been forced into vocational schools by a grading system that has been unable to distinguish them among those who are truly suited towards higher education.

What makes matters worse is that they are *right*. With the hate of a society that couldn't or wouldn't appreciate their qualities, they return with computers and

electronic equipment to saw through the pillars of the same society's entire socioeconomic system, often with a nearly psychopathic lust for destruction.

> **Carceres Ex Novum**
> *"There was an alternative to normal life. I was sick of the normal, sick of always being last. I found friends that I never had to meet face-to-face, and so my teenage years passed, and I became an interesting person. When I started at university the gigantic Internet came to my room, and the world was beamed to me. I had millions of people close by, without ever having to look them in the face. I sat there all the time, only pausing to eat and go to class. I didn't meet anyone, no one knew me. And I was comfortable. Thanks to the attention of the anonymous people on the other side of the screen, I did not feel lonely. But time ran out, and the real world crept closer. Of course, I knew I could run away forever, but I would never be able to hide from them, the ones whose values transformed me into a lonely, asocial rat, who spent all of his time with the computer. And I hated them."*

Certainly some of the activities engaged in by hackers are illegal, and certainly this is wrong from the viewpoint of society. Nevertheless, it would be to severely underestimate hackers to say that they commit these acts in a routine fashion, for "lack of something better to do", or for their own profit. There has been too much judgment and too little understanding in the hacker debate.

But now for something completely different.

---

1. I am here deeply indebted to Christer Ericson, who shared his knowledge of the Apple II movement in Sweden; this information had hitherto not been written down, and therefore difficult to retrieve.

2. Currently, even CD-ROMs are copied to a great extent. Especially MP3 (or MPEG Layer 3), a system for sound compression, has become popular as it provides a means for the mass distribution of music CDs (which I personally believed to be pure fantasy until about a year ago). This compact music format compresses a sound CD at a ratio of 1:12, and a normal pop song is transformed into a 3-4 Mb file, which can easily be transferred across the Internet. In five years, I'm sure videos will be distributed across the Net!

3. I'm sure you notice that I'm getting personal now.

Chapter 6
THE BLEEP CULTURE

The American Heritage College Dictionary defines electronic music as follows: "Music produced or altered by electronic means, as by a tape recorder or synthesizer."

Electronic music has long existed as a subculture within "real music", especially in Sweden. In 1948 (the same year that **IBM** started marketing the first commercial computer) a certain **Pierre Schaeffer** created the first electronic music composition, which he called *Études aux Chemins de Fer* (Etudes for Trains). Electronic music was born in his studio for *Musique Concrète* (Concrete Music) at Radio France. Concrete music is music that is not limited to pure tones, and incorporates sounds from everyday life, such as long, continually changing notes without tone quality, etc. In 1952-53, the musician **Karlheinz Stockhausen** worked with Schaeffer, and brought some of Schaeffer's ideas home to Germany. Since then, this form of music has spread and is on the curriculum at different public institutions as a very small branch of classical music. As opposed to Schaeffer, who preferred to work with taped recordings of real sounds such as those of trains or birds, Stockhausen focused on using only electronically created sounds. In Sweden, this music form was basically unknown until it was introduced in **Harry Martinsson**'s science-fiction opera *Aniara* in 1959.

This chapter is not about classical electronic music - there are plenty of texts on the subject. Furthermore, this book is aimed at regular people who think that art should reflect something, i.e. that one should not constantly try to break out of existing concepts and conceptual systems to appear as incomprehensible as possible. Electronic music is a form in which the music has to be interpreted on more levels than the musical. In other words: this book will stick to a broader aspect of popular culture. This is not to say that the art of electronic music is not interesting; it is just not particularly interesting for the purpose of this book.

It is unnecessary to point out that the history of electronic music stretches farther back than the history of hacker culture. However, the phenomenon of electronic music has had a profound influence on hacker culture, and in its pop-culture manifestation in the forms of synth-pop, techno, acid, house, etc., it has played an important role for the generation that grew up with computers. One of its main uses has been to display the beautiful side of the computer. Electronic music was the first area in which computers were used to create art, and as opposed to other forms of electronic culture, electronic music has its roots in Europe.

The first time a computer played music was in 1957, at Bell Labs in the United States. The song was called *Daisy*, which is the same piece that the intelligent computer *HAL* (in **Stanley Kubrick**'s film version of **Arthur C. Clarke**'s science fiction novel *2001*) starts humming as it is being disassembled. Naturally, this is not a coincidence, but rather the intention of the director to return the computer to its "childhood state" (in a double sense) as it loses its advanced electronic identity.

The world in the 70's and 80's: With the introduction of the first cheap Japanese synthesizers, regular people (who were not trained musicians) started using electronic

instruments, and electronic pop music was born. The difference between, for example, the Hammond organ or Pink Floyd's monophonic synthesizers and the new generation of electronic instruments was that the latter could store rhythms and entire pieces of songs in their digital memory, which could later be modified. In particular, quantization (which adapts notes played to a given rhythm) was (and is) greatly criticized by "serious" musicians. They thought that simple and rhythmically perfect melodies were destructive to music, and they distanced themselves from it. Another factor that abhorred musicians of the old school was that music played by machines would not be limited by the dexterity of a given musician, which allowed the ability of the ear to perceive sound variations to set the limits for the music. A "groove" of several hundred beats a minute, or pieces with tone lengths of several hundredths of seconds - songs like those scare the living daylights out of musicians who are accustomed to being able to analyze the music they listen to.

For the new electronic musicians, the perfect quantization, the possibility of a high pace, and synthetic "sound images" constituted a measure of beauty. Among the pioneers, the most notable was the German band **Kraftwerk**, who built their own synthesizers and should be considered classics of the genre. Kraftwerk's importance for synth music can hardly be exaggerated. No single group has had as much influence on electronic pop music as these futurists - futurists in the sense that they saw the inherent beauty of the technology, rather than a tool for reproducing other ideals. They made contact with the previuosly named Karlehinz Stockhausen at an early stage, and drew lots of ideas and inspiration from classical electronic music.

Kraftwerk, and in particular its member **Ralf Hütter**, are also extremely politically aware and openly supports hackers. Sometimes, Ralf even refers to himself as a hacker. The mentality of these German gentlemen has thus influenced - and been influenced by - the digital underground culture around the world. Chaos Computer Club member Pengo, who was previously mentioned in connection with illegal hackers, was a Kraftwerk fan, and he listened to their records over and over while breaking into computers around the globe. He was not alone in this. Even though hackers in general have disparate musical tastes, from Bach to death metal, there are few who do not enjoy electronic music in some form or another.

While a "normal" educated musician perhaps sees the computer as a tool for producing compositions, musical arrangements, and nice-looking sheet music, a futuristic musician sees the computer as an instrument, something to be played by its own right, and which - like a saxophone or a harp - possesses an inner beauty. The futuristic musician can sit for hours and adjust different parameters to extract personal sounds from the machine, and he/she loves it as much as a guitarist loves to extrapolate his/her scales up and down in the search for a greater personal touch.

While a "normal" musician creates his or her profile through finding new techniques to manipulate his/her existing instrument, the electronic musician works with numeric parameters, spectrum analyzers, and one-handed play. Some don't know how to play an instrument at all, and stick to writing the music note by note in something like a "musical word processor". The method may be radically distinct from traditional music creation, but that doesn't mean that electro-pop has less 'soul".

Peter Samson, as one of the very first hackers at MIT (yes, we're back there again), had managed to get a PDP-1 computer to play Bach fugues solely based on numerical input. His program could be said to be the first sequencer made by an amateur. A sequencer is a computer program or a machine that remembers the notes to be played, and allows the user to change the notes, replay them, then store them again to replay them at some other time. Since that day, we have enjoyed a living, machine-made music culture. Many musicians of the old school react with outright xenophobia against this new way of working with music, rather than enjoy its benefits and try to understand what the point is.

Among Swedish electro-pioneers there was **Page** (which is still an active band). During the early 80's the group was one of the first (and for its genre, also one of the most successful) so-called synth-pop groups. Many jumped on the synth bandwagon, but have presently been forgotten. Who listens to groups like **Trans-X**, **Ultravox**, or **Texas Instruments** today? Not many, even if there are still quite a few synth-pop fans around the country. The genre has returned in the form of groups such as **S.P.O.C.K.** or newcomers **Children Within**, which are both very talented Swedish bands.

As a reaction against the frequently well-groomed and "nice" synth bands (read: Howard Jones, Depeche Mode, etc.) that flourished in the mid-80's, there came a new and incredibly heavy form of synth music: Electric Body Music, or simply *EBM*. Mostly, it was just referred to as "raw synth". The English band **Cabaret Voltair** had "invented" the style in 1978, but it was not until now that it reached popularity on the Continent and in America. Among others, **Portion Control**, **Front 242** (who coined the term EBM), **Skinny Puppy**, and **Invincible Spirit** joined the trend. One can compare the arrival of heavy synth music to the introduction of grunge (personified by Nirvana) as a reaction to "poodle rock" - there were simply too much corny stuff out there. Less successful was perhaps the tendency of many heavy synth bands to flirt with nazi symbolism and clothing, and many groups (including Front 242) had to make public statements denying any connection to or support of neo-nazi movements.

In the 90's, many groups have grown weary of the EBM concept, since it started to become a bit trite. For example, **Ministry**, **Die Krupps**, and the Swedish band **Pouppé Fabrikk** had switched to Crossover, a type of music that mixes EBM and different types of metal, often in the style of the trash-metal pioneers **Metallica**.

Ambient

In 1978, the former Roxy Music keyboard player **Brian Eno** released a record named *Music for Airports*, using his own record company called Ambient. Ambient is originally an esoteric form of artistic music. The underlying idea is to produce a complete environment rather than just a musical "sound carpet" with rhythms and ordered notes. Naturally, it is advantageous to create a sound image from an unfamiliar and exciting environment if one is interested in making quality, penetrating ambient music. A simple method for creating ambient music is to just set up a couple of microphones in a steel mill, a suburban apartment, or whatever environment you want to incorporate.

Eno supposedly got the idea for making such music after being hospitalized following a car accident. He was confined to the bed with the stereo on, unable to get up to

either turn it off or turn up the volume. The silent whisper of music combined with the sounds from the street below made him realize that this was actually a real music style. Peripheral music - like the music we listen to in supermarkets or airports - contains its own logic and does not at all resemble "regular" music. Ambient music is music that should be listened to while doing something else, concentrating on other sounds, yet it should be subconsciously enjoyable. In psychology, the phenomenon is classified as subliminal perception. The music creates a totality together with external sounds and does not place requirements on the listener's attention.

Eno didn't actually "invent" ambient music. The eccentric and ingenious composer Erik Satie made a few less-appreciated attempts at creating "furniture music" in the early 1900s, and in the 60's, the musical artist **John Cage** wrote *Four Minutes, Thirty-three Seconds*, a piece for silent piano, which is considered by many to be the ultimate ambient composition. The point was that the listener should concentrate on the sounds in his or her environment. To get the most out of the piece, one should perhaps read the score. Cage also worked with electronic music, where he introduced ideas from Zen philosophy about how the music should be organized but still display a chaotic nature. These ideas have, served as a basis for the study of improvisational techniques. They have also had a great influence on ambient music, and this is mentioned on the covers of Brian Eno's records.

Together with installation art, this music form says a great deal about ambitions within modern art: to create a total environment and place the beholder inside it[1]. The concept of Virtual Reality is considered to be the optimal combination of installation art and ambient music. An artificial, man-made environment of the type that writers for ages have been able to create using the reader's imagination - but tangible, detailed, and accurate. A world built on pure information.

Electronic music pioneers such as **Tangerine Dream** (which debuted with *Electronic Meditation* in 1969), and some symphonic rock groups like **Hawkwind**, experimented early on with creating alien, futuristic sound environments using early synthesizers and manipulating all types of electronic equipment (for example, guitar amplifiers) to produce strange sounds.

Brian Eno is still a prominent figure in ambient music. Before ambient music became well-known, it was often filed under labels such as New Age or Meditational. These terms are nowadays used for artists like Jean-Michel Jarre and Vangelis, who represent a sort of mood-charged elevator-style music, suitable for active as well as passive listening.

Modern DJ's such as **Alex Paterson** and **Bill Drummond** (The Orb/KLF) and **Sven Väth**, inspired by techno and industrial music, have succeeded in the art of making rhythmical pop music with elements of ambient music without ruining the basic concept. Especially The Orb's Adventures Beyond the Ultraworld and Väth's Accident in Paradise are considered important milestones in "modern" ambient

Electronic Film

The last subject I will touch upon in this chapter is not about music. Electronic film has existed basically since the introduction of the TV, but never developed into a genre of its own until the late 80's. We can compare electronic film to electronic

music, and define it as film that is created only by electronic means. The first time anything of the kind was done was when a TV camera was aimed at a TV screen, and thus created a flowing feedback pattern. That type of effect has also been used in music, to spiff up a melody and add new dimensions; there's hardly a guitarist that does not know how to employ feedback in an electronic amplifier to create new sounds. For music, this form of manipulation came about as early as the mid-50's through Stockhausen. For TV and film, it was never a matter of making electronic film its own art form. Instead, technology was mostly used to create special effects. A shining example is the vignette for the English TV series *Doctor Who*, an illusion of a trip through a long, colorful tunnel, created solely with the help of feedback patterns.

The art of filmmaking has developed in many directions, but electronic film in particular seems to repel many filmmakers. In film, there is no tradition of creating pictures without people. Since its inception, film has been based on theater, and thus on dialogue. The mere thought of making a film without people is absurd to most directors (*Translator's note:* and then *Star Wars: The Phantom Menace* came along...). In music there is, to say the least, a much older tradition of making music without song. One could say that music, as opposed to theater and film, has more to do with directly generating emotions and moods than trying to reflect real events or psychological occurrences.

In animated pictures, there have been several attempts to take a step away from people and trying to create a symbolic universe. Mostly, however, it has only led to compromise. Virtually all animated films are fables, i. e. they describe things that actually occur in human society. Basically all events that are described in cartoons involve actors with certain human physical and psychological attributes that have been put in some human-like situation. The few attempts at creating animated film like modern art, through the use of symbols and patterns without "life", have almost exclusively produced incomprehensible results.

Also relevant is the fact that film, up until the 90's, was extremely expensive to produce and did not lend itself to frivolous experimentation. It was necessary to have an established market potential or government financing to afford to make a movie. Neither of these institutions is very receptive to experimental ideas. With the introduction of cheap video technology in the late 80's and early 90's, it became possible to experiment with film in an entirely new way.

The computer has also made an appearance in electronic film. Here, as in music, it is the general opinion that the computer should remain merely a tool, a means of creating completely normal commercial or artistic film. Among those involved with animation and computer graphics, ideas are radically different. One of the most distinct and beautiful examples of electronic film is a series of short movies created by George Lucas' *PIXAR*, a company that was founded by the film mogul for the sole purpose of developing computer technology for motion pictures. It goes under the collective name of *Beyond the Mind's Eye*, and is well appreciated among those who already have been involved with electronic culture. Somewhat paradoxically, in this case it was the commercial film industry that financed the development of one of the most alternative art forms there is. Some of PIXAR's movies are regular movies intended for a wide audience (like cartoons but more detailed), while others are very experimental[2].

I refer to films containing only exploding geometric figures, camera pans over incomprehensible landscapes, fractal images, and psychedelic color patterns as ambient films, since the idea is about the same as with ambient music - to set a mood without a linear or coherent content. The style is related to so-called parametric film, in which the technique, especially camera positioning and panning, is and end in itself to lend the film a certain mood without resorting to traditional narrative methods.

Electronic film is very popular at rave parties, and also a given ingredient in many techno music videos, a music style which will be discussed in the next chapter.

---

1 To "expand the frames" is considered a general characteristic of postmodern art.

2 They've made a commercial breakthrough with the movie Toy Story.

Chapter 7
RAVE, TECHNO AND ACID

During the 80's, something strange occurred in Sweden. The DJ's that had grown up in the seventies (and were intended as replacements for the grossly expensive and uncontrollable live music) suddenly acquired artistic ambitions. Small companies in the form of a mix between record companies and DJ houses started appearing all over the Western world. They produced records containing music for one single purpose - to be played at discos and dance clubs. It should be as rhythmic as possible, and at a rate of about 120 beats per minute - a perfect pace for dancing. **Swemix** and **Nordic Beats** were companies that were typical of Sweden. Among the DJ's who became successes by combining dance and pop music were **Robert Wåtz** and **Rasmus Lindvall**, later known as **Rob n' Raz**, and they were most famous for adapting tracks from the rock group **Electric Boys** to the dance floor. Others preferred to stay less commercial and do *their own thing*.

During the middle and end of the 80's, and in Sweden in particular in 1987-88, the new dance culture emerged. It was careless and carefree dancing for its own sake, nothing well-organized and tidy that you subjected yourself to for social reasons at discos or in physical education classes, but rather wild, uninhibited dancing. It was the resurrection of the rhythmic, ritualistic dance that had for centuries remained repressed and subjugated by the West's religious and ethical values, and it returned in the form of *acid house*. Naturally, established society, with its politicians, musicians, and counselors, was outraged and terrified. And naturally, all the young people with enough brains to be rebellious bought acid house records to freak out their parents (including your author, who bought his first acid record, *House Nation* by **MBO**, in 1987).

Pure *house* was the most successful in the beginning, probably because it was based on funk, soul, and disco music a la George Clinton and James Brown rather than synthetic music. The synthetic parts were limited to some bass line, generated by a drum machine or stolen outright from some Kraftwerk record. The style was created in Chicago, and supposedly derived its name from the fact that dance parties were often held in warehouses (one of the first European house music clubs was thereafter named **Warehouse**, and was located in Köln, West Germany). Together with the contemporary Detroit-based *techno* genre (which was purely electronic), this new dance music came to be called *acid house*. Early house bands include **The Royal House**, the previously named **MBO**, and **D-Mob**. When the music gained in popularity, the two styles became mixed together, particularly in Europe where it was simply called *acid*, and no one really knew what music belonged to what style. The first really influential European house clubs appeared around Manchester, England.

Acid house was a special form of dance music which used *samples* (fragments of sounds) in specific ways. It was inspired by the cacophony of machine sounds employed by industrial music (as with **Throbbing Gristle** or **Einstürzende Neubauten**), William S. Burroughs' style of building larger texts from small text fragments (read more about him in the next chapter), and from the art of collage and mosaic. The acid musicians constructed a mosaic of sound phrases, and were almost exclusively DJ's who knew how to emphasize good dance rhythms. You could say

that it was the first instance of *concrete music* (the brainchild of Pierre Schaeffer) reaching a wide audience. Sampling machines were first introduced among musicians engaged in making concrete music.

Musically speaking, acid house developed the already existing electro-pop trend of well-composed riffs, in the form of synthetically generated loops that set the mood and ambience of the song. "Acid" is unfortunately also a slang term for lysergic acid-25 (LSD). Acid house has, however, probably not derived its name from any such association. It has been said that the true originator of the term is the slang expression "burn acid", which was DJ jargon and referred to the sampling sounds from records. There are, of course, others who say that this is just a euphemistic lie, and that the term originated from a few English musicians who visited Detroit around 1986, buying anything with the word "acid" on it in the search for Grateful Dead and other "hippie" recordings, but instead ended up with a slew of strange synthesized music which turned out to be early techno and house. The name for the genre supposedly emerged from this event. Acid house also has a characteristic sound, a little heavier and faster than regular dance music, but milder than the "raw synth" mentioned earlier. Sounds from synthesizers and drum machines such as **Roland 303, 707, 808, and 909** were especially popular (hence, for example, the house group **808 State**).

Acid music gained popularity at the time of the golden age of personal computers. 1987-88-89 are considered the absolutely most intense years of the early history of personal computing culture, which is why many demos, pseudonyms, and group names among the subcultural hackers drew inspiration from acid house. The two cultures rest on the same cultural base of amateurs, and emerged thanks to the increased availability of low-cost computers and consumer electronics during the same period. Also note a vague influence of hacker culture on acid musicians: DJ's with names like **Phuture** or **Phusion** (if you observe the spelling) have obviously been inspired by hackers. Acid house also formed a kind of symbolism for youth rebellion during these years.

There has long existed a total conceptual confusion eith respect to dance music. Acid house grew explosively into a number of sub-categories; every larger city in England and Germany seemed to develop its own house genre, with the same trend taking place in the US. Many quickly tired of the eternal compromises between electronic dance music and the verse-refrain style of rock music, or rap (which was mandatory within hip-hop), and reverted to the original and purely electronic dance music: *techno*.

Techno

Techno sought to return to the roots of electronic pop music - the sounds and harmonies used in regular dance music had grown tiresome, and acid house had started sounding the same across the board. Acid was no longer breaking new ground, and it was time for something new. DJ's who were now full-fledged electronic musicians sat through their nights listening to **Kraftwerk, Ultravox, D.A.F.** (**Deutsche-Amerikanische Freundschaft**) and other early synth bands that had contributed to music culture, in an attempt to find the good stuff that had been left behind and at the same time try to create something new. And they succeeded, especially by using early synthesizers such as **Prophet**, **Fairlight**, and **Roland**

brands. The reason for this return to yesterday's technology was supposedly that they couldn't really afford anything else.

Techno was, as noted earlier, born in Detroit. The origin of the entire genre can be traced to three DJ's named **Magic** (Juan Atkins), **Reese** (Kevin Saunderon), and **Mayday** (Derrik May). They claim to have been inspired especially by Kraftwerk and **Parliament** (George Clinton). Mayday toured England in 1987 and provided inspiration for the underground acid scene through his compositions. Most likely, this legendary DJ has lent his name to the enormous *Mayday* rave, which is held annually in Germany and has reached astronomical proportions.

Frankfurt had early on become inspired by Detroit techno and created its own version, *eurotechno*, by trashing their Japanese synthesizers and hunting down old relics from the seventies. **SNAP** invented the winning combination of a black rapper and a female vocalist, and **LA Style** made a loud and provocative song called *James Brown is Dead*, to signify the end of techno's affair with funk and R&B. Groups like **2 Unlimited, Pandora, Captain Hollywood Project,** and **Culture Beat** fall under the collective term *eurodance* (in the US, this genre is called *techno/rave*).

These and other early eurotechno bands brought something new that many had long been waiting for. They abandoned the 120 bpm that had been the mark of beauty for acid house, and pushed the pace of their songs to a level that most closely resembled energetic punk. The tempo increased on dance floors around the world at the same time that MTV grew really large and further expanded the production of popular culture. We ended up with a new, wearied youth generation which was called *Generation X*, who walked out of movie theaters if nothing had happened by the first ten minutes of the film.
At the same time, the indefinable **KLF** (Kopyright Liberation Front) appeared from nowhere and toured the hit lists with only one album and an incredible amount of singles, only to later withdraw from the scene and, in their own words, "never again make music". The group consisted of **Bill Drummond**, the disillusioned former manager of (among others) *Echo and the Bunnymen*, and **Jimmy Cauty**, a former member of *Killing Joke.* They introduced a totally new element to popular music by combining the instrumentation and dance-oriented tempo of dance music with classical rock formulations. The result was music palatable to synth, techno and rock fans.

KLF were very aware of what they were doing. In the early stages of their career, they wrote a book titled *The Manual*, and promised a full refund to anyone who could not make it to England's hit list with the help of the book. Before they became KLF they called themselves **The Timelords** and **The Justified Ancients of Mu Mu** (a name which together with much of KLF's image is taken from the cult book *Illuminatus*!). In reality, you should probably consider KLF's commercial career as an example of modern art making a protest against the pop industry. At the end of their career, they actually hated this self-perpetuating machine that churned out the same garbage over and over again. Throughout their career, the group was characterized by a total lack of respect for money and established pop music, as well as a generally cynical view of life. The leader, Drummond, was highly inspired by Zen Buddhism, and provoked those who posed questions about the band by accusing them of being under the influence of the four mistresses of Lucifer: *Why, What, Where,* and *When,* which are

questions that according to Zen cannot be answered by words. Early on, Drummond worked with Alex Paterson on *The Orb*, and the two together could be said to have invented the genre of *ambient techno*.

KLF also clearly shows the connection between attitudes in the underground dance culture and among hackers. As many other DJ's, they sampled extensively from other artists, and more or less held the opinion that music should not be patented. On one occasion they sampled ABBA and wrote (somewhat provocatively) on the back of the album that "*KLF hereby declares all material on this record free of copyright*", which eventually resulted in the entire issue being burned on a field somewhere in central Sweden. This took place after KLF failed to convince ABBA to withdraw their threat of legal action that they received from ABBA's Swedish representatives. On another occasion, Drummond began to "liberate" the group's equipment during a gig at a London club, which forced the club owners to intervene to stop the guests from taking the machines home with them.

In England, there is a whole array of strange musicians in addition to KLF: among others, the ambient music revolutionaries **Black Dog Productions** and an idiosyncratic group named **The Prodigy**, who invented their own style of music called *breakbeat*. These groups, like KLF, appeared in the late 80's in synch with various independent bands such as *Pop Will Eat Itself*. The explosive development of the music business in England was due to the very pop industry that KLF specifically protested.

A considerable proportion of people in England go to "in" clubs and listen to the latest music before it is released, and the top hits list is a creation based on lobbying, without any connection to reality whatsoever. In actuality, England's Top 40 is simply an institution of power that the pop industry employs to tell the public what they should buy. Since entries on the list go up and down at a violent rate, new music and new artists must be generated constantly (*translator's note*: At the time of this translation, a clear-cut example would be *The Spice Girls*). In this frenzy, hundreds of artists get their chance to show what they can do, for better or for worse. Originality is much more interesting than technical skill. In this manner, the pop industry sought out acid house music from the small suburban clubs, and the improbable event that this narrow genre made the hits list actually occurred. This phenomenon has turned England into the "engine" behind European popular music.

In Germany, Sven Väth and a myriad of other DJ's produced a mix of techno and ambient clearly influenced by the eighties' acid house: *trance*, which in England was combined with influences from the Indian vacation paradise Goa and labeled *goa-techno*. Some half-crazed Dutch guys who called themselves **Rotterdam Termination Source** made a piece of music using only drums and sound effects: *Poing*. In this manner they created a genre called hardcore techno, which has developed into a hybrid of techno and death metal, often using a tempo of 300-400 bpm. This hybrid has gotten some former metalheads into techno.

Electronic pop music is never static: there's always something new, and there's constant experimentation in small studios around the world. Crossover techno, in which techno is mixed with other music genres, springs up everywhere. It is often very commercial, with perhaps the exception of the hyper-experimental **The Grid**,

who have for the first time in their career made a commercial success with *Swamp Thing* - a mix of techno and banjo pieces. *Jungle* is a genre which is both a predecessor to and a continuation of The Prodigy's breakbeat-techno - a mix of techno, rag and dub music which seems very promising and which is also not particularly commercialized. The most hardcore is *gabber*, which is a corrupted version of hardcore techno. God knows what's going to be invented next: *gospel techno*, perhaps?

Other musicians, such as Future Sound of London, Black Dog Productions and the Swedish **Lucky People Center**, have approached electronic music and make up a genre known as progressive house, i. e. house music which is going somewhere, and is always under development. These people want to escape the concept of genres by breaking all norms. Thanklessly, genre-breaking becomes a genre in itself; there is a similar phenomenon within jazz.

As soon as a genre becomes commercial, as when techno became eurodance through U96, the smaller clubs tend to invent some new variant and sneak back into the underground. Examples of this include Jungle, Goa-techno and Gabber. Jungle is, at the time of this writing, on its way out of the underground, and new styles are most certainly being created as we speak in some studio in Germany, England, Holland or Belgium. You can hold whatever opinion you want on this; in practice, the entire underground club culture is simply a concept factory for the pop industry. They find something new, polish it and water it down a bit, and then release it for a mass audience. If you believe in infinite artistic integrity and creative art, it's probably a horrible thing to witness. On the other hand, maybe we should be thankful that we're not listening to the same chewing-gum pop music of twenty years ago.

Clubs and Raves

Techno is mostly played in small private clubs, even though it is today *possible* to sell techno albums to people who are not DJ's. As a cultural manifestation, techno has strong ties to the dance floor, and the two could be said to constitute a unified whole.

Dance music has changed the music market. In the old days, you listened to the radio and checked out your friends' preferences, bought the records and listened to them at home. Nowadays, you go to a dance club or even a rave, and become influenced by the music you hear there - the type of music that's made for dancing. Later, you might by an album or two. Eurodance mix albums are especially strong sellers.

Techno is not designed for "easy listening" at home, and it can have a stressful effect if it is used as background music. In England, where the public traditionally is very open to new forms of music, heavy and uncompromising techno music has made a commercial breakthrough; likewise in Germany, which with its tradition of electronic music *a la* Kraftwerk welcomes any new innovations in that realm. Even in Southern Europe, really heavy techno tracks are played on pop radio.[(1)]

Raves are still very underground events in Sweden and Scandinavia, even if its interest base has grown explosively since 1988. Today, there are *thousands* of happy ravers in Sweden, who are often willing to travel far to attend a good rave. In Germany and Great Britain, raves are already accepted cultural events, which in some cases attract up to150,000 people, such as the well-known *Mayday* rave in Germany

(which is sometimes described as the Woodstock of our time). Special raves are also arranged for different genres. Raves in Scandinavia are usually not announced in the daily press; the information is spread through the grapevine and through flyers that are available given the right contacts.

A type of rave that receives a lot of attention is the so-called *bryt-rave* (English: *break-rave*), which entails breaking into a warehouse, setting up a sound stage and starting to dance. It is reminiscent of a sort of house occupation, and if the number of attendees is large, the police stands powerless. This type of rave has been somewhat frequent in Hammarbyhamnen (*Hammarby Harbor*) in Stockholm. One could make a connection to the Prodigy track *break & enter*, in which sounds of glass braking and doors being pushed open accompany the music. The sense of revolt and insolence against society is complete.

The rave culture is primarily based on the Trance genre, which can keep a dance floor alive all through the night with its long songs in a perfect dance tempo. A rave is not an event to attend to get drunk or pick up someone. A rave is a place for dancing, listening to music, meeting and looking at other people. Whoever attends a rave with different intentions will invariably be disappointed.

Rave culture is claiming expansion - even futuristic dress and other methods of creating a homogeneous group identity have started to develop. The rave sites (mostly warehouses) have also started to receive futuristic interiors to give more of a "cyber-feeling" to the environment. The phenomenon has gained a Swedish face through **Mikael Jägerbrand**, editor-in-chief of the relatively new magazine **NU NRG Update** (pronounced "New Energy"), which has a run of about 1000 copies and has a layout that really screams "underground"; the page layout is reminiscent of American tabloid classifieds. It is of course a good move - ravers *love* being underground. Despite its small circulation, the magazine is not sectarian or single-minded, and it shows a certain sense of distance and social awareness.[(2)] There's also a few smaller fanzines, and naturally a few electronic bulletins and magazines.

Clubs, Trends, and Drugs

The (Swedish) debate around dance events such as acid parties and raves is severely inflamed by the narcotics debate. The underground dance culture is under no circumstances endorsing or approving of drug use. Unfortunately, sometimes people attending dance events can be total spacebrains[(3)] . The main purpose of dance parties was and remains dancing and music. Originally, acid parties were completely drug-free events.

As early as the late 80's, the discos on Ibiza (a Spanish island resort) hooked on to the acid house trend and created their own version, *balearic beat*, a mix between house, flamenco (!), and a few other styles mostly associated with the artist **Paul Oakenfold**. Ibiza is primarily visited by rich people, mostly from England, and it has drugs in abundance.

The reason for the popular connection between drugs and acid house/rave is thus that those who enjoyed partying all night before the introduction of the acid parties, brought their strange fashionable drugs when they went to visit one. Especially the "designer drug" Ecstasy, a mix between amphetamines and LSD, has figured heavily in the media. Ecstasy is originally a "yuppie-drug", which has become a sort of

exclusive marijuana for the rich. In the beginning it was sold as a diet drug. The greatest culpability for the narcotic stamp on rave and acid culture falls on English upper-class youths. The drugs ruined the reputation of all the intense house-clubs around Manchester, and the stigma remains.

Nonetheless, Ecstasy, amphetamines, and cocaine are present at some rave-like events. As expected, it seems to occur more at purely commercial dances, to which the "in" crowd that want to stay abreast of the new culture is drawn. Enthusiasts at small techno clubs are mostly of the opinion that Ecstasy is a nuisance which ruins the reputation of techno culture. Unfortunately, since everything that is prohibited is also "rebellious", drugs have spread to several acid and techno clubs, including Swedish ones. The clueless middle-class rebel thinks, as usual, that you're a *real* rebel only when you do drugs. Independent thought is never popular among conformist groups. In short: ravers with brains stay away from drugs, and those who don't know anything naturally think drugs are really cool (no, it's true - people *never* learn).

Large clubs are frequent in major cities. They are kitschy, well decorated, with mean bouncers and a fairly long line regardless of whether it's full or not (to create demand, of course). They are not about supporting some subculture, even though many DJ's from the underground scene get a chance to make some money in these clubs. Drugs are consumed in the bathrooms.[(4)]

The terror in homes around the country is complete. The poor parents of these young people remember with horror those few years at the end of the 60's, when they themselves were swept up by the wind from San Francisco, smoked marijuana and hasch, and tried LSD. Not many are willing to admit to that today, but their fear of their kids doing the same thing today is genuine. The main theme then was protesting the Vietnam War and society, and the main theme today is dancing and having fun. Ravers don't need politics as an excuse to meet and enjoy themselves. Drugs are tangential, and not at all as prevalent as media would have it appear. Fear and misunderstanding often inflates the problem to bizarre proportions.

One thing that ravers do enjoy are so-called *smart drinks* - energy drinks that help rave dancers keep dancing a long, long time. Mostly it is a matter of substances that can be found in any pharmacy or herbal medicine store, but with different labels. There is no reason to suppose that this should be harmful - middle-aged Swedes have consumed the pills for decades without suffering harm. What is worse is the tendency to mix prescription drugs with the drinks, which is something that cyperpunks in particular do sometimes (more on this in the next chapter). Most of the "emergencies" reported about drugs on rave parties is due to journalists attending some event and seeing these sugar pills and sodas on the bar, frequently wrapped in some pastel-colored paper or foil, which naturally appear very ominous. If you interview young people who have been to a rave, they most likely will say yes to having taken Ecstasy, even if they've actually consumed a bunch of St. John's Wort. It happens, sometimes.

Some member of the debate has tried to submit the fact that the dancing itself is harmful. The statement that the capacity of ecstatic dance - which is imprinted in our genes since thousands of years - fails by virtue of its own stupidity. Such a statement is thus rather an expression of conservative cultural values or even xenophobia, which seems to be a characteristic of many "opiners". Obviously, the people that do not

attend regular dance clubs and listen to Stairway to Heaven for the 18803rd time, while drinking themselves silly, and are not there just to try to get laid, must be *suspect*… cluelessness, in short.

Even in Sweden, frightened cops have broken up rave parties for no reason whatsoever in their total ignorance of how underground culture works. Some police raids against rave dances most closely resemble ethnic discrimination - of the same kind practiced by customs agents and retail security officers who target people of different pigmentation or dress. Some cops are apparently susceptible to excessive stereotypical categorization.

The cause of the cultural phenomenon of rave is that the actual dancing at the larger, commercial clubs has become secondary. The organizers are mostly interested in selling as much beer and liquor as possible, and the patrons are more oriented towards boozing and picking up someone than dancing. The inherent value of the dance has been abandoned.

It has occurred to me that it might actually be a good thing that rave suffers from a bad reputation. It prevents people with purely commercial interests from advertising gigantic rave parties, and thereby commercializing the vibrant underground technoculture. Sometimes it even seems that ravers are somewhat amused by having a "bad reputation", for identifying with the underground. In Sweden, this negative image has only had the effect of attracting more young people to the parties.

Music and Music Culture

In reference to electronic music, it generally seems as if every new generation of innovative musicians is scorned by the previous one: classical electronic musicians look with distaste on electronic pop music, synth pop fans despise heavy synth and techno musicians, techno musicians dislike hardcore techno musicians etc. etc. It might be redundant to mention that classical and rock musicians scorn all forms of electronic music.

This is probably a necessary state of affairs. It is the distancing from older norms that creates a new subcultural group within an accepted domain, and this is how culture grows and develops. The argument is applicable to literature, film, theater - in short, all types of art. Techno music and techno culture is, especially due to the influence of television, inextricably associated with the art of video and computing. That techno is inseparable from dance has already been illustrated. This development of popular culture has resulted in many artists that are more like some form of product than people. The music is created in a studio, performed by a group of photo models, etc. Popular music becomes more than music - it becomes part of a culture. You don't buy just a record, you buy a lifestyle. Fashion, dance, film - everything is included. It could be summarized and called "art". Popular art.

Art grows and develops when individuals, with a desire to create something new where not everything has been tried, go against the norms and create something new. Mostly the individuals are young, such as Sex Pistols, Grateful Dead, Bob Dylan or Jack Kerouac (well, they were young when they started). Sometimes it is some eccentric artistic soul like Marcel Proust, James Joyce, or Frank Zappa. When a young artist breaks out of the norms there arises, given the right circumstances, a new

subculture, which under even more conducive circumstances creates a new spirit of a generation.

The smaller the Earth becomes, and the farther our mass media reach, the more subcultures develop, generations change faster, and society changes faster. This is a characteristic of the post-industrial society which I will later explore further. Let it be stated that the breaking of norms and creation of new ones is very important for these new styles of music. It also has a considerable importance for the more central points of this book.

We will now see how the pulsing rhythm in culture generated an entirely new literary genre, a new view of society, and - soon - a new ideology.

---

1. In Sweden, as of late 1996 no such breakthrough has taken place. Perhaps the Swedish public is simply too conservative. However, things are slowly moving forward. Kalle Dernulf, of P3 (part of Swedish national public radio), is probably the one who has dedicated himself the most to spreading Swedish and foreign techno in the ether.

2. Jägerbrand and the Swedish Rave Organization (SRO) are at the time of this writing organizing a "raverixdag" (English (loosely translated): *Rave Congress*) to coordinate Swedish rave organizers. Someone remarked sarcastically that "they seem to have to make *everything* political", but in light of the Nacka Police Department's dubious raids against Docklands (a rave site) during the Spring of 1996, the need for an organized resistance group is understandable.

3. Some have made the observation that it shouldn't be a great experience to attend a rave on a "downer" drug, such as hasch. I have personally observed that it appears fairly abundundantly at raves; why, I do not understand. Possibly it may be due to the hasch (THC) having a mildly psychedelic effect. In this context, I'd like to take the opportunity to mention that I'm personally neither for nor against drugs *per se*, which you might conclude from the strong formulation above. What I am against is the tendency to blame drug use on culture. On drugs in general I don't have a clear and expressed opinion, rather I reserve the privilege of ignoring that debate, which is sure to piss somebody off.

4. If someone interprets this to mean that I think that these "beer cafés" are the pathetic hangouts of the "in" crowd, that someone has interpreted me correctly.

Chapter 8
CYBERPUNK

Cyberpunk is originally a literature- and film-oriented movement. We will begin with literature.

There are different science fiction genres (abbreviated: **sci-fi**), and the definitions are somewhat arbitrary. Sci-fi bibliographies often range across such wide areas as *fantasy* and *horror* , but this book is not about science fiction literature in general. I will therefore proceed to the part of sci-fi that is called cyberpunk.

The definition of cyberpunk is usually that it is a book that resembles something written by **William Gibson** ; a type of futuristic account of society where advanced computer, nano-, and biotechnology as well as artificial intelligence is part of the ordinary. The world is rigidly segregated by a small, ruling elite of multinational corporations and a large, brutal mass of regular people. Governments have yielded to large conglomerates and mafias, which control the world. The action generally takes place in enormous metropolitan areas of a ghetto-like character. Drugs of all kinds are widely available, the pace is fast, and personal and environmental descriptions are superficial and often (in the case of Gibson) chock-full of trademarks and digital jargon. A typical cyberpunk story is set around the year 2020.

Cyberpunk is usually referred to as *dystopian* , as it describes something close to the opposite of a *utopia* . Most early science fiction novels were utopian, where disease was a thing of times past, a unified political system had replaced constant conflict, and the action usually centered around a group of scientists on a mission across the universe, or on space heroes such as *Flash Gordon* . The TV series *Star Trek* is a definitive utopia. It is not the case that a utopia has no problems; it is simply that "the good guys" are always win and never morally questionable. All utopian chronicles are optimistic visions of the society of the future.

In a dystopia, many problems remain in the world, the natural environment is almost completely ruined, and politics is (as usual) chaotic. The books are therefore much more plausible than classical sci-fi works, and has acquired a wide readership among people who normally do not read sci-fi. Earlier, some were of the opinion that it was unnecessary to descrabe realities that were *worse* than the one on Earth. Some dystopian authors, like Stephen King, therefore abandoned science fiction in favor of writing horror literature. Dystopias are, however, more auitable for social criticism than utopian works. Since many dystopias are satirical or comedic, cyberpunk constitutes a sharp contrast through its cold realism. Other notable dystopias are Karin **Boyes'** *Kallocain* and **George Orwell's** *1984* .

Just like most US science fiction, cyberpunk has its roots in so-called pulp fiction. Pulp is a rough cellulose material used to make paper, and pulp fiction derives its name from the rough, porous quality of the paper it was printed on. Since the film industry was still at an embryonic stage, people read much more books and magazines, and pulp was the "crude", cheap literature. Comics and TV series such as Flash Gordon are also called pulp, since they were inspired by stories and illustrations from these magazines. Pulp seems silly and incredibly far-fetched to the normal

Swedish reader, but for sci-fi lovers across the world, pulp is the origin and source of all modern science fiction, and the cause of its own subculture.

B**ruce Sterling** , Gibson, and a few other sci-fi authors had their own pulp magazine called *Cheap Truth* . Although it wasn't produced in the 50's, it was run in and with the same spirit as the best early pulp magazines. They thought that no really good sci-fi was being written. They encouraged people to get their own word processors and write *good, vivid, and readable* science fiction. Not seldom did they come down on best-selling authors in the genre. An interesting detail about Cheap Truth was that it wasn't copyrighted, and that copying and distribution was encouraged.

Cyberpunk is a little more than this, but the literary genre is basically synonymous with a small group of American authors, of which William Gibson and Bruce Sterling were the most famous. A few 2000 AD comics, especially *Judge Dredd* , are also considered cyberpunk, since their world is somewhat similar to Gibson's dystopias. The term cyberpunk was supposedly coined by a gentleman named **Gardner Dozois** in a review of Gibson's first book, *Neuromancer* . Dozois is said to have, in turn, gotten that label from a short story by **Bruce Bethke** , which had been submitted for his review. [(1)]

The message of the cyberpunk novel is one of warning - the stories are nightmarish visions of a future society that we risk becoming subjects of, unless we take precautions. The word *cyberpunk* is derived from *cybernetics* = humans or society in the interaction with machines (from the greek *kybeternetes* = first mate or pilot), and *punk* = virtually lawless individual with a mildly anarchistic social view, cowboy style, living in the underground.

---

1. This resulted in a considerable amount of controversy. Bethke considered it his right to define the term "cyberpunk", since he had invented it. Bethke's definition does not coincide with Dozois's

Chapter 9
AN ELECTRONIC INTEREST GROUP

The story of hackers, phreakers, telephone companies, and justice is told (from an American perspective) in Bruce Sterling's *The Hacker Crackdown* (1992). The reason this science-fiction author decided to write a history of hackers, is exactly what I have tried to illustrate with my arguments so far: that aspects of electronic cultures overlap. The whole thing started when the U.S. Secret Service tried to clip the wings off the underground hacker movement, and on some occasions strayed far outside the limits for law enforcement intervention.

They really wanted to *nail* the hackers, who had grown extremely powerful in just a few years, through a national crackdown (hence the title of the book), with the intent of teaching the hackers a lesson. This crackdown was named *Operation Sundevil.* The Secret Service busted into the homes of American teenagers, grabbing everything with wires coming out of it. The computer, the printer, the portable stereo, mom's and dad's computers, all of it. That wasn't enough: they also took *manuals* , or anything remotely resembling one: science-fiction novels and regular compact disc records, for example.

All of you can probably figure out what happens if you take all the hacker's machines away from him or her. He/she becomes totally powerless, with no means of keeping in contact with friends or communicate in open electronic discussions. The hackers not only had their wings clipped; they also had their mouths sewn shut. This is exactly what the Secret Service wanted, and probably no one would have been concerned - not even Bruce Sterling - if they had stayed content to just raid hackers. Many hackers arrested during the crackdown were given sentences that prohibited them from using computers for a certain period of time.

On March 1, 1990, the Secret Service committed a mistake: they went into the gaming company **Steve Jackson Games** , in Austin, TX, and confiscated all the computers that they could find, including one which had a completely new game stored on its hard drive: *GURPS Cyberpunk* (GURPS sands for Generic Universal Role Playing System, developed by Steve Jackson Games to make it easier to switch between roleplaying settings without having to switch gaming systems).

Steve Jackson Games, therefore, make *role-playing games* , and the game GURPS Cyberpunk was written by a hacker going by the pseudonym **Mentor** (his real name was **Lloyd Blankenship**), and who worked as an author at the company. When the company demanded the return of its computer, or at least the files for GURPS Cyberpunk (which was just about to be marketed), their request was denied, with the justification that it was not a game but rather a manual for perpetrating computer crime. Mentor himself was a hacker, and had written an excellent and realistic game which focused on breaking into different computer systems. The game was considered dangerous.

Anyone who's seen a roleplaying game knows that it is a matter of a kind of *books* used as reference material for the games, in which the players try to create and enter a world of the imagination. *GURPS Cyberpunk* , therefore, was a *BOOK* , released by a

publisher, with an ISBN number just like any other book. The fact that the U.S. Secret Service had tried to stop the publication of *a book* , simply because the contents were held to be *too dangerous* , was not well received by conscientious citizens of the U.S. The freedom of the press is constitutional in the U.S. (like in Sweden), and a fantasy-oriented role-playing game like *GURPS Cyberpunk* has the same official right to exist as *The New York Times* , whether it teaches computer crime techniques or not - as long as it doesn't advocate the perpetration of crimes.

After a period of fuss in regards to the Steve Jackson Games case, the **Electronic Frontier Foundation** was formed, led by (among others) the Grateful Dead lyricist **John Perry Barlow** .[(1)] They were financially supported by **Mitch Kapor** , who was one of the creators of the spreadsheet program *Lotus 1-2-3* . The organization had supporters among the users of the electronic conferencing system **The Well** , created by the magazine **The Whole Earth Review** in San Francisco. WELL is short for **Whole Earth 'Lectronic Link** , and in principle functions as a gigantic BBS with connections to the Internet. (You could also view it as a metaphorical "well of knowledge".) Many users of The Well are old hippies and Grateful Dead fans, who dearly value their rights of free speech and assembly. Many are what I call university hackers, engineers, or programmers. The hippie-programmer combination is not unusual at The Well. (I mentioned earlier that the hippie culture originated at the universities in the Bay area. Consider Mitch Kapor, for example - before he started making business software, he was a meditation instructor.)

San Francisco is almost a chapter of its own. It is the Meccha of the electronic world. The universities Berkeley and Stanford are in the area, and close by is Silicon Valley. The majority of modern computer technology comes from San Francisco. It is where the first personal computer, the Altair, was built, and it is also the home of EFF, The Well, Whole Earth Review, Wired, and MONDO 2000. Virtually all forms of popular electronic culture have originated in San Francisco, and it is also where Virtual Reality was first marketed. At the same time, I would say that San Francisco's reputation is a little exaggerated. It has just as much to do with American attitudes and marketing as real knowledge, and the expertise that computer technology rests on has been researched and developed all across the world. However, it is a natural nexus for amateurs as well as the pros of the computer industry. Silicon Valley, in particular, has had great significance, with its thousands of bored upper-middle-class engineers waiting with anticipation for anything to happen on the electronic frontier. These people constitute the innermost core of EFF.

EFF has quality contacts inside the entire American software and hardware industries, and champion *the electronic rights of human beings* . The organization does not protect hackers, as is often said, but it protects the rights of hackers. EFF is therefore a *civil rights organization* . Like the cyberpunks, EFF is ideologically influenced by libertarianism, but on many issues (such as "intellectual property"), they are on a collision course with the libertarians. I will now try to illustrate how threats against civil rights and individual integrity are manifested in the information society.

The Right to Communicate

EFF stated (and states) that it is a violation of integrity to take someone's computer away from them. It is as violating as taking away the right for an individual to use pen and paper. A hacker is used to communicating with the world by computer, through

BBSs, the Internet, etc. Taking the computer from the hacker is akin to taking the typewriter (word processor, pens, or paper) from the author. EFF sued the Secret Service for constitutional violations in connection with the raid on Steve Jackson Games - and they won. The organization now works towards a constitutional amendment protecting electronic expression.

In short: a computer criminal should not be prevented from using computers (everyone uses them nowadays), but from committing more computer crime. You don't prevent a counterfeiter from working at the mint - you teach him to stop printing fake currency. Properly used, the illegal hacker's knowledge is useful to society.

Integrity
EFF has grown since its inception, and currently sponsors a public debate about computers and humans in a future information society. It wants to protect the right of the individual not to be registered and controlled by authorities, simply because it is now possible thanks to the advent of the computer. The organization therefore advocates the use of the encryption program PGP, which I discussed earlier. Why? Well, SÄPO (the Swedish National Security Police) - or some other internal intelligence organization - should not be allowed to examine all postal transmissions in Sweden. They should not be able to read all electronic mail, either. *But* , they could (if they so wished) put a fast, efficient computer to the task of searching all electronic mail for certain keywords, in order to quickly trace new political groups. (It is astonishingly simple to construct such a program; I could even do it myself.) Let's say that every piece of electronic mail containing the words "REVOLUTION", "WEAPONS", or "SOCIETY", in any combination, would be copied and sent to an analyst. You would never know.

According to **Philip Zimmerman** (creator of PGP), it is precisely because of this that one should encrypt one's mail so that no third party could read it. Of course, in democratic Sweden, we would prevent internal organizations from doing such horrible things. Nevertheless, there might be good reasons to encrypt one's mail. Why?

First: there are people besides SÄPO and the local revenue office that might want to see if you're writing something inappropriate. Second: do you trust the authorities? If so, why not just send them a copy of your personal communications, so that they can check them and be sure that you're not sitting around conspiring? What do you, a conscientious citizen, have to hide? Why not let the police search your house for illegal weapons? You see where I'm going - encryption protects the privacy of the individual from governmental intrusion.[(2)]

All the chaos surrounding PGP started on April 10, 1991, when the U.S. Congress made a statement about encryption programs. It clearly stated that it expected everyone involved in the manufacture of encryption technology, of any kind, to incorporate back doors so that the government could read the encrypted information if necessary. The message was a frightening one: you may keep secrets - but keep no secrets from the government. Shortly after, Zimmerman's colleague, Kelly Goen, went around San Francisco and distributed PGP do different BBSs using pay phones. (!) He held that Congress was in violation of the Constitution, and performed this act in order to protect American society from totalitarian supervision. recently, the European

Union sent a similar missive to the nations of Europe. (Americans are much more sensitive to these matters than Swedes - which is fortunate, I should say. *Translator's note:* Nevertheless, and ironically perhaps, the privacy rights of individuals in the U.S. are in much worse shape than in the Scandinavian countries - due to *private* record-keeping organizations such as the credit bureaus, which have become a sort of universal information source that sells all the information it has to anyone willing to pay for it).

Encryption, by the way, is not expressly an American thing. Us Swedes have been in the cipher game for at least as long. As early as WWII, we decrypted German communications going through Sweden. In 1984, the "expert" **Ragnar Eriksson** and his friends at SÄPO made an encryption system which, with the approval of the executive branch, they tried to sell together with other security "know-how". Alas, the system was worthless, since SÄPO has never had any encryption experts worth their name, and no one wanted to buy the system.[(3)]

Those who are professionally involved in encryption (thus *not* SÄPO, but the military and the universities) almost always encounter upstarts who think they've invented the world's best encryption system. Common to all these parvenus is that they want to keep their systems secret, as they consider themselves so bright that no other person has ever been on the same track. All the pros release their algorithms (encoding principles) and tell people how the system works; if it is good enough, nobody can break the cipher *even* though they know how it works. Some examples include DES (Data Encryption Standard), and IDEA (International Data Encryption Algorithm) - which is used in PGP. (SÄPO did not want to publish their algorithms...) Neither DES nor IDEA are impossible to crack - it's just that it would take a few million years for today's computers to do so, using current deciphering techniques.

As an illustrative example, I will mention a common beginner's crypto which entails adding a sequence of random numbers to a digitally stored text. It would be very hard to crack if the message was not any longer than the sequence of numbers, but with longer messages this randomness can be removed as easily as static can be filtered out of a radio signal.

Sweden Awakens

Today, Swedish police have already been guilty of questionable activities relating to the freedom of expression. They have confiscated BBSs, used as an exchange medium for private electronic mail, and probably also examined the private mail stored on these. This has been carried out on suspicions that the BBSs were used in the distribution of pirated software. It can be compared to sifting through all the mail in one of the Postal Service's boxes simply on the suspicion that somewhere in this box there is information about a crime. Would you want your mail read simply because it happened to end up in the same box as a letter from, say, a car theft ring? (I don't even know if the police have the right to do such a thing, but I don't like the thought of it.)

"Holy Christ", the police say, *"those who use a BBS are despicable hackers! Thatdoesn't have anything to do with normal people's privacy, does it?"*

It's great that they were hackers, and not *Jews* or *immigrants* , but simply regular, honest hackers, which we all know are terribly criminal. Hundreds of BBS users,

regular Swedes with no criminal records, have had their right to privacy abridged simply because they fall under the fuzzy (to say the least) category of *hackers* ? And the police are upset because they have found encrypted material in these BBSs, which is hard or impossible to read. I *really* feel sorry for them.

Consider that today's BBSs will, in the future, be replaced by the Internet, through which you are expected to send all your mail. What will happen then? Are we going to have cops running around auditing the mail, seizing large quantities of mail when they suspect something illegal might be lurking inside the pile? But, but... the police follow the law, and according to the law, electronic documents or communications are not covered by the freedom of the press. Hopefully, they are protected under the freedom of speech, but not even this is certain. Everything is very fuzzy, and no one seems to know what the facts are. Legislation is in progress.

Considering all the threats against integrity, the observant citizen naturally wants protection against surveillance, and therefore acquires an encryption program. American intelligence agencies want you to use their "Clipper Chip" instead of your own crypto. The "Clipper Chip" is a very good encryption program which, according to themselves, only the Secret Service has a back door to. The European governments have something similar in the works, which has at the time of this writing not been formalized.

Another use for encryption (besides making your mail unreadable) is to put a *seal* on your messages - a kind of electronic check digit, which can mathematically prove that the sender is who he/she claims to be, *and* that the content has not been changed. This way, electronic bulletins can be mass-distributed without having to worry about somebody "cutting" them, at least not without being noticed. This method is used by, among others, SWIFT, which is an international bank transaction system.

Those interested in the underlying technology of encryption should pick up a book on the subject. American cryptographers (like Zimmerman) are monitored by military intelligence agencies. (I don't know if this is the case for Swedish crypto-scientists.) In some countries, e. g. France, all encryption by private individuals is prohibited.

Swedish Rights

What about civil rights in Sweden and the rest of Europe? Is an organization like EFF necessary on this side of the Atlantic as well> Maybe - especially since European police agencies learn about computer crime fighting by peeking at the USA. In Sweden, police have also confiscated computers and disks, but also magazines, T-shirts, and printers, in American fashion. The police in the U.S. didn't know what to do with all the stuff they seized - and the Swedish police doesn't know either. It's not a mystery why it takes a virtual *eternity* to sort out hacker crimes, considering the amount of junk that the investigators collect as evidence. When I did an inventory of my own collection of about 200 disks, it took me over a month, and I only made superficial notes of the contents of each file. A criminal investigator has to be *a great deal* more thorough for his evidence to stand up in court, and a well-organized hacker can, in worse cases, have *thousands* of disks.

The time span and delays for the prosecution of a hacker is worse than those for refugees, with the difference that these cases are eventually dismissed. To the extent

that the hackers ever see their equipment again, it is most often outdated and without value. The police are still holding computers seized six years ago. In many cases, the hackers' computers are considered instruments of crime rather than communication channels. Even Swedish hackers' rights of free expression have been infringed during police raids - whether they have been criminals or not. Remember where **Cervantes** spent his time while writing *Don Quixote* . (In prison.) Should the pen and paper have been wrested from him simply because he was a criminal? In at least one case, the Swedish police has been charged with violating rights of free speech and freedom of information.

As early as 1984, Sweden's National Police Board determined that seizure of equipment could cause problems, and that this should only be done in exceptional cases. Today, it's more of the rule than the exception. If they had been able to follow their own directives, which said to copy the information and lend it to the victim, the situation would have been much more pleasant for both parties. In that case, the hackers would not have had to have their computers stored in police warehouses for decades.

We also have a law of criminal forfeiture, which means that equipment used in the commission of a crime can be considered forfeited, and subject to sale or destruction. This might be reasonable in the case of specialized equipment like lock picks, "blue boxes", or other directly criminal equipment, but *computers* ? If a typewriter is used for criminal purposes, it is thus forfeited? Can we have just an ounce of freedom of speech, too?

The information age has now caused some prosecutions against the distribution of specific, protected information to become completely unmanageable. Are you struck by the same thought as I? That this plays into the hands of the cyberpunks? If information really *can* be owned - can we in that case uphold its copyright in a rational manner? Or is our old society in about to change with regards to copyright? Relax, there is a cure for all this. *Computers* are very good at controlling large amounts of information, and quickly at that. The organization **BSA** (**Business Software Alliance** , an association of companies in the software industry) is apparently prepared to have a program called *Search II* stand witness in cases against companies suspected of piracy. The program works by reading the contents of a computer's hard drive and registering which programs are installed. The reason for doing this as opposed to seizing equipment, is that corporations, as opposed to hackers, raise one *hell* of a racket if you take all their computers. So far, so good.

When companies and (sometimes) people are charged with piracy, the police rely on BSA and the Search II program for technical expertise. It is a bit strange that BSA, which represents the plaintiff, is also relied on to collect evidence. Strange, to say the least. Now, allow me to insert a small provocation, which might help you think along new lines:

Q: Do we want computers to witness against corporations and individuals?

Q: Why not leave the entire justice system to computers? Automated, powerful, cost-effective - comes in all colors - no difficult interrogations or delayed trials...

Personally, I don't think we should let computers stand witness until they're at least as intelligent as humans. But if a human can testify under oath as to the credibility of what the computer says, then OK. We have for many years allowed objects to act as witnessed, or *evidence* , as we call it. All evidence, however, has to be interpreted by one or more people before it becomes practically meaningful. What is relevant is that computers are evidence which has a hitherto unlimited potential for lying, since they can be manipulated in any way by anyone. I think we should stay clear of electronic justice for a long time - the risk of judicial corruption is obvious.

The question of computers keeping tabs on individuals is a little more sinister than it appears at first glance - information technology, if properly applied, can be used to prevent or *totally eliminate* certain types of crime. Do we really want this? Do we want an intelligent breathalyzer in our car, which tells us when we can't drive? Perhaps such supervision of driving habits will be legislated in the future. Do we want the recipient of a phone call to always be able to know who we are?

For example, there is a program called *Net Nanny*, which is a "baby-sitter" for the Internet. It can be set to supervise children communicating over the Internet, and will automatically shut down the connection if some "dirty old man" starts asking for a name or a phone number. Even if the purpose seems noble, one could ask what would happen if an extraordinarily benevolent government should apply such filters to all of its citizens' communications. I mean, why not pull the plug as soon as someone starts talking about certain kinds of explosives, or starts using to many violent words - just in case... (Note: irony.)

As opposed to a cop, the computer is *everywhere* , and basically free. Should we let our possibility to choose between obeying or ignoring the law be eliminated by computers? Should they become our collective, electronic conscience, and give us an electronically monitored utopia in which there is no crime, since no crimes *can* be committed? It is not as simple a question as you could think, if you consider it for a while... the EFF, and other organizations, are of the opinion that it is *inhuman* to take away the individual's right to disobey. So far, all social control has been based on self-control, a condition which is threatened by automation. There is a risk of principles being upheld for the sole reason that the computers have been programmed to uphold them. This is one of the things that **Paul Verhouen** 's cyberpunk film *Robocop* is about - mechanical beings who with never-ending efficiency chastise the citizen into obedience.

B = Bob
C = The Car

B : Hi Car.
C : Hi Bob!
B (*jumping into the driver's seat*): Let's go...
C : Just a moment, Bob, your voice is a little off... you haven't been drinking anything, have you?
B : Oh no, of course not...
C : You'd better blow before I'll let you drive anywhere.
B : Is that really necessary?
C : Yes.

B : OK then... *(brings out a plastic bag with a nozzle, and squeezes air from it into the mouthpiece on the dash)*

C : Come on, Bob, I wasn't born yesterday. That wasn't your breath. Would you like me to call a cab for you?

B (*stomps away from the car in a huff*)

Freedom of Expression

Well, what about the freedom of expression? Has an electronic book as much of a right to exist as one printed on paper? When the director of datainspektionen (**Translator's note:** *Datainspektionen* is a Swedish governmental institution that regulates the permissible content and organization of computer databases - to my knowledge, no comparable institution exists in the United States) , **Anitha Bondestam** , stated that the somewhat childish text files found on certain BBSs, which describe how to make bombs and weapons, could be *illegal* - did we examine this statement as critically as we would if she had said that *books* describing similar contraptions could be illegal?

For your information, I can reveal that it is *in no way* illegal to write books on bomb construction - provided that you do not encourage the reader to apply this knowledge. (If you're in the military, and happen to write such a manual for internal use, you might even get promoted.) It may be morally questionable, especially considering that the readers are often teenagers, but it is definitely not prohibited. A parallel would be *Hembränningsboken* ("The Moonshine Manual"), which gives detailed instructions on how to make your own hard liquor. This book is not illegal. *Datainspektionen* makes a lot of funny statements which don't seem to have anything to do with their institutional purpose.

Datainspektionen does a lot of really good things. Above all, they protect freedom of information and individual privacy, and the right to know in which databases one is registered. The problem is that the institution sometimes assumes the role of pontificator, which is not its purpose.

From where will a Swedish EFF originate? I would bet on its birth somewhere among people that guard the freedoms of speech and the press. *Föreningen Grävande Journalister* ("The Investigative Journalists' Association"), with **Anders R Olsson** at the lead, has long had an agenda reminiscent of the ideas of EFF. As far as I can understand, this started with a book, written in 1985 by Anders Olsson, called *Spelrum* ("*Playing Field*"). In it, he describes the complicated structure of government, and its desire to control the individual, in a captivating and agitative manner. What William S. Burroughs says through his fictional accounts, Anders Olsson articulates through non-fiction, to put it simply. He doesn't construct his theories based on libertarian ideas about individual freedom, but rather on a description of the *machine*, which he calls *Sweden, Inc.*, as a gigantic, dominating social mechanism built on bureaucracy and the wish to control the individual.

Anders has also advocated that journalists should enlist the help of hackers to enter, and examine, the proprietary computer systems of the government and other organizations. As described in the previous chapter, this took place in the case of the *Ausgebombt* BBS in Vänersborg. In his book *Yttrandefrihet och Tryckfrihet* ("Freedom of Speech and the Press"), he considers it fully justified to hack into

computers owned by corporations, governmental institutions, and other organizations, in order to obtain information of public interest. He emphasizes that it is the *purpose* of the act, not the act in itself, that is most important. In his opinion, the constitutional (Swedish) protection of freedom of information, found in the articles on freedom of speech and the press, protects the hacker while looking for information with the intent of publicizing it.[4]

---

1. Remember the name **John Perry Barlow** - he is one of the greatest visionaries and contemporary philosophers that I have encountered. Like Jean Baudrillard, he belongs to the tiny number of people that have something sensible to say about information society.

2. This concept is normally called simply "privacy".

3. Perhaps they have acquired better "experts" now.

4. Anders has recently published another book about freedom of information: *IT och det Fria Ordet - Myten om Storebror* ("Information Technology and the Free Word - the Myth of Big Brother"), where he shoes that the fear of oversight can be used to conceal more than necessary; he defuses the paranoia surrounding large databases, and shows that it is quite difficult to "know everything about a person" through them. Instead, he points to another danger - giving confidential privilege to information that should be public, by maintaining that it is sensitive. He also defines four useful terms, which I interpret as follows:
Freedom of Speech and of the Press : The right to express one's opinion in the ether or in the media, without risking being silenced or prosecuted.
Privacy : The right to be free from intrusion into individual privacy by government or other institutions of power. (Computer databases, drug testing, etc.)
Freedom of Information : The right to stay informed of the internal structure of governments or other institutions of authority. (For example: the Freedom of Information Act). This right is especially important to journalists.

Chapter 10
COMPUTER CRIME: TERMINAL SLAVES, CREDIT CARD FRAUD, AND CENSORSHIP

What really constitutes a computer crime? Where is the line between harmless exploration of a computer system and real crimes?

In the eyes of the law, computer crime is any type of crime involving a computer in some way. If I hit somebody over the head with a computer, it could theoretically be viewed as a computer crime. A more specific definition would be that computer crime is the act of transferring or damaging information in cyberspace without permission. This definition is accurate in most cases. In Sweden, the authorities mostly concerned with computer crime are: *the Police, the National Security Police (SÄPO), Military Intelligence and Counter-espionage, the Crime Prevention Council (BRÅ), the Department of the Interior, and Datainspektionen* (see the previous chapter for details on this authority).

Additionally, other involved parties include the *security departments of the large corporations,* a few *non-profit organizations* , *informal networks,* and (naturally) *criminal organizations* . It is not surprising that all these people view the problem in totally different ways.

The National Police Board classify computer crimes under the following categories:

1. Computers or software used in the commission of a crime
2. Computers or software subjected to criminal tampering
3. Software that has been illegally copied or modified
4. Illegal entry into, or use of, computers or computer networks

Most computer crimes committed have nothing to do with hackers. Mostly, it involves people at banks, the Postal Service, governmental insurance agencies, or private corporations in charge of billing and payments. Many succumb to temptation after seeing how *easy* it is to transfer money back and forth between accounts, grant themselves financial aid or welfare payments, falsifying invoices, etc. It is really only an "improvement" (exacerbation?) in the old ways of economic crime. An example is a Swedish social worker who gave himself 400,000 Swedish crowns (about $50,000) in welfare payments, and then went to Venezuela to bail out a friend that had been jailed for political activities. He was able to do this because he knew about some weakness in the disbursement system: welfare payments were only reported every fortnight. This is typical of the most extensive form of computer crime. Compared to this type of crime, hacking and phreaking are a drop in the ocean. The worst computer

crimes are perpetrated by people in respectable positions, and are almost *never* exposed. But of course, you already knew this.

The reason that these crimes do not receive as much publicity as the hackers' pranks is that the former relates to a very sensitive relationship: integrity and loyalty within the company or the governmental institution is very important for protection against external threats. It is, however, much more difficult to ensure that one's employees are satisfied and loyal than blaming hackers working from the outside. This principle has been used by entire countries to avoid having to deal with internal problems. By shifting the blame to, for example, Jews, communists, or Muslims, they can create a clear picture of the threat and a target for aggression, while keeping attention away from one's own problems.

The average age of the average computer criminal is between 30 and 40 years. Half of the criminals have worked for more than 10 years within the company. *45% are women* . Hackers? I don't think so. (Source: Nätvärlden #8, 1994, p. 36 [a Swedish computer networking magazine]).

So much for internal computer crime.

A more "hacker-like" crime is defrauding ATMs (cash machines) or credit card companies. During the early period of ATMs in Sweden (1960's), when the withdrawals were still logged on punchcards inside the machines, someone went around and withdrew around 900,000 crowns (about $120,000) over Easter holiday, using fake ATM cards. This is not as easy to do today. Perhaps. Many Swedish hackers have access to the machines used to read and imprint the magnetic strips on the cards. They have also ferreted out *a lot* of knowledge about the nature of the information stored on these strips, mostly of general interest to the system. It is, however, difficult to enter an ATM using a "back door". The banks have developed their own telecommunications network which is inaccessible by regular telephones, and it is through this system that ATM transactions take place.

As for myself, I am constantly fascinated by people's trust in magnetic cards. All cards with a magnetic strip, like ATM or credit cards, are standardized, and can be copied using appropriate equipment. A friend of mine amused himself by withdrawing money using his old credit card. He had simply copied the information from his ATM card to the credit card. I was also not in the least surprised to learn (in April 1995) that some youths in Helsingborg (a city in southern Sweden) had reproduced local public transit cards and sold them at half price. (Courtesy of the hacker named *Wolf* , mentioned in chapter 4). The telephone company's own phone cards are frightfully insecure; this is also true of the cards used for cellular phones and satellite decoders. Often, it is the case of a totally unprotected standard format.

Apropos cards: *Credit cards* are, unfortunately, very popular among hackers. Let us take a look at some statistics from 1989, when there was about six to seven million credit cards in Sweden. In this year, revenues from credit card transactions reached a total of around 20-30 billion crowns (about $300 million), divided into about 50 million transactions averaging about 400 crowns ($50) each. 18,000 fraud cases were reported that year, in which each report would cover about 50 instances of fraudulent use (i. e., somebody used someone else's card about 50 times before it was reported).

The police would rather not investigate any cases involving less than 50,000 crowns ($6,000). I can't even begin to speculate about today's figures. It is, however, unlikely that those 18,000 crimes were committed solely by hackers.

It is often ridiculously simple to call for free or shop using someone else's credit card. Previously, before stricter verification measures, many hackers *"carded"* merchandise from abroad. Especially computer and other electronic equipment, of course. I have already discussed how card numbers are obtained through social engineering, dumpster diving, and other techniques. If a phreaker cleans out your credit card, you will most likely never find out. The credit card companies do not give out this information to their customers. The most common explanation is *"a technical error"*.

With the exception of stealing credit card numbers and their associated codes, hackers do not consider themselves to be in the business of computer crime. A hacker considers computer crime to be one in which computers are used for the purpose of acquiring anything besides information. A criminal using hacker methods is therefore not a hacker, but a computer criminal. Traditional hacking is about curiosity, *not* greed.

Sabotage

Computer sabotage is a rare but venerable form of computer crime. The word *sabotage* is derived from the French word *sabot* , which means "wooden shoe". It originally refers to the time when French textile workers threw wooden shoes into automatic weaving machines, because they were upset that machines had stolen their jobs. An mechanized loom is in many ways similar to a computer, so you could say that sabotage originally was computer sabotage. This type of activity has been around since the English instigator **Ned Ludd** (and his *luddists*) destroyed looms and Spinning Jennys in the mid-18th century.

Swedish anarchists have often threatened to sabotage computer centers. (Especially through the underground magazine *Brand* ["Fire"].) Like most anarchist threats, it's all talk. Swedish anarchists seem to have a hard time finding and accessing computer centers, so they stick to destroying Shell gas stations and other easily identified targets. The IRA, however, has bombed some computers in Northern Ireland. In the U.S., as early as 1969, a group of peace activists known as **Beaver 55** entered a computer system in Michigan, erasing around 1,000 data tapes that supposedly contained blueprints for chemical weapons. This was carried out with the help of ordinary magnets.

There was also a French activist group called **CLODO** (Comité de Liberation ou de Detournement des Ordinateurs). Between 1979 and 1983, these activists destroyed a number of computers in the Toulouse region. They wanted to protest against a computer society in which (in their opinion) computers were used to control people - direct descendants of the original *saboteurs* , in good French tradition. Groups like this make up the militant branch of the civil rights movements to which EFF and Chaos Computer Club also belong.

The most frightening example of this type of activity is perhaps the *Unabomber* (Theodore Kaczynski), who carried out 16 bombings which, altogether, killed three people and injured 23. On Wednesday, August 2, 1995, the *Washington Post* and *The*

New York Times published excerpts of a manifesto written by Kaczynski, and which turned out to be a well-written argument against the explosive growth of technology in modern society.

It is not only the hardware that can be subject to sabotage. Obviously, programs and other information that is stored on a computer can be tampered with. An editor at the *Encyclopedia Brittanica* , in Chicago, became so angry over being fired that he changed a great number of words in the encyclopedia. Among others, he changed *Jesus* to *Allah* . There are innumerable examples of employees exacting revenge on their employers in a similar manner. Another sabotage took place in Israel. By accessing an Israeli newspaper's computers, a 19-year-old hacker managed to publish a false article about his computer instructor being arrested and charged with drug-related crimes in the U.S. (A rather amusing *hack* , in my opinion, but still rather serious considering the importance of mass media in our society. Compare this to *Captain Midnight* , in chapter 4.)

Nazis

Distributing (like the phreakers did) stolen credit card numbers and codes, passwords for computer systems, and similar information, is - obviously - illegal. Some BBSs, like *Ausgebombt* , run classifieds for weapons, steroids, and items that might well be "hot". They can also contain hard-core child or violent pornography, or racist propaganda. Swedish nazis discovered technology at an early stage, and frequently communicate electronically. At least one organization that I know of, with ties to VAM (**Translator's Note:** VAM = Vitt Ariskt Motstånd - "White Aryan Resistance", a Swedish white supremacist group, and a bunch of freaking psychos. I just noticed that the English initials for the organization would be "WAR"), have had guest speakers on computer-related topics.

To be a racist, however, is not illegal. However, incitement to violence and ethnic persecution are very illegal. I personally don't find this relevant to a discussion about hackers. Most hackers are not racists, nor in the least interested in steroids, stolen firearms, or child pornography. When it comes to BBSs, you should follow the same rules that apply to the rest of society: if you see something suspicious on a Swedish BBS, which could constitute a prosecutable offense - call the police. Also keep in mind that those heavily involved in a political movement like neo-nazism usually don't waste time and effort starting and running BBSs without good reason. Before letting your thoughts and actions be guided by hate and disgust, you should consider that these people have often thought long and hard about what they are doing. Have you?

Incitements to criminal action or spreading racist messages is equally illegal whether it is carried out through computers, magazines, or leaflets. On the Internet, most system administrators have enough of a sense of responsibility to remove such garbage when they come across it. If you find something suspicious on the Internet, it is usually simplest to find out who is responsible for the computer on which the information is stored, and inform them. Calling the Swedish police is usually pointless, since most of the Internet exists abroad (primarily in the U.S.). In some countries, it isn't even criminal to distribute racist information or similar stuff. In those cases, the Swedish government is virtually powerless.

The only methods for an authority to contain information stored in another country - with more lenient laws - are to either cut off the nation's computer systems[(1)] (which is neither easy nor desirable), or through international legislation by the UN. But there is another way! The Internet is built by people, for people, and functions through people. *You can give your honest opinion to those responsible for distributing the information.* In the worst cases, you can convince the person responsible for the computer on which the information is stored to remove it. Before resorting to such measures, however, you should think twice. Many view the Internet as a gigantic library, and if you come up with ideas about "censoring" this library, you should consider the fact that you are attacking free speech, and be prepared to take responsibility for that. In such a case, your actions are comparable to going into the nearest library, picking some books out of the shelves, taking them out on the street and burning them.

Information technology has thus brought global problems to your desk at home. How ironic. Now it is no longer possible to shut out world problems; you have to *get involved* . Dear God. Personally, I think this type of discussion is so useful to ordinary Swedish society that it outweighs any threat posed by this "dangerous" information. The problems of Sri Lanka and the Ivory Coast are suddenly our problems as well. As long as child porn is permitted somewhere in the world[(2)] , there will also be such material on our own Internet. Such matters are *everyone* 's problem, like environmental problems. The problem should be solved in its home court: the World. The UN, perhaps.[(3)]

The Police

The Swedish police - through the National police Board - have a computer crime expert, superintendent **Hans Wranghult** in Malmö. He took his studies, as did most European experts in this field, in California. His most prominent work is a report called *Datorkriminalitet - Hackers, insiders, och datorstödd brottslighet* ("Computer Crime - Hackers, Insiders, and Computer-Assisted Crime"), which seems to be an edited version of his class notes from the States, slightly adjusted to Swedish conditions. (I am holding my breath in anticipation of his future creations.) Despite this report being a very detailed treatment of computer crime and various perspectives relating to it, it relays a very simplified picture of hackers. Apparently, Hans has listened mostly to his teachers, and never asked any amateurs what they thought of hackers. His section on hackers begins as follows:

"Originally, the word hacker was a label for the person who was responsible for testing computer systems within the organization for which he worked. The method used was to subject the system to all kinds of attacks, in order to spot errors or weaknesses in the software or the security systems."

This statement is not true, since the first hackers were students in charge of *developing* computer systems, and the statement is indicative of a basic view of hackers as always being busy testing or cracking security systems. If you have read this book from the beginning, you know that this is a fairly small aspect of hacking culture. Another possibility is that Wranghult is simplifying intentionally, in order to motivate his men. The police base their work on a dichotomous "us-against-them" style of thinking, and if he had started talking about good hackers as well as bad ones,

the limits of the law's thinking (with regards to hackers) would perhaps have become a little fuzzy.

He is especially critical of the image of the hacker as a hero, which is blasphemy in his opinion. If he had known how journalists employ hackers, as when Chaos Computer Club hacked into information about the West German nuclear power program, or when the anonymous hacker exposed the *Ausgebombt* BBS, he would have been forced to reconsider his vilification of hacker activities. Apparently the police have thought twice about this, because in June of 1995, they announced that they would be happy to enlist the help of hackers to combat computer crime.

In regards to S Ä PO's interest in hackers and computer culture, there is not a lot of available information. This is not unusual, since it's how things work. **Bengt Angerfelt** and **Roland Frenzell** are in charge of computer security issues at SÄPO, and their work probably consists mostly of gathering information and knowledge about computer crimes, so that someone will know what to do if there is a threat to national security. Hopefully, they know more about computer security than anyone else in Sweden. Considering the fiasco with the encryption system, they should have improved their expertise by now.

Military intelligence is also interested (naturally) in computer security issues. I know even less about this - but the only thing I know for sure is well-known among hackers: military intelligence collects as much information as they can about system and data security. This information is then used to, among other things, improve *their own* security. No military person would ever have the urge to bring this knowledge to the state or the business world. There are some obvious reasons for this. Business in general, and especially the computer companies, are concerned with the security of their equipment. For example, if the American NSA (National Security Agency) informed a company that manufactured a certain operating system of their system's security gaps, these would immediately be fixed. *Why is this not in the interest of military intelligence?* Very simple, really: since the software systems are exported, the military can use the security weaknesses to attack foreign computer systems in case of war. The military (at least in the U.S.) has its own hackers and virus creators. I mean, why not? These weapons are hardly controversial, and not limited by international agreements. Of course, they're armed to the teeth with tools for electronic warfare. By being aware of security glitches, one can protect oneself and attack others. For the same reason, Swedish intelligence would never advise Ericsson about faults in the AXE systems.

A number of Sweden's best hackers have been hired as security experts by SÄPO as well as military intelligence and counter-espionage agencies.[(4)] Probably, this expertise is used in "bugging" electronic communications (which is not illegal, in contrast to telephone surveillance).

Big Brother Wants to See You

But what about the distribution of information that may be "dangerous to the public"? It is not as intuitive to propose that information such as *The Terrorist's Handbook, drug recipes, bomb blueprints,* or perhaps *technical information about telephone cards* should be illegal. A popular term for this is - strangely - *sociopathic*

information . To be a sociopath means to exhibit aggressively antisocial behavior, and belonging to a group that does not accept current social norms

Therefore, hackers, ravers, anarchists, Freemasons, and other subgroups can be viewed as sociopathic. So can Rotary. Sociopathic information, therefore, is information that is written by socially maladjusted people. For example, spreading liberal ideas in a totalitarian communist country would have to be considered very sociopathic. It is not against the law to be socially maladjusted. It isn't even prohibited to distribute sociopathic information. However, there are a few authoritarian elements in our society that would like this to be so. During my research for this book, I have fortunately only found one example of this Big Brother attitude:

In a funky report from **Institutet för Rättsinformatik** ("The Institute for Legal Information"), attorney **Anders Wallin** tells us how *he* thinks the law views sociopathic information. In around 50 pages, he manages the feat of repeatedly condemning so-called sociopathic information, while failing to mention even once that this information is actually not illegal. Rather, he leans on a legal paradigm that views anything that threatens society as it is today as dangerous, by definition. Imposed on ideology, this would be called conservatism. Wallin mentions, among other things, that he hasn't been able to find the sociopathic *The Anarchist's Cookbook* in any Swedish library, and goes on to lament the fact that similar information *is* available on several Swedish databases. What he doesn't mention, however, is that this book has been *cleared* for publication. If you want to read a really sociopathic book, go find **Jerry Rubin's** *Do It!* , which is available at many Swedish libraries. It also happens to be published by the respectable publisher Pan/Nordstedts. The list can be made longer.

Apparently, sociopathic information is a term applied to books that normal people shouldn't read, because if they do, they will become corrupt. Alternatively: books that youth shouldn't read, or they will become corrupt. Or: books that not everyone should read, for their judgment cannot be trusted (as for myself, I am rather childishly fond of the freedom of the press). At the same time, I have to say that I don't think that everything in Wallin's report is bad. What I find erroneous is the implicit call for censorship that exists between the lines of this report. Wallin thinks it's horrible that young boys should be able to read hacker books and terrorism manuals. And I understand him - there are those who have managed to cause great damage using knowledge found in such material. Apparently, someone in the U.S. managed to blow up their little sister. I am not blind to such things. But Wallin has obviously *read this material himself...*

This drives cyberpunks up the wall, and is regarded - justifiably - as authoritarianism. The final responsibility for prohibiting teenagers from building bombs at home should be with the parents. And if the kids are old enough to have left the nest, I would consider them worthy of our trust. Actually, I believe they can handle reading these books, if they find it amusing. I happen to consider a person that manufactures a bomb at home to have more than one loose screw, and not at all a reason to abrogate the rights of normal people to free speech and press. I willingly confess: I own oogles of sociopathic information. Yep, it's true. I have, among other things, used them for research of this book. Almost all of the information I possess is in a digital form, and because I like to, I distribute it with abandon, which I consider not at all irresponsible.

Making Computer Viruses Illegal??
Prohibiting the manufacture of computer viruses is also questionable. Especially since there aren't any plans to criminalize *possession* of computer viruses - only their creation. Can I not produce a computer virus and infect my own computer if I feel like it? This seems strange, in my opinion. A relevant fact is that you could make a computer virus with paper and pencil, if you wanted to. It is not until it is fed into a computer and distributed that it can cause damage.[(5)]

Big Brother: *What do you want to make viruses for? There's no good in that. Don't do it. Don't do it, I tell you. Why are you writing poems? Where's the good in that? Don't. Go to the factory instead, and do some work. Be of use, I tell you.*

On the other hand, I agree that the intentional distribution of computer viruses should be criminal. The debate has been going on in the U.S., where, for example, the well-known virus fighter **Alan Solomon** (known as **Dr Solomon**) has clearly stated that he would consider a ban on virus manufacturing as violating the rights and freedoms of the individual. Furthermore, a virus can not be accurately compared to a bomb, since an isolated computer with a virus on it poses no public threat. Especially if the user know what he or she is doing, which is usually the case when it comes to virus makers. Additionally, a virus does not consist of something tangible (like chemicals or metal), but only of pure information. A computer virus *can* be constructed through a series of commands written on a piece of paper; it is simply a case of the same information in different forms. Thus, a virus on paper would be legal since we have freedom of the press, while a virus in machine-readable form would be illegal since we do not have freedom of information? Aren't they the same thing?

Our modern Trojan horse, in the form of a computer virus, will most likely meet the same end as **Karl Gerhard** 's play *Den ökända hästen från Troja* ("The Notorious Trojan Horse), which was quickly and definitively banned as it criticized the Nazi infiltration of Sweden in the 1940's. Unwanted art should not be exhibited (in the interest of the State), and you do not at all know best what to do with your computer (sarcasm ;-).

"Datainspektionen" and Integrity
The vanguard of the computer crime-fighting forces in Sweden consists of *Datainspektionen* . This governmental agency's primary purpose is ensuring that state institutions and corporations follow **Datalagen** (the Swedish Data Code), which has been constructed specifically to protect the individual from a totalitarian information society. Datainspektionen was born in 1973 as a product of an international public debate with its origins in San Francisco. In connection with the Census of 1970, when for the first time all data was electronically registered, many had begun drawing parallels to **George Orwell's** *1984* , and this gave birth to a debate about data integrity. The insinuation was that government, to a certain extent, was collecting information that they had no legitimate use for, and which could be used to control citizens in every aspect.[(6)]

The former director of Datainspektionen, **Jan Freese** , who still seems to exert considerable influence on the agency, is an important philosopher in the field. In practice, it seems that much of what Jan writes or speaks is adopted by

Datainspektionen without further discussion. This is not so bad, since the guy mostly displays common sense. He has made several sound propositions for information legislation, and prepared Swedish society for the information revolution to a great degree. Especially good is his proposition of a *general integrity law* , covering databases containing information on individuals and privacy violations, whether or not computers and electronics are involved. This law should, according to Freese, regulate (quoted from *Datateknik* #8/1995):

** Access to and searches of private property*
** Physical searches of persons, medical check-ups, and psychological tests*
** Surveillance/espionage*
** Illegal photography/recordings*
** Electronic surveillance ("bugging")*
** Distribution of privileged information*
** Use of third parties' names, images, and similar information*
** Abuse of third parties' communications*

And this is also basically the kind of record-keeping that the EFF, cypherpunks, and others are working against. The difference, in the case of cypherpunks, is that they are of the opinion that the regime (in the US) has totally failed to protect the integrity of the individual. They even suggest that the government cannot handle these matters without becoming totalitarian. *Thus* , the individual should protect him- or herself through cryptography, anonymity measures, etc. The libertarian heritage is apparent, based on the American pioneers, who had to protect their farms and land with their own arms since the legal system was not fully established. That time is so far back in Swedish history that it's become foreign to us. We are used to government taking care of everything.

The reason that more and more people arm themselves with encryption is that the electronic parallel universe, cyberspace, is barbaric and uncivilized, and that even government employees appear to act instinctively and arbitrarily with regards to computers. If an integrity protection law like the one proposed by Freese had existed at an earlier stage, the problem would be absent. *However, note the following:* Datainspektionen is subordinate to the executive branch of the Swedish Congress. If the government gets the urge to register all political dissidents, Datainspektionen cannot do anything about it, despite it being written into law that the executive should consult Datainspektionen before creating any database on its own initiative. Datainspektionen is *in no way* a safeguard against a totalitarian society! Only those who blindly trust institutions and governments would dare to rely on Datainspektionen for this purpose.

From hacking to computer crime

Can hacking lead to crime? The answer is a clear YES. Hacker groups, like any other, have their share of psychopaths and deviant followers. Social engineering in itself must be considered a giant step away from social norms. It *is* dishonest to deceive other people, and viewing the person at the other end of the phone line as an object is frighteningly cold-blooded. Some phreakers have constructed blue boxes that they've sold for around $1500, and this activity is clearly not rooted in ideology.

Phreakers defend their criminal activity in the classical manner: first of all, only large corporations are victimized. Losses from credit card fraud against private individuals are usually absorbed by the issuing banks. At the same time, they nonchalantly ignore the fact that they create a hell of a hassle for the individuals who have to prove to the credit card companies that they didn't use their cards themselves. The elitist attitude often becomes an excuse to do whatever one feels like. At the same time, it should be noted that media as well as credit card companies exaggerate the consequences of being subject to credit card fraud. Even credit card company investigators can think, and generally understand that a well-educated father of two doesn't make repeated conference calls across half the world just for the hell of it. Many investigations are dismissed at an early stage.

Second, hackers often point to the fact that they don't derive any *material gain* from hacking. Hackers are known for breaking into phone companies and stealing *only* manuals. This, of course, confuses prosecutors. A hacker does not fit tour stereotype of a criminal who absconds with other people's property for their own gain. For an hacker hungry for information, the crime *itself* is the reward, which may seem a little odd.

Manufacturing a computer virus, or spraying graffiti on a concrete wall, does not offer much in the way of profit. Possibly it could be sabotage or vandalism, but it is not a matter of organized crime. Perhaps virus manufacturing is, like graffiti, best viewed as an unpopular form of art; a product of our time, in which everything artistic must be sanctioned, planned, and spontaneity virtually extinguished.

Hacking a network is more a matter of *exploring* the system than *stealing* system time. In some countries, like Canada, it is permitted to walk into another persons house, look around, and leave, as long as nothing is stolen or damaged. From an ethical perspective, it is a tricky problem. In the Netherlands it was, until 1987, completely legal to enter a computer as long as nothing was destroyed or modified.[(7)]

Third, they defend their acts on ideological grounds - by which society is described as generally corrupt, and the real crooks are the large corporations and currency traders, who manipulate all of humanity to run their errands through their speculation. The opposite is the beauty of established society, as **Oscar Wilde** once expressed it: *It is better to live unjustly, than without justice.*

In this view, it is permissible to speak and theorize about making society more just, while direct action must be regarded as illegal, from a social perspective. It is the same principle that covers all undemocratic actions - whether it concerns those of hackers, environmentalists, or peace activists. If you break the law, you commit a crime. Period. Personally, I think that any activists who break the law, be it hackers or cyberpunks as well as tree-huggers, peace activists, or anti-abortionists who blow up abortion clinics, *should* be sentenced and jailed if society deems it necessary. It is not the responsibility of society to decide which values serve to justify illegal acts. My opinion, on the other hand, is due to the fact that I firmly believe in humankind's ability to achieve results in a representative democracy.[(8)] Anarchists, on the other hand, conclude that there should be no laws at all. (Which *I* can't really agree with). It's a question of values, and in our present society, un-legitimized actions are considered criminal. If those actions victimize individuals, they're misdirected.

It's been submitted that hackers could form entire underground syndicates and cooperate with the Mafia. This is, so far, mere speculation. In my opinion, the hacker mentality is not really fit for organized crime. The hacker immediately retreats when he/she feels physically threatened, and removed from his/her protected existence behind the screen. This doesn't mean that he or she is *chicken* , but rather that the whole thing is "for fun".

Many hackers receive strange requests like *"you who are so technically skilled, couldn't you build a pirate decoder... ", "couldn't you (whatever)"* , The fact is that even though the hackers definitely *can* do this, they very seldom do. Hackers are anti-authoritarian and detest being bossed around. *"Figure it out on your own!"* is the most frequent answer. The hacker doesn't want some subordinate role as technical genius in some criminal organization. Why should he? He could make a lot more money in a *low-paid* computer job than any criminal organization could offer, with the possible exception of the Mafia or foreign intelligence agencies. However, they are often willing to give advice, tips, and ideas: *"Are you stuck?", "Have you found anything interesting?"* - but as far as economic motivation (not curiosity) is concerned - forget it.

I would go so far as to say that we should be grateful that the little annoying hackers discovered security glitches in the computer systems, rather than the *big fish* . During the golden age of phreakers (in the 70s), several large gambling syndicates used blue boxes, which they manufactured on a near-industrial scale and sold at usurious rates. You can hold any opinion you want about this, but no one can deny that the hackers' activities have been *important* to industry, if not always *beneficial* . (Otherwise they wouldn't have become such a popular topic). When Bob in Springfield makes his own phone cards and sells them for $20-$100, this is hardly to be considered industrial-scale production or even production for his own gain. Considering the simple equipment used in the process, and the time spent on constructing it, it would more closely resemble a total loss. It would, therefore, seem to exist an ideological reason for constructing the phone cards. Freedom of information? Anarchy?

Personally, I would have to say that the "hardware viruses" in the form of an electronic device called *Big Red* , found in some American and Australian banking computers, are much more frightening than anything *any* hacker has *ever* invented. This thing copies, encrypts, and hides important information on a computer's hard drive so that some informed people can easily access it. Big Red could very well be constructed by the Mafia or some international intelligence agency. These must have been deliberately installed from the *inside* of an organization, as opposed to the hacker's curiosity-driven exploits.

As of July 1995, an unusually sophisticated computer theft ring was still operating in Sweden. They entered offices and only stole computers, not monitors or keyboards (these were cut off). From some older models, only memory chips and hard drives were taken. In order to work undisturbed, the gang cut the telephone company's alarm cables by gong through access boxes on the street, in the way the hackers of the film *Sneakers* did it. The gang communicated via radio, and the police even succeeded in taping their communications. Still, they weren't caught.

There's no doubt as to the origin of these thieves. Some of them are definitely some type of hacker, others are more hardened techno-criminals. The similarity to Gibson's characters is striking: the only loot is information technology, memory is worth its weight in gold, and the criminals possess fantastic technical skills. I will not for one second deny that these offenders have learned many of their skills used in their ventures through different hacker magazines: Rolig Teknik, Phrack, any number of books from small, obscure publishers. (And certainly, from common textbooks). But this is actually not the problem.

The problem is *us.* The problem is that we watch movies like *Sneakers, The Saint, Why Me?* etc., in which we can identify with the romantic or comical criminal, despite the fact that we objectively judge such a person to be the enemy of society and scum deserving of all that is coming to them. We need the criminal, or in this case, the *technologically advanced criminal* , to know that it's still possible to circumvent all electronic security systems. Because - if we can't escape technological supervision, well, then we *can't* become lawless, and then being lawful is no longer a free choice. There is no longer any anti-career that we can look down upon in our eternal quest to jet upwards through the social hierarchy. There is no honor to preserve, because if no one can be dishonorable, one cannot know what it means to be honorable. Crime exists in the form of an engine that drives us to act straight, warns us if we approach the edge of propriety, and makes us feel content with our successful lives. We, of course, do not run around at night, cutting cables, and stealing computers, do we? We work during the days and *sleep* at night. Each day needs its night. Every society's glowing, law-abiding segment needs its photophobic underground movement.

We award our geniuses two types of careers. Either they go through twelve years of high school and four years of college to become engineers and continue their careers upwards or sideways in the chase for *more* status, *more* money, and *more* exciting work projects. (Imagine, I could be CEO one day... I'll have to read up on some finance too... make the right contacts, hold the right opinions...). But what if you don't like school? What if the awfully long education bores you, but your interest is still burning for electronic devices and computers? No problem. Society has something for you too: *vocational* education, *no* status, *no* money, and *no* exciting work projects like PLEX programming or control system construction. You will never go to the right schools, know the right people, or read the right books. You won't have the correct social heritage. *This is despite the fact that you are perhaps intelligent and capable and would be more suitable for Ericsson's training programs than anyone else!* The hiring practices at high-tech companies are tastefully oriented towards turning non-degreed applicants back to the slums they came from.

Remaining option: anti-career. Use your knowledge to break down society's security systems so that the poor citizens will know it's not invulnerable. Give them something to fight and live for. Give them an external threat so that they won't have to take a look in the mirror. Be an outlaw to set the parameters for the lawful. Don't think that crime doesn't pay - sometimes it does. Just as long as a few get caught now and then so that the good people will have something to abhor.

Your criminals are the devils that let you see the angels within yourselves. I'll be damned if they're any worse than you![(9)]

Corporate Security Forces

One of the most unpleasant computer crimes I know of was committed (and perhaps is still being committed) by **Telia** . In April 1995, the electronic magazine **Z Central** (a subsidiary of Z-mag@zine) made public that Telia possessed its own net surveillance unit, which had as its mission to gather information about subscribers suspected of being phreakers or hackers. Using phone-switch computers, they could easily record who made what calls and where. It seems that Telia systematically traced and surveilled some hackers, which really is something that only the cops have a right to do. This information was further distributed to other companies which Telia suspected of having been infiltrated by these hackers. These procedures are illegal, according to the fourth section of the Data Code, which prohibits registering information concerning possible criminality without the prior permission of Datainspektionen. Permission is almost never granted - in order to prevent totalitarian social control.

It should be added that this discussion about Telia's phone usage registration is not a new one. As early as 1981, Telia had an electronic surveillance machine named **TAL-T M80** , which permitted the logging of all usage on a particular line, and could send the log to a central computer for storage. Since then, Telia has introduced this type of surveillance to virtually any phone in Sweden, since this function is built into every AXE switch. In reality, anything you do using a phone is recorded by the AXE switch. If you pick up the phone and then dial *one* digit before hanging up, this action is registered as a time and a button-press in a computer. Telia is then able to retrieve a complete listing of all calls and non-calls performed - *anything* that has taken place on the line. The information, according to Telia, is used to assess and improve existing systems, and to resolve disputes with subscribers. The info is stored on computer tape for about six months.[(10)]

Anyone that has worked for a large corporation will understand why Telia can't resist registering and analyzing its business. However, distributing such information is against telecommunications as well as privacy laws. Telia, of course, acted in "good faith" in its attempt to "help" the victimized companies, but that doesn't excuse the breach of privacy involved. I've even seen indications that Telia use their databases for various purposes within the company. The information is ruthlessly consulted by Telia's security departments when they suspect hacker activity, in order to extract information from hackers about their possible transgressions. (In many cases, Telia's own computers suffer from inadequate security.[(11)]) This takes place despite the fact that this information is not even supposed to be available to the police...

To facilitate computer crime-fighting, they've begun to investigate the possibility of constructing a so-called *expert system* , an artificially intelligent agent instructed to analyze the bands in which all Swedish phone calls are registered, in the search for *behavior patterns* that seem suspect. This involves checking out people that make long and frequent calls without interruptions, call a lot of toll-free numbers, etc., in order to compile a database of "suspicious" subscribers. Hopefully, Telia does not intend to use the system, since this would imply a completely illegal data-handling procedure. But what price is too high to maintain security?

Telia serves as an example for large corporations' views on computer crime. Of those crimes committed against Telia's technological installations, 87% consist of theft and

vandalism, while computer intrusion and technical manipulation makes up about 10%. The latter category includes hackers' and phreakers' activities, but also a great deal of other activity that has nothing to do with those underground groups. (*But,* since hackers have a definable culture and system of ethics, they're easier to point out and condemn). In addition, Telia is a company that suffers from an almost paranoid fear that someone will understand how their systems work. All communications companies feel this way. Since the technological safeguards at Telia's switches are inadequate, they rely on a *psychological* form of protection, which simply means that information is kept secret so that a possible attacker cannot know how the systems work. In the same manner, it protects its own organization, its own internal phone numbers, etc. Even *within* the organization, safeguards are in place. They are diligent about not giving any more information than necessary to operators. There is no comprehensive understanding of Telia's systems except among CEOs, high-level engineers, and system developers. The only road to those positions lies in internal advancement. Knowledge in regards to Telia's systems is therefore only supposed to exist within the organization, and no one outside Telia should know anything about how the switches really work. *Hands-off* , as opposed to "hands-on", that is. Just use the system. Don't ever try to figure out how it works, even if you're interested. Do not examine, do not rummage among the cables, just *call, pay,* and *be happy!*

The reason that Telia has its own security organization is that the police has neither the time nor the funding to investigate Telia's problems. (As I mentioned earlier, they are reluctant to investigate fraud amounting to less than $8000 or so). Telia has officially said that the company needs about 30 security managers plus about 10 or so specialists within the areas of physical security, system security, data processing, secrecy, and information security. The last category is the one that is supposed to make sure that I, among others, should not know the information contained in the previous sentence. (These figures, however, originate in the time when Telia was still called Televerket, and had to release information because of the freedom of information laws). Presumably, the information security officials now have a structured organization which ensures that potentially dangerous information does not leave the company or end up in public records.

Another thing, which should be completely made clear, is that large corporations like Telia cannot afford morals. Once they have discovered fraud affecting the company, they first have to decide whether it pays off to go after the criminals and improve security before taking any action. If improving security poses too much of an inconvenience for legitimate users, resulting in loss of customers, it is more cost-effective to let the hackers be. This has led to many hackers raising their eyebrows and wondering whether the communications companies are laid back, stupid, or just plain moronic. In reality, their only concern is money. That's why it's still so easy to call using fake credit card numbers - it is simply too expensive to effectively address the problem.

At this point, allow me to make a connection. When I spoke of cyberpunk, I mentioned that William Gibson et. al. chronicle a future in which all finance and development is handled by large corporations, with a strictly hierarchical organization and a ridiculously strenuous work ethic. In the R&D labs, new technological innovations are pushed out by bored engineers with their fingers constantly on the fast-forward button. Everything in the organization of these companies is designed to

make the people inside the hierarchy feel as important as possible, so that they will work as effectively as possible and push their underlings to work even harder. The result is a frighteningly effective but psychopathic organization, which can push social development beyond any imaginable limits.

Those hackers that have been forced to enter Telia's regional offices in the capacity of informers, have - with awe - described the rigorous security procedures. They have passed many doors, all with flashing diodes and demanding access cards to prevent the wrong person from being in the wrong place at the wrong time. At the very top of the building, there are the offices of the highest executives, after a total of perhaps five doors that all require pass codes. The hierarchy demands that the offices gain size as they gain altitude. At the top, they are posh. This is the final goal of all the residents of the building. The denizens of the lower levels of this tower of power are not allowed to pass through as much as half the doors leading to the top level. In this manner, the eternal desire to climb to the top is preserved.

The hacker is called to this place. The man on the other side of the desk is not evil. He is not inhuman, psychopathic, or simply cruel. He is diligent. He believes in the ten stories of concrete through which the hacker has just been transported. He has been, for his entire life since leaving the university, a part of this hierarchy. Since he is a CEO, he has been among those displaying the greatest loyalty and faithfulness to the company and the entire social system which has enabled it to exist. He can not, for the life of him, imagine that any of this could be based on an incorrect assumption - that there could be anything wrong with the market economy system, a giant wheel in which he himself is but a tiny, tiny cog. Somewhere deep inside, he retains a small illusion of freedom and independence which he nurtures tenderly.

He has a lot of respect for the hacker. The 20-year-old on the other side of the table managed, after all, to breach all the walls he has built. And the hacker didn't accomplish this through violence, but through intelligence. He manipulated Telia's computers. He was one step ahead of Telia's own security teams. The boss is impressed. But at the same time he knows, based on his fundamental appreciation of the society which lets him live in a plush two-story house with a housewife, two kids, and two cars, that this kid is wrong. The boy is a criminal, and should be treated like one. He knows that he is dealing with a dangerous individual. He has completely swallowed the myth of the hacker as a cold-blooded, anarchistic antagonist. It his *him* , the Chief of Security, who is right. The concrete, the desk, the condo, the market, the school system... all of these back him up. Of course he's right. How else are things supposed to work?

Of course, he has to know how the kid did it. Since he knows that he's right, he feels entitled to use any means available. In the concrete chambers in Göteborg, Farsta, and Kalmar, his devoted servants stand at attention - **IBM 3081 d, AS/9000, Sperry 1100/92 -** computers that obey his every command. Even before the hacker was brought to the office, he had lists printed of all the calls that this individual had made during the last six months. An exhaustive list, with dates and times down to the second. *So he called his girlfriend in the middle of the night after a two-hour call to a toll-free number in the States? Why? Is she involved as well?* It'll be a long interrogation. The hacker on the other side of the desk doesn't know that the list that is about to be put in front of his nose by Telia's security chief is totally useless from a

legal point of view. Nothing is witnessed or signed; only five calls have been traced. These calls constitute the only binding evidence.

The hacker, with his boring middle-class background, looks across the table and straight into the eyes of the impressive boss. He locks gazes with Gibson's psychopathic Tessier-Ashpool concern. He sees the enormous company's pulsating brain sitting in front of him, dressed in Lacoste pants and a white shirt. The question is whether he understands this.

The BBS that Vanished

Let's imagine that a group of cyberpunks, in the near future, create a BBS named *Pheliks* to spread information using a powerful personal computer with several telecommunications lines. Stored on this BBS is pirated software, drug recipes, anarchist pamphlets, in-depth descriptions of Telia's AXE switches, documentation for smart credit cards, and much more. The software industry, spearheaded by Microsoft, are pissed. The credit card companies, spearheaded by Visa and Mastercard, are pissed. The police, wishing to maintain order, knows that this is against the law and feels compelled to act. Unfortunately, the cyberpunks are aware of the possible countermeasures of the police and other authorities, and have implemented their own counter-countermeasures. When the authorities call up the BBS they are greeted by the following message:

> **Pheliks BBS - open 24 hours at 28.800 bps.**
>
> **NOTE: Pheliks BBS is open to amateurs. Police, journalists, researchers, or other persons in an official capacity, as well as business persons or representatives of non-profit organizations, are NOT WELCOME. If you belong to any of these categories, we humbly but firmly ask you to terminate your connection to Pheliks BBS. Press ENTER to confirm that you do not belong to any of the above categories. Press +++ath0 to terminate the connection.**

Through this messages, paragraph 21 of the data code is invoked, with the result that anyone not complying with the request is guilty of a computer crime. In this way, every form of electronic search is made impossible, and the BBS is not threatened by governmental agencies or research institutes, which are bound to stay within the law. *Journalists* could in this case appeal to their moral right, as a third power of the State, to breach the data code in the public interest. The software companies, in the form of Business Software Alliance, would also (most likely) not give a shit about the data code and proceed despite the message. After a scoop in the papers, combined with repeated anonymous tips (read: lobbying) from the BSA, and combined with some sort of surveillance indicating that there might even be illegal drugs in the same location as the BBS, the police could raid the BBS after all.

However, the cyberpunks have predicted this scenario as well. When the cops bring the BBS computer to the station, they find that the part of the hard drive containing the BBS's information has been encrypted with the *Securedrive* program. This software uses 128-bit DES encryption, known to be uncrackable. To encrypt your hard drive is perfectly legal - businesses do it to protect confidential information from theft, and as opposed to everyday locks, encryption cannot be opened by force. At the

same time the police turned the computer off, it became useless as evidence. For investigative reasons, of course, the cops could keep the computer for a century or so, and in this manner prevent the suspicious activity from recurring. Unfortunately, computers are not that expensive. Even before the investigation has begun, the well-organized cyberpunks have gotten a new computer and restored the entire BBS from tape backups stored in a totally separate location. Companies use the same method to protect valuable information from theft, fire, or hardware malfunction.

The police can then, given reasonable cause, install surveillance equipment and record the traffic to and from the BBS, record cyberpunks keystrokes, etc., in order to make a successful bust. But this is very expensive, and there has to be a good reason for such measures. It is also probably that the software companies resort to illegitimate measures. Perhaps they retain a samurai hacker, like the computer cowboy Case in Gibson's novels, to enter the BBS and crash it on the orders of the company. Perhaps some company manages to convince Telia to shut down the BBS's phone lines. In this way, established society can protect itself against the cyberpunks, and maintain the ideals that have been threatened.

The real danger occurs when too many groups like that appear, hiding from governments and companies, or form an organized, nationwide base. The worst thing that can happen is that the BBS moves to an unknown address on the Internet, possibly in Taiwan or Chile. If you can afford to rent space on a computer on the other side of the world (which probably is cheaper than having your own), there are no problems with maintaining such an operation from Sweden. This is when the cyberpunks can go from information syndicate to broad, underground, political movement. And this is the real threat to established society. It is not certain that it is a threat to society from a historical perspective. I will return to this question.[12]

---

1. German authorities took this approach in trying to shut down *Radikal* , an extreme-leftist magazine, which - intelligently enough - has stored their files on a computer in Holland. The endeavor became a fiasco: about thirty supporters copied the documents to their own computers, with the result that Germany would have to disconnect the entire world to get rid of *Radikal* .

2. Japan, for example, has a very liberal view of material that people in Sweden would most likely put in the category of child pornography.

3. I am not fond of international governmental organizations except as forums for discussion. As such, they excel. On the question of international retaliations and such, I am undecided.

4. I. e., computer crime sometimes pays - if you're the baddest.

5. Some may object to me defining this in my own terms. This is because there is no legal framework within which to discuss the issue.

6. I am greatly indebted to Anders R Olsson for many of the details regarding the

origins of the Data Code and the inception of Datainspectionen.

7. This is probably the reason that Europe's largest hacking magazine, *Hacktic* , is based in Holland. The hackers later started an Internet company called XS4ALL, which is one of the largest and most controversial Dutch internet providers.

8. On the other hand, I don't think that this type of government is ideal, nor that it will last in the future.

9. In case you are wondering: yes, I've studied social psychology as well.

10. I have obtained this information from an anonymous technician at Telia. Ronnie Bjarnfält, at Telia National Security, claims that the logs are normally only kept for 24 hours. I have personally seen logs comprising three months of telephone traffic.

11. Anonymous hacker in october 1996: *"I am inside Telia's firewall again... they installed a new one that was much better, but I got around it..."*

12. All "fictional" events in this episode have occured in reality.

Chapter 11
ARTIFICIAL INTELLIGENCE

Discussions about artificial intelligence (AI) are frequent in many contexts, not least in those that are treated in this book. That's why I've given AI a chapter of its own.

AI is a multi-disciplinary science, encompassing electronics, computer science, psychology, sociology, philosophy, religion, medicine, and mathematics. This is by no means an exaggeration; creating AI entails knowing how "normal" intelligence works, which is easier said than done - since the only object we know with certainty to be intelligent is the human brain. AI ultimately concerns the study of behavioral sciences in order to build models based on natural science. Our intelligence, it has been discovered, is strongly connected to our way of knowing the world, or our perception.

AI research is a hot item at the universities, and not without reason: for the first time in history, there is *money* to be made in AI. Companies that are increasingly employing electronic means for communication and administration are in need of computer programs to handle routine tasks, like sorting electronic mail or maintaining inventory. So-called intelligent *agents* are marketed, customized for various standardized electronic tasks. From a cynical perspective, one could say that industry for the first time can replace thinking humans with machines in areas no one had thought could be automated. (I should add that it can hardly be called *automation*, since the truly intelligent programs actually *think*, as opposed to just acting according to a list of rules).

There is a number of approaches and orientations within AI. Among the most prominent there are: *expert systems* (large databases containing specific knowledge), *genetic algorithms* (simulated evolution of mathematical formulas, for example, to suit a certain purpose), and *neural networks* (imitation of the organizational structure of the brain, using independent, parallel-processing nerve cells). As information databases like those on the Internet become larger and more numerous, agents can work directly with the information without having to understand people. Why assign a person to do research when you might as well let an agent do it, more quickly and for less money? (Whoever has ever looked for information on the Internet will realize how useful a more intelligent search tool would be).

There is also research in the field of *artificial life*, which really are "living" organisms that live and reproduce in computer systems. Computer viruses constitute one form of artificial life, albeit somewhat unsophisticated and destructive. Artificial life has hitherto not achieved any substantial success. (Unless you want to view computer viruses and all the companies and consultants that make a living fighting them as a success - they have evidently boosted GNP). Research in the field of artificial life began with a program called *Life*, by **John Conway**, and was a mix between a computer game and calculated simulation. **Bill Gosper**, hacker at MIT, became virtually obsessed with this simulation. Later on, it was improved and renamed *Core Wars*, the idea being that many small computer programs would try to expand and fight over system memory (*core* memory), with the strongest ones surviving. The programs are exposed to various environmental factors similar to the demands put on

real life: lonely or overcrowded individuals die, programs are exposed to mutation risks, system resources vary with time (daily rhythms), aging organisms die, etc. **Tom Ray** has been especially successful in the field with his *Tierra* program. His artificial life forms have, through simulated darwinistic evolution, managed to develop programming solutions to certain specific problems that were better than anything man-made.

I have already mentioned that hackers have a respect for artificial intelligence that is completely different from that of people in general. A person growing up constantly surrounded by computers does not see anything threatening in the fact that machines can think. He/she sees the denunciation of AI as a sort of racism directed towards a certain life form. If you criticize artificial intelligence, saying that *it can never be the same, only humans can think*, etc., then consider the fact that there is no scientific basis whatsoever for supposing that the human brain is anything but a machine, although it may be made of flesh.

These thoughts date back to **Ada Lovelace** and **Charles Babbage**, two of the progenitors of computers, who discuss the subject in a piece called *Thinking Machines*, published in the 19th century. However, these ideas did not become widely known until the 1960's, through films such as the horror movie *Colossus - The Forbins Project* (1969), in which intelligent military computers take over the world. This notion also figures in the *Terminator* films, with the only significant difference being that the computer's name is *Skynet* - thus, not much new under the sun in popular sci-fi. The fear of artificial intelligence actually dates all the way back to **Mary Shelley's** *Frankenstein* (1818), and perhaps even further back in history.

In the fiction of Frankenstein, the fear of AI is personified. This story, about a scientist who creates a lethal intelligence, has become one of the new symbols of the industrialized world, in the same class as early Greek mythology. There is a connection between the Bible and Frankenstein, in that the creation (mankind in the Book of Moses, the monster in Frankenstein) rebel against its creator (God and human, respectively). In Judaic mythology there is a corresponding myth about the clay-man **Golem**, who runs amok when its master forgets to control the creature. It has occurred to me how far ahead of its time this myth was: Golem was made of clay, and computers are made of silicone, which is made from sand. The maker of Golem, **Rabbi Löw**, feeds a piece of parchment with the name of God on it into the creature's mouth, in order to make it "run". This is comparable to the engineer "feeding" software into the computer. To stop the runaway Golem, the Rabbi removes the parchment from its mouth, whereupon the creature collapses into a pile of dried mud, robbed of its spark of life.

Thus, the fear that mankind - like God - will create intelligent life from dead matter is found as early as in the two 19th-century myths described above. This rather unfounded fear of *rebellion against God* makes up the foundation of much of the hostility directed towards AI research. The fear is based in the Biblical myth of Adam and Eve eating the forbidden fruit, and the possibility that another creation will follow in our footsteps. I will, however, overlook these myths, and instead focus the argument on the philosophy underlying AI-research: *Pragmatism* with its heritage of Fallibilism, Nihilism, and Zen-philosophy. (Don't let these strange word discourage you from reading on!)

One could ask *why* scientists promptly have to try to create artificial intelligence. After all, there are already people, so why attempt to create something new, better, something alien? Asking this question of a scientist in the field is akin to asking a young couple why they promptly want to have children. Why raise a new generation that will question everything you have constructed? The answer is that it's something that simply just happens, or is done: it is a challenge, a desire to create something that will live on, an instinct for evolution. This is perhaps also what partly motivates hackers to create computer viruses: the pleasure of seeing something grow and propagate.

Our entire society and our lives are so interlinked that they cannot be separated. Society, machines, and humanity - everything has to progress. Evolution doesn't allow any closed doors, and AI is, in my view, only another step on the path of evolution. I see this as something positive, while others are terrified. At the same time, one shouldn't forget to note the *commercial* interests underlying the expansion of AI. Computers reading forms, sorting information, and distributing it, is obviously simply another way for the market to "rationalize" people out of the production chain, automating clerical work, and making the secretary and the accountant obsolete. The board of directors of a corporation is, as usual, only interested in making money and accumulating capital. *Wouldn't you?* What is the hidden nature of this complex entity (or as I would refer to it, *superentity*) that we call *"the market"*, and which constantly drives this process of development forward?

If you are interested in knowing more about AI and its philosophical aspects, it is to your advantage to read a book called *The Intelligent Age of Machines*, by **Raymond Kurzweil** (1990). To learn more about the inner workings of AI, read **Douglas Hofstadter's** *Gödel, Escher, Bach: An Eternal Golden Braid*, which is both an elevating and depressing work. In one respect, it is a scientific validation of Kafka's thesis: *to correctly comprehend something and at the same time misunderstand it are not mutually exclusive*, which is an observation that (fascinatingly enough) is akin to the paradoxes within Zen Buddhism, a religion that in some aspects border on pure philosophy. To explain some of AI's mechanisms, I need to explain some things about the part of Zen that is associated with philosophers like **Mumon**, and which has less to do with sitting around in a lotus position and meditating all day. Zen, in itself, is a philosophy that can be dissociated from Buddhism and viewed separately. Buddhism is based on respect for life, in all its forms, Zen, by itself, makes no such demands, being a non-normative, non-religious philosophy.

Zen, or the Art of Breaking Out of Formal Systems

Zen has also become one of the most influential "new age" philosophies in the West during the 80's and 90's. Books like *Zen and the Art of Motorcycle Maintenance* sell amazingly well. among other things, Zen Buddhism suggests that the entity that Western tradition calls God (and what the Buddhists call the Brahma of the Buddha) is in fact a sum of all the independent processes in the universe, and not a sentient force. Therefore, God is equally present in the souls of humans as in the circuits of a computer or the cylinder shafts of a motorcycle. Put simply, Zen is one long search for the connection between natural processes, in the cosmos or the microcosmos, and this search in itself constitutes a process that interfaces with the others. Zen Buddhism is *the search in itself*, the point being that Zen (an abstract term for "the answer") will

never be found. Searching for Zen means that one continually come to a point where one answers a question with both *yes* and *no.* For example:

> Q: Is the ball in the bottle?
> A: In one way, yes, if the bottle's inside is its inside, and in one way, no, if the bottle's outside is its inside.

Zen constantly toys with our way of *defining* our environment, our method of labeling things as well as people. Zen teaches us to see through the inadequacies of out own language and assists us in dismantling fallacious systems, as in when, for example, we've gotten the idea that all criminals are swarthy (or that all hackers break into computer systems!). Zen is the thesis that no perfect formal systems exist, that *there is no* perfect way of perceiving reality. Kurt Gödel, the mathematician, proved that there are no perfect systems within the natural sciences, and the fact that there are no perfect systems within religion should be apparent to anyone who isn't a fundamentalist.

Zen could be said to be based on the following supposition: *The only absolute truth is that there are no absolute truths.* A paradox! - which is, naturally, a perfect starting point for the thesis that reality cannot be captured and all formal systems (like human language, mathematics, etc.) must contain errors. Even the proposition that reality is incomplete is incomplete! *Truth cannot be fully expressed in words* - hence the necessity of art and other forms of expression. I will end the discussion of Zen now, but hopefully you understand that many become confused and annoyed when one tries to explain Zen, given that the explanation is that there is no explanation. For example, note a quote by **William S. Burroughs**: *"language is a virus from space"*, expressing his frustration with the limitations of human language. Even Nietzsche criticized language, finding it hopelessly limited, and feminist **Dorothy Smith** has a theory concerning the use of language to control the distribution of power in society.[(1)] In the Western philosophical tradition, the equivalent of Zen is called *Fallibilism*, a philosophy based on the theory that all knowledge is preliminary. This has subsequently been developed into a philosophical theory called *pragmatism*, which views all formal systems as fallible, and thus judges them based on function rather than construction. Gödel's Incompleteness Theorem is probably the most tangible indication that this conception of the world is correct.[(2)]

A lot of modern mathematical theory of so-called *non-formal systems* are associated with both Zen and Chaos theory. A non-formal system creates a formal system to solve a problem. In order to have a chance of understanding a (superficially) chaotic reality, we must first simplify it by creating formal systems on different levels of description, but also retain the capacity to break down these systems and create new ones. For example, we know that humans are made up of cells. We also know that we are made up of atoms, and as such, of pure energy. Nature invites to so many levels of description that we have to sift through them to find those that we need to complete the tasks we have selected. This is called intelligence.

There are also other philosophies that draw on parts of Zen: for example, *Tao* views contradictory pairs such as right/wrong or one/zero (the smallest building blocks of information) as holy entities, and focuses on finding the "golden mean" between them (the archetype is *Yin* and *Yang*, a kind of original contradictory pair). Our Western

concept of thesis-antithesis-synthesis also belongs to this group. The strength - and weakness - in these approaches are that they instill in their followers a belief that *moderation is always best*, which can be both true and false according to Zen (depending on how you view it). All such attempts to force reality into formal systems are of course interesting, but definitely temporary and constantly subject to adaptation. Another philosophical system using this mode of thought was the pre-Christian Gnosticism, where the original opposites are *God* and *Matter*. These become intertwined within a sequence of *Aeons* (ages of time, imaginary worlds, or divine beings). Gnosticism probably originates (in turn) from an old Persian religion called *Parsism*, created by the well-known philosopher **Zarathustra**, who initially claimed that the world was based on such opposites.

Zen's way of thinking is partially a confirmation of the so-called *nihilistic* view of reality, in which objective truth does not exist, and partially a denial of it: it is simply a matter of point-of-view. Objective truth exists *inside* formal systems, whereas *outside* them, it does not. By breaking out of a formal system in which reality is described in terms of right and wrong, or intermediate terms such as *more right than wrong*, one finds a part of the core of intelligence. Being intelligent means being able to build an ordered system out of chaos, and thoroughly enough to be able to view one's own system from the inside and adjust one's own thoughts according to its rules. AI research has - in an amazing fashion - shown that this ability is completely vital to *any intelligent operation whatsoever*.

The difference between the real world and the one pictured inside the formal system of one's own creation has ruffled the feathers of such grandfathers of philosophy as Plato, Kant, and Schopenhauer. It has made them decide, after languishing analysis, that the real world is defective and incapable of approaching their own perfect, mathematical world of ideas. (Please note my mild insolence; as a 24-year-old layman I shouldn't be able to claim the right to even speak of these great philosophers. The alert reader would notice that I'm very busy questioning traditional authorities ;-). In science, this conflict is known as the subject-object controversy. Even in such "hard" sciences as physics this conflict has proved to be decisive, especially in *Bell's Theorem* (well-known among physicists), which has puzzled many a scientist. (I'm not going to go into the details of Bell's Theorem, but I'm employing it as a reference for those who are familiar with it).

When AI researchers sought the answer to the mystery of intelligence, they came into conflict with scientific paradigms. We need to use intelligence to understand intelligence. We need a blueprint for making blueprints; a theory of theoretical methods, a paradigm for building paradigms, etc. They found a paradox in which a formal system would be described in terms of another formal system. This is when they took Gödel's theorem to heart - a proof that all formal systems are paradoxical. The solution to the problem of creating a formal system for intelligence was self-reference, just like a neuron in the brain will change its way of processing information by - just that - processing information. The answer to intelligence wasn't tables, strict sets of rules, or mathematics. Intelligence wasn't mechanical. For intelligence to flourish, it would have to be partially *unpredictable*, *contradictory*, and *flexible.*

Many hackers and net-users are devoted Zen-philosophers, not least because many of the functions within computers and networks are fairly contradictory. The section of

computer science concerned with AI is self-contradictory to the highest degree. *Programming* is also the art of creating order from an initially chaotic system of possible instructions, culminating in the finished product of a computer program. If this section has been hard to understand, please read it again; it is worth comprehending.

Humans as Machines - The Computer as a Divine Creation

Most hackers view people as advanced machinery, and there's really nothing wrong with this; it is simply a new way of looking at things, another point of view within the multi-facetted science of psychology. Hackers in general are futurists, and to them the machine (and thus the human) is something beautiful and vigorous. I'll willingly admit that to a certain extent I also view humans as machines, but I'd like to tone that statement down a bit by saying that we (like computers) are *information processors* - we are born with certain information coded in our genes, and in growing up we assimilate more and more information from our environment. The result is a complex mass of information that we refer to as an *individual*. The process by which information is handled and stored in the individual is known as intelligence. The individual also interacts with the environment by symbolically absorbing and emitting pieces of information, and thereby becomes a part of an even larger process, which is in itself intelligent. (If you're of a religious persuasion, this could be taken as an example of hubris) But what about the *difference* between computers and humans?

Two things: the computer knows who has created it, and human life is clearly time-limited. It has been proposed that the uniqueness of a human "soul" is a product of just these two factors, and that it's therefore only uncertainty and finitude that makes life "*worth living"*. Of course, the theory could be challenged by proposing that its two premises are negotiable from a long-term perspective. Hereby the reader will have to draw his or her own metaphysical conclusions; the subject is virtually interminable, and the audience inexhaustible.

> *"I have seen things you humans can only dream of… Burning attack cruisers off the shoulder of Orion… I saw the C-rays glitter in the Tannhauser Gate… All these moments will now be lost in time, like tears in the rain."*
>
> (The android Roy Beatty in **Ridley Scott's** *Blade Runner*, understanding some of the meaning of life in his final moments)

By delving deep into psychology, the subject becomes simpler. An intelligent system, whether artificial or natural, must be checked against a surrounding system (what we might term a *meta-system*) in order to know the direction in which to develop itself. In an AI system designed to recognize characters, "rewards" and "punishments" are employed until the system learns how to correctly distinguish valid and invalid symbols. This requires two functions within the system: the ability to exchange information, and the ability to *reflect* on this exchange. In an AI system, this is a controlled, two-step sequence: first information is processed, then the process is reflected upon. In a person, the information processing (usually) takes place during the day, and the match against the "correct" pattern occurs at night, in the form of dreams in which the events are recollected and compared to our *real* motives (the *subconscious*). The similarity is striking.

Through this line of reasoning, we can draw the conclusion that people have an internal system for judging correct action against incorrect action. As if this wasn't enough, we also know that we can alter the plans by which we act - i.e., we are not forced to follow a specific path. In this sense, humans are just as paradoxical as any informal system, since we have the ability to break out of the system and re-evaluate our objectives. However, the great philosophers of psychology, **Sigmund Freud** and **Carl Jung**, found that there was a set of symbols and motives that *were not* subject to modification, but rather common to all persons. Freud spoke of the overriding *drives*, mainly the sexual and survival drives. Jung expanded the argument to encompass several *archetypes*, which referred to certain fundamental notions of what is good and what is evil.[(3)] These archetypal drives, which seem to exist in all animals, appears to be the engine that propels humans into the effort of exploring and trying to understand their environment.

This is the most fundamental difference between persons and machines. There is nothing that says that we should have to let intelligent machines be driven by the same urges as we are. Instead, we can equip them with a *drive* to solve the problems for which they were constructed. When the machine evaluates its own actions, it is then constantly driven towards doing our bidding. **Isaac Asimov**, the science-fiction writer, suggested such things in his robot novels through the concept of the laws of *robotics*, by which robots were driven by an almost pathological desire to please their human masters. This relationship is also found in the modern film *Robocop*, in which an android policeman is driven by his will to indiscriminately uphold the law.

Towards an Artificial Age - AI and Society

Aspects of AI is mirrored by the media of our time - *Blade Runner* is about the difference between man and machine, AI figures heavily in cyberpunk novels, music and film, and in 1995 the movie Frankenstein makes a comeback in the theaters. Coincidence? Hardly. An exciting example of this trend is Arnold Schwarzenegger's role as the robot in *Terminator 2*. In the film, the artificial intelligence holds human characteristics, as a result of being programmed by a human rebel instead of a brutal military force. It also touches upon aspects of the consequences of carelessly handling technology (as when Rabbi Löw lost control of his Golem). Of particular interest is the scene in which the robot, being machine, simply follows its programmed instructions to obliterate people standing in its way as opposed to finding peaceful solutions. The lead character, John (which incidentally happens to be a skilled hacker), discovers a dangerous "programming bug" in the robot's instruction set, which he corrects. The message of the film is that technology and AI are good things - if used properly and supervised by human agents. The real danger is people's ignorant nonchalance.

The Swedish movie *Femte Generationen* ("The Fifth Generation") again deserves being mentioned in this context. Fifth-generation computer systems are simply another name for artificially intelligent systems.

Lars Gustavsson makes a strong impression with his beautiful sci-fi novel, *Det Sällsamma Djuret Från Norr* ("The Strange Beast from the North"), which treats the metaphysical aspects of AI in a thorough and entertaining manner. His thoughts on decentralized intelligence are especially exciting, which suggest that a society of ants could be considered intelligent, whereas a single ant could not - and in this manner, all

of humanity could be viewed as one cohesive, intelligent organism. This view is taken from sociology, which has become very important to AI research.

Flows of information are an indication of intelligence. This is confirmed in the model of society as a unitary sentient force. The intelligence of individuals and societies are undoubtedly related; the ability to store and process information through the construction and dissolution of formal systems is a sign of intelligence. Society is an organism, but at the same time it is not (yes, this is very Zen). These ideas go all the way back to the founder of sociology, **Auguste Comte**. I have myself coined the term *superindividuals* as a label for these macro-intelligences known as *corporations, the market, the state, the capital,* and so on. I will return to this subject further ahead.

Again, it is possible to emphasize the relatedness of chaos research and intelligence; intelligence can be seen on many different levels, each constituting a formal system in itself. One system is akin to another, and they form as strangely coherent pattern. Our intelligence seems to be united with our ability to enforce chaos.

Alan Turing and the Turing Test

Alan Turing was one of the very first people concerned with making machines intelligent. He proposed a test that could decide whether or not a system was intelligent - the so-called Turing Test. It consisted of placing a person in a room with a terminal that was either connected to a terminal controlled by another person, or to a computer that pretended to be a person. If the test subjects couldn't tell the difference between man and machine, i. e. that they couldn't make a correct judgment in half of the cases, the computer could be said to be intelligent.

This test was rather quickly subject to criticism by way of a theory called The Chinese Room. This entailed running the Turing Test in Chinese, with a Chinese-speaking person at one terminal and a person that didn't speak Chinese at the other. For the non-Chinese person to have a chance to answer the questions posed by the Chinese-speaker, he/she was to be presented with set of rules consisting of symbols, grammar, etc., through which sensible answers could be formulated without the subject knowing an ounce of Chinese. By simply performing lookups in tables and books it would seem like the person in fact spoke Chinese and was intelligent, although he or she was just following a set of rules. The little slave running back and forth, interpreting the Chinese-speaker's questions without knowing anything, was compared to the hardware of the computer, the machine. The books and the rules for responding constituted the software, or the computer program. In this way, it was argued that the computer couldn't be intelligent, but rather only capable of following given instructions.

However, it turned out that this objection was false. The one that the Chinese-speaker is communicating with is not solely the person sitting at the other end, but the entire system, including the terminal, books, rule sets, etc., that the poor stressed-out fellow in the other room used to formulate answers. Even if the person sitting at the other end of the line was not intelligent, the system as a whole was intelligent. The same goes for a computer: even if the machine or the program is intelligent in itself, the entire system of machine + program very well could be. The case is the same for a human - a single neuron in the brain is not intelligent. Not even entire parts of the brain, or the

brain itself, are intelligent, since they cannot communicate. The system of a person with both a body and a brain, however, can be intelligent![4]

From this follows the slightly unpleasant realization that every intelligent system must constantly process information in order to stay intelligent. We have to accept sensory input and in some way respond to it to properly be called intelligent. A human without the ability to receive or express information is therefore not intelligent! A flow of information is an indication of the presence of intelligence. From this stems the concept of brain deat - a human without intelligence is not a human.

We might finish this chapter by defining what intelligence really is (according to Walleij): Intelligence is the ability to create, within a seemingly chaotic flow of information, systems for the purpose of sorting and evaluating this flow, and at the same time incessantly revise and break down these systems in order to create new ones. (Note that this definition is paradoxical, since it describes the very process by which the author was able to formulate it. You can't win… :)

---

1. Probably a form of structuralism.

2. "Correct" is always a vague term in the field of philosophy. Don't take it too literally, and keep in mind that this is popular science...

3. Theories which are now out of favor with the established authorities. Oh well. Enimvero di no quasi pilas homines habent.

4. Or maybe not. It is impossible for a person to become intelligent without the society that surrounds her, and therefore it is the system of human + society that is intelligent… etc. etc

Chapter 12
VIRTUAL REALITY

I will now talk about something that is horribly overestimated, but inevitably influential when it comes to the future - at least when viewed as a phenomenon. I hesitated for a long time before deciding to include virtual reality (VR) in this book, but I realized that it obviously belonged to the subject of electronic culture. The reason for my hesitancy is that this area of research has been so hyped up and misunderstood that it has assumed almost religious proportions.

Virtual reality was originally a term that meant imagined reality. It's the same sort of reality that role-playing enthusiasts occupy when they navigate an imaginary world. In its original form, this artificial environment requires a considerable degree of imagination and patience. VR has progressed from traditional pen-and-paper role-playing games to interactive role-playing games on the Internet, so-called **MUD**s (Multi-User Dungeons), and not until the 90's did the term become synonymous with the technology that allows the creation of realities using computer-generated sound and graphics. In a MUD, a certaain protocol is established in order to communicate directly with other people, which uses a language that is an extension of the written word. It is possible to state which way one wishes to communicate with a fellow player. For example, one can make clear the one wishes an utterance to be taken ironically, coldly, or erotically. One could write: "Say 'hiya!' in a humorous manner to X", by which X receives a message like this: "Y says 'hiya!' to you in a humorous manner". It is also possible to strike poses, and to emote feelings. You might receive a message such as: "Y smiles an ironic smile".

This mode of communication over the Internet has had a decisive influence on the language that is used in written debate in the electronic universe. The most well-known conventions include the sign for humor, :-) (a smiley-face, sideways), and the sign for irony, ;-) (a winking smiley-face), as well as writing in ALL CAPITALS to indicate shouting. In addition to these, a slew of more or less commonly accepted symbols has arisen. This is the first step towards network-based transmission of symbols with another meaning than the purely linguistic. It creates the first possibility of using "tone of voice" and body language in artificial worlds.

IRC (Internet Relay Chat) is an extension of MUDs. It is possible to do pretty much the same things in IRC as on a MUD, except it's a little closer to reality. Some set up private IRC conferences and chat within an exclusive group, while others spend their time on some of the many open groups, such as #Sweden, which works sort of like a text version of phone chat, for Swedish speakers. Today, about 1,000 Swedes use IRC on a regular basis.[(1)] IRC has a rigid technocratic hierarchy in which those who know more about the system have more power, and can push other people around about as much as they please. Democracy doesn't exist: on every channel there's a number of "royalty" (so-called chan-ops, or channel operators) who sometimes "fight" for control over the channel. In IRC there is also the possibility of conducting information trading, which entails trading information using one simple command: */dcc send nick file*. IRC has already developed into a subculture, with its own values and pecking orders. A surprising number of women use IRC.

This technology is just the first step of a progression that will take us to infinitely more sophisticated forms of communication than we know today. In experimental facilities, the imaginary environments become more and more real, so much that many have started to question the difference between real and imaginary reality, concluding that it is mostly a matter of definition. But let's start at the beginning.

No single person has been more important to virtual reality as **Jaron Lanier**. Jaron moved to California in 1981, with the intention of living as a hippie and playing the flute on the streets. Instead, he stumbled into a job as computer game programmer. After some time in the field, he started a company called **VPL** (Visual Programming Languages) with his own money and started a non-profit project which involved developing a programming language. Programming languages are the languages that people use to communicate with computers and tell them what to do, Examples of common programming languages include BASIC (Beginners All-purpose Symbolic Instruction Code), Pascal (after the mathematician of the same name), and C (named by someone who thought the naming conventions for programming languages had gotten out of hand).

Now, Jaron didn't want to write any old programming language, but THE programming language. He thought programming was one of the most fun things he knew, but it was reserved for an all-too-small group of people. He thought everyone should be able to program. Instead of just allowing a tiny elite of programmers to build mathematical and symbolic models of reality, he wanted to place this tool in the hands of the common man, with a minimal amount of prerequisite knowledge. The language was finally named *Mandala*.

Many people that try using a computer for the first time thinks the whole thing is too abstract and contains too many theoretical concepts. A computer student I had once said:

> *"You can tell me that this here is a command, and that it has this and that property and works in such and such a way. It's like telling me that this is a hammer, and it works like so. I'll never understand unless I get to hold the hammer."*

He hit the nail on the head. If people won't adapt to computers, then computers would have to adapt to people. If Mohammed won't come to the mountain, the mountain will have to come to Mohammed. That was Jaron's idea: make the computing environment as real as possible, remove that keyboard if it causes so much frustration, and take away that two-dimensional screen if flat symbols are so hard to understand. Create an entire reality around the user so that he or she feels at home. The concept of virtual reality was born. Of course, this idea was not entirely new. The first time the concept of VR came up was supposedly in 1965, through **Ivan Sutherland** at Utah university. But Jaron was the first one to try to realize these ideas, and make *money* off them.

VPL was founded in 1985. Since then, nothing's been the same. In 1991, us regular people made our first acquaintance with VR as **W Industries** released its computer game *Virtuality* everywhere. Newspapers, radio, TV - everyone told the story about this new and fantastic invention. It was also at thaat time that people started making comparisons to William Gibson's novel, *Neuromancer*, and discovered obvious

similarities between the way the lead character, Case, connected his brain to a computer to enter cyberspace, and the gols of VR. That was when people seriously started questioning the direction our society was heading, and it is also among the reasons that William Gibson is such an important writer.

All of it is not as strange as it is sometimes presented. By applying sensors to the body that register all its movements, the computer can sense how you move about and then generate sound and visual impressions that agree with the way we're used to perceiving reality. The sound is created by a quadrophonic sound system that allows us to place sound spatially, and images are displayed three-dimensinally since the computer draws an image for each eye. This is VR today; no more, no less. Objects can be perceived as three-dimensional and sounds can be generated as to make us think they came from the object in question. Nothing strange there, just normal manipulation of our sensory capacities, just like a computer screen or a loudspeaker, only more sophisticated and refined. Machine-generated hallucinations or tangible dreams are other possible terms for the technique.

Jaron, then, envisioned VR as a form of programming language, primarily intended for creating models to facilitate research and education, and to make the capacities of the computer more accessible. This is not exactly how it turned out. Some inventions have the ability to shock their inventors by turning out to have applications far wider in scope than the inventor could ever dream about. Nuclear power is probably the most frightening example of this. VR was transformed from a programming language into a *medium*.

We have a handful of media in our society. We have various sorts of literature. We have theater and film. We have radio and television. We also have *multimedia*, like computer games and *hypertext*, which is a kind of improved text that allows us to read textlike a database instead of like a book. And now we have VR, and that too is a form of medium. More specifically, it is the most powerful medium that humankind has ever created. VR envelops you in all dimensions and commands your complete attention, just as if it was your real life that was involved. You can run, but you *cannot possibly hide* from it. (Imagine what a fascinating medium for commercials: Depends diapers chase you into a corner and suffocate you to death.)

When Jaron was well underway with his project, he realized that he needed help to complete it. He enlisted the aid of the MIT media lab, which had already helped in enlightening the world through the *graphical interface*. (An interface is the set of things that exist as a bridge between the computer and the user, like the screen and the mouse). This was later to be used by Xerox, Macintosh, and Microsoft (in that order), and we nowadays know it under such product names as *System 7* and *Windows*. The military got into the action, as usual. They had already experimented with flight simulators to train pilots before sending them into action. VR was viewed as a possibility of improving the simulators, and even to develop very accurate systems for *remote presence*, in which a pilot might be able to steer a plane into enemy territory while physically being located in a bunker back home in HQ. Such a system would be an economical way of maintaining pilot ranks, as well as permitting them to build planes that could stand physical stress way beyond the tolerance of any human pilot. Like RC planes, but cooler (and much more dangerous). Therefore, the military blew

a huge load of money on VR research. War, as always, has a way of making technological research move by quantum leaps and bounds.

It's difficult to say what importance VR will have in the future, In a way , it changes nothing - we all experience VR every night, in dreaming. The difference is that in VR we can control the content, and employ highly *tangible* dreams for our own purposes. One of the greatest areas of VR application is therefore in psychology, since dreams has a primary importance in the study of the human mind. It is quite reasonable to expect VR to be used in very sophisticated therapy. *Or* brainwashing, if that's what's desired. Brainwashing is not always a negative thing; in inpatient psychiatric care, rapists and killers are treated with a very advanced form of brainwashing to cure pathological behaviors. Such care can certainly be improved and become more effective with VR. Conversely, VR can be abused.

As a medium, VR holds enormous potential. When we communicate across electronic links, we don't feel as if we actually meet someone. The anonymity that goes with a telephone receiver allows us to spit out the most daring utterances, since we don't feel physically intimidated. When we speak on the phone, we are constantly distracted by other events in our surroundings. When we communicate via Internet, it is impossible to use any form of real body language or tone of voice. The only way to communicate feelings in an electronic conference is by writing lightning-quick and misspelled sentences to express upset, or using typographical conventions to communicate states of mind.

In VR, we can use as much body language as we want to. We can make the encounter totally similar to reality, as if we were meeting in the same room. We can make it *more* than real - we can inflate ourselves to twice our size if we want. We can disguise ourselves as anyone, and decide exactly what the room should look like. I can experience it as if we're at your place, and you could feel as if you were at my place. We can actually be in two places at once, so that both of us feel at home! (Translator's note: the old line that goes "your place or mine" would become obsolete.). I could be at a steel mill, with the noise in the background, and you can be in the forest listening to the birds singing. I think you're sitting on a treestump, and you think I'm sitting on an anvil. Anything's possible.

In sociology, the science that studies the relations between humans, the concept of *symbols* is used to denote that exchange of information between people that goes deeper than language. As opposed to language, such symbolisms cannot at present be stored or synthesized. This is one reason for inventing written languages. A language that can be stored enables a cultural heritage that spans generations, and gives humanity a so-called *collective consciousness*. The concept of a *symbol* includes, in addition to spoken and written language, body language such as glances and involuntary movements (in linguistics, gestures and such are called *paralinguistics*).

Symbolic language between people consists of genetic as well as learned components. Animals that cannot speak or write communicate exclusively through "primitive" symbolisms of the sort I just mentioned. Symbols can be thought of as the bonds that tie people together in groups, societies, and entire systems of societies. Not unexpectedly, symbols figure heavily in AI research; most AI researchers view all of a person's consciousness as the construct of a flow of symbols in one form or another,

and intelligence itself as one great information-processing system. (But I've already talked about that…)

The goal of virtual reality is that all symbols should be able to be stored and synthesized. It's supposed to become the perfect medium of communication between people - even better than reality. And this is perhaps what makes it so frightening. The computer offers the possibility of twisting symbolic language. If you control the computer, you could use it to appear as great and conceited as possible, and your own picture of reality would be distorted so that other people appeared as dorks. The line between illusion and reality could become fuzzy indeed.

It is completely impossible to predict what this would do to our way of perceiving the world, and other persons in particular; the only thing that's certain is that it *will* change. Sometimes, people speak of the cultural or sociological *atomic bomb*, where VR is a threat that could destroy all our norms or even our entire perception of reality. Any prediction in this field at present must be considered pure speculation, since no one communicates by VR to any great degree.

However, sci-fi authors already warn us of the dangers of VR. One of the first examples is Philip K. Dick's short story called *Wholesale Memories*, later made into the movie *Total Recall*, and other examples include the *Illuminatus!*[(2)] trilogy, our beloved *X-Files*, and the movie *Videodrome* (1982). All of these are based on the horrific scenario of not knowing what is real and what is imagined[(3)] - in other words, *paranoia* based on reality. I have myself written a short story in this vein, and begun another which I never completed:

> *"Sometime that year, a group of eager scientists inserted the first Carcer chip into the skull of a deaf-dumb and quadraplegic test subject. When the affluent layers of society gradually migrated towards a better, artificial world, these slaves, people whose will would never make itself known due to the iron grip of the Carcer chip, would be left behind to run the power plants, the farms, the food processing plants, and all the other necessary societal institutions.*
>
> *Many free persons understood that the Carcer project was inhumane fromk beginning to end, that the people in the bonds of the chip no longer had a will of their own. Yet they were reluctant to leave the material well-being that they had built for years in a world that didn't exist. Their brains were connected to the machines by electrodes, and their peripheral nervous systems with its arms, legs, and eyes, were disconnected. Physically, they lived out their days suspended in a tank filled with isolating liquid kept at body temperature.*
>
> *The freedom of a number of less privileged individuals was worth sacrificing for the free men and women that now lived in invulnerable bodies made of data, and who mentally controlled political events. (...bla bla bla)"*

But - to be honest - don't worry. People are rather sensible beings, all things considered. There is no reason to suspect that we wouldn't be able to exploit this new

resource in a reasonable fashion. However, virtual reality in combination with AI gives us a new picture of the importance of human beings vs. society, which is the subject of chapter 15.

---

1. This number is constantly rocketing upwards.

2. Fredric Jameson has claimed that the entire cyberpunk/tech noir genre is simply a reformulation of the theme illustrated in *Illuminatus!*, which is a global network of interwoven organizations and informal circles (which actually exist in some form) described as a metaphor inside the computer - the electonic network. The incomprehensible electronic organism becomes a model for the incomprehensible power. I don't agree. The computer is fascinating in itself, and one is not a symbol for the other. Possibly, you could view the two as an important concept-pair.

3. One philosopher who's written a great deal about the dissolution of reality in a kind of "virtual reality" or "hyperreality" goes by the name Jean Baudrillard.

Chapter 13
NET-ATTITUDES, TECHNOCRACY, AND DEMOCRACY

Selling and owning information is a profession today. Journalists, PR professionals, consultants, and lobbyists base a large portion of their professional pride on the *ownership* of information. Naturally, they don't want to share their information unless they get something in exchange, and the things we give them in exchange are decent salaries and social status. Their professions are at risk of being fundamentally changed by information technology, and many of them are aware of this. How?

At MIT, the first hackers left their programs (in the form of long strips of paper with holes in them) lying in a box next to the computer. They did this partly so that whoever wanted to could examine them, but also so that whoever felt like it would be able to improve and expand the programs. This open-hearted attitude is an example of typical "hacker mentality", and has since then characterized almost all research and program development that has taken place over the Internet. This falls under *Rule 1* in the chapter about cyberpunk: the *hands-on imperative*.

There are lots of programs that have been developed according to a principle called *Stone Soup*. This is one of the oldest - if not *the* oldest - methods in software development. The first hackers at MIT, in the 60'd, worked according to this principle. Today it works like this: a programmer manufactures the core of the project, a working program that provides the *foundation* for the end product (the stone in the soup). The programmer then puts the program on the Internet and tells all the amateur programmers out there: *"Here's the program - if you find any faults and know how to fix them, then please do so. Then send the changes back to me."*

The original programmer then assumes the role of editor, accepting suggestions and constantly adding to and modifying the program. The end product is then distributed for free. The PC programs *Fractint* and *Pretty Good Privacy* (PGP) are just two of the great mass of programs that have been created in this manner. Even if an amateur may not be able to accomplish a lot by him- or herself, he or she is still often an expert at *something*.

One of the first stone soup programs that was really successful was **Tiny BASIC**, a competitor of Bill Gates' Altair BASIC, which managed to stand out by being much better than Gates' BASIC, and *free.* (Guess if that was a thorn in the side to some people). Among modern stone soup products there are entire operating systems such as **Linux** (a project started by **Linus Torvalds** at Helsinki University, referred to by many as the most successful hacking project of all time), **X-Windows**, and the **EMACS** text editor, used in making countless textbooks and college essays. All of these programs are free.

The communications protocol stack called **TCP/IP** (Transfer Control Protocol/Internet Protocol), which is about to conquer the entire market for network communications, is also stone soup. (It is used to make computers "understand" each other when "talking" over a network - TCP/IP is to a computer as a telephone receiver

and a dial is to a person). This protocol stack is judged by those who develop the Internet, and is constantly revised and improved as the "editors" send out *RFC*s (Request for Comments). TCP/IP is completely free, and no one has made money from its invention. It has (without any marketing whatsoever) become so huge simply because no one is fighting over copyrights or trying to keep "commercial secrets" to themselves. On the other hand, it's not hard to make lots of money from the *knowledge* of how TCP/IP works. The knowledge about the product is therefore of greater value to the market than the product itself. This is why some of the people who know TCP/IP are very secretive about their knowledge, in order to maintain a demand for consulting services.

The companies that are marketing their own communications protocols are naturally displeased about this. That's why they gladly disseminate lies which claim that TCP/IP is of poor quality - even that it's bad and worthless. The most common argument is *"the more cooks, the worse the soup"* - which means that a lot useless junk supposedly makes it into the programs. This is patently false. The discussion groups evaluate every proposed change before it is incorporated. It's a shame that such rumors are sometimes published in major newspapers and magazines (none mentioned, none forgotten). I prefer to listen to experts like **Peter Schaeffer** who know what they're talking about.

At the front of the defenders of this fundamental technological principle there are people like **Richard Stallman**, a former MIT hacker who referred to himself for a while as the last real hacker. He established the foundation for **GNU** as well as **EMACS**, and his point of view is that software shouldn't be subject to ownership. He is also an influential force behind the *Free Software Foundation*, which is an organization that primarily concerns itself with the promotion of free software. He has had many software companies up in arms over his method of copying ideas without copying program code, which is known as *reverse engineering* or simply *deconstruction*. It involves analyzing a program on an object (machine-code) level, noting its functions, and then creating a program that performs the same tasks. Stallman's productivity in this respect is so legendary that he is referred to as perhaps the greatest and most motivated hacker ever, and fully capable of doing the job of an entire development team on his own. He has also had an influential role in the organization *League for Programming Freedom*, which has as its mission the liberation of software from patents.

Stone soup software also has the advantage of being easily modified or analyzed in order to find out *exactly* how it works, since all documentation is accessible to whoever wants it. This is in contrast to software that's been manufactured by corporations, which lock source code and documentation in a vault and charge exorbitant prices to share their knowledge when a problem occurs. The intention is that the user should think that the program is so incredibly fantastic that only the in-house programmers (which are presented as some kind of wizards) are able to understand and improve the program. Talk about a monopoly on information.

Well.

Imagine the stone soup principle being applied to a piece of text, like the one you're reading now. If I had access to an Internet server, I could put this document in

hypertext form (which is a kind of text invented by **Tim Berners-Lee** subsequent to an idea put forth by **Ted Nelson**, in which consistent subjects or general keywords are electronically linked in order to allow the reader to quickly jump to different points in the text) and put something like this at the end:

> *"All of you who are reading this - send in revisions and addenda to me, and I'll put them in the text."*

It's all free. Anyone could get the document off the Internet. I don't profit from it except for gaining knowledge, and no one else does either. If my document became popular and reached a wide audience, a few experts would (with some luck) contact me with corrections and additions. Not much, but just enough to cover the subject on which that person is an expert. Then, I could assume the role of editor and collate all of this information, put new links in the hypertext and facilitate searching and notices of updates to the text. I would feel that I was doing something useful, but I wouldn't be able to earn a living doing it. After a few years, my document would become an entire database covering almost every aspect of computer culture, more comprehensive, editable, and thorough than any national encyclopaedia, and furthermore it would be written at the grassroots level by people who love what they do.

So why don't I?

Answer: first of all, I don't have the time or energy.[(1)] Second, it is not a matter of solving a technical problem like those in a computer program; this text is multi-faceted and highly subjective. It bears the mark of my own values and judgments, and I want it to remain as such in the future. Every word is written by *myself* and no one else. Call it pride. Further, it has a beginning and an end, and it is possible to critique it as something coherent and static, not as something that is constantly morphing. It is possible to form a *clear* view of the text that lasts a few days, and this is the advantage of the statically fixed text versus the ever-changing one.

If this were a practical problem of a technical character within any of the natural sciences or medicine, the situation would be radically different. Such hypertext documents are created around the world as we speak. They grow together, forming a world of information, accessible to anyone, anywhere, who has access to the Internet. It's known as the World Wide Web (WWW). By extension, the human *hypertextual heritage* will grow into a mass of information of such mammoth proportion that it will be impossible to get one's mind around it. It will be like a library of memories for all of humankind. Hypertext is also changing more and more into *program code*, which erodes the distinction between regular, literary text and computer programs. The professions of author and programmer blend together. This is what multimedia *is.* The tools used to create multimedia products are not called computer languages, they're called *authoring programs*.

Some authors of fiction have adopted the idea of publishing their creations for a wide audience, on the Internet. Since fictional writers generally want their works to be read and only incidentally to make money, this is a natural step. The first well-established author to put some of his work on the Internet was **Stephen King**, on September 19, 1993. Many other authors thought this was a great idea, and published some of their

older books on the Web. In Sweden, **Lars Fimmerstad** was the pioneer in this aspect, with his novel *Välkommen Hem* ("Welcome Home"), and shortly thereafter **Ola Larsmo** followed in his footsteps with his short story, *Stumheten* ("The Speechlessness"). The more established an author is, the more conservatively he or she approaches electronic publication. To a certain extent they live off their book sales, and feel threatened by a form of publication through which they cannot yet get paid.

This progress within media is in step with the trends in organizations, which are being transformed into networks - loosely connected associations without staff or representatives, established for the purpose of answering one single question or solving one specific and well-defined problem (making stone soup), and that have so far stayed connected through mail correspondence and phone calls (exchanges of information). Do not confuse a "network" with a "computer network", even if many "networks" employ "computer networks". Your local bridge club is a "network", and the Internet is a "computer network". A common denominator of all networks is that they distribute information of some kind. (Confusing?) Mnemonic device: bridge club = a network of people, the Internet = a network of computers.

So what's the point of all this?

Well, it is that network documents will quickly become so numerous that it will be impossible to get an overview of them. Therefore, it is (as always) necessary to go through a long and hard learning process, *or* hire a consultant, to access a specific piece of knowledge. A typical consultant is a watch group that cover some specific area of interest, which we usually refer to as the technical press, only in this context it's electronic. The need for specialized journalism therefore exists in the information society as well. At the time of this writing, such journals cannot get paid for their information services, but a system is under development. That means that you will be able to *buy* information about anything using your own computer. Naturally, you don't pay with cash, but with numbers.

These technical journalists will basically become the first people to earn their living solely by processing information; they'll be the first ones to enter into the total information economy. The other papers will follow, one by one. Some newspapers, such as **Aftonbladet/Kultur** (a major Swedish evening paper) have anticipated this, and are preparing themselves for the entry into the information economy by experimenting with electronic editions. Other papers remain content with simply publishing electronic complements to their printed material. (In the experimental stage, all of this is free! Grab the chance now that you have it, because it won't come back). In addition to this, and as a natural consequence of it, we'll get a huge number of electronic fanzines[(2)], due to the amazing *simplicity and cheapness* of making an electronic publication. (The hacker culture has spawned hundreds or maybe even thousands of such magazines.) No printing costs, no contracts, no advertisers, just information and motivation. Culture without biznizz.

Cynically speaking, journalists are experts at information trading. It's probably the only profession that even before the time of computers made a living solely by producing and processing information. *Journalists* do *not* think that information, and therefore knowledge, should be free and universally accessible. On the contrary, each

journalist (at least each specialized journalist) jealously guard "their" information sources, not revealing them without very good reason. The journalist is just as conservative and stingy as the elitist and sectarian hacker groups. *For the public good* is one thing - but even journalists have to eat. It's about protecting one's intellectual property. The truth is that the fourth state, just like the government and the corporate world, also consists of personal contact networks and hierarchies in which string-pulling ability is very important. Even journalists are totally ignorant of hacker ethics, which to a high degree influences their reporting when it comes to hackers.
The guidelines surrounding electronic publishing indicate the emergence of two new types of media. One will be stored on CD-ROM disks and will contain huge stores of knowledge, such as a database or a searchable encyclopaedia. **Interface** magazine was first in Sweden to try this. The other type is *Online Services*, which provide news and information updated daily, hourly, or even more frequently. The first Swedish online service was probably **Text-TV**. The first Swedish online magazine on the Internet was **Datateknik**.[(3)] At the moment, it is not possible to charge for online services, but that capacity is on its way.

In the long term, CD-ROMs will run into problems. It will soon be very easy to copy the disks, so why should I buy the paper, the encyclopaedia, the dictionary, or whatever, when I can copy it off my neighbor? Once you try to protect the information from being copied, you can bet your ass that some hackers will come around and crack the protection and copy it anyway. Online services don't really suffer from this problem.[(4)] Some prophecy the total disappearance of disks in favor of online services, but this is unlikely to happen soon. The need to own the physical form of something, like a compact disk or a print magazine is still strong in our generation.

Others say that mass media will disappear. That depends on how you look at it. Mass media *as it is today* will certainly go away, but we will also equally certainly get a new definition of mass media. Print publications will most likely remain until we find a way to make electronic information as portable, but that day will come.

The magazine called *The Whole Earth Review* has aroused public interest in electronic media in the USA. The popular magazine *Wired*, which I mentioned earlier, is one of the publications that have received a boost from the progress at the electronic frontier. This paper has become extremely popular, not least due to its youthful layout. It has paved the way for several similar magazines across the world, such as Sweden's **Z Mag@zine** and **Hallå**, which have apparently gotten their whole business idea from magazines like Wired. They write about the Internet, BBSs, everything falling into the category of media and information technology, and fashion and trends. Both publications have (intentionally) refused to acknowledge the existence of the other. Both are currently out of print, but Hallå is restarting soon.

Other American magazines that seem to be great sources of inspiration for this type of media are **RayGun** and **Gray Areas**. **MONDO 2000** is a tad too provocative for the more distinguished circles, as it has a rather conspicuous air of hippie and yippie philosophy. Some people are irritated by these magazines, since they write mostly about each other (media writing about other media, journalists about other journalists, etc.) Seeking a cause for this, one would most likely conclude that media products are changing due to the entrance of information technology. Text and images are

becoming easier to edit and distribute, and the purpose of journalists is under re-evaluation, etc. It's also not surprising that journalism is of interest to journalists. With the role of media as the "fourth state", critiquing itself is probably necessary function. To spice it up, the subjects are often things that are exciting in real life. Preferably hacking, of course. They're the ultra-hyped spearhead of the "information revolution".

The *hackers* don't think these magazines are anything special (as the publications seem to think themselves sometimes), but rather refer to them bluntly as *hacker-wannabes* - trying to write as if they're something they're not. Sweden, for example, is full of Schyffert-wannabes, Guillou-wannabes, and Bildt-wannabes. (As for myself, I'm a Visionary-wannabe ;). The frequent use of trite terms like *cyber, powerful, IT*, and *(insert latest catch-phrase here)* is a common denominator for hacker-wannabes, plus that they use Macintosh computers. (Translator's note: *HEY! What the hell do you think I started translating this text on?*).

The tendency of aggressive competition among hackers is similar to the brutal reality of everyday journalism, and this is probably the reason that these magazines inherit hacker culture and ideals. Few of these journalists seem to understand the friendly, non-American part of hacker culture, which is not as interesting since it's not as illegal, contains much less confrontation, and built more on friendship than competition. This is of course not so strange, since journalists love conflict and in many cases spur it on. (Conflicts inspire *great* headlines, and attract readers.)

Technocracy

The Internet is often referred to as "anarchistic". This is a gross exaggeration. The Internet is fundamentally *technocratic* and *decentralized.* As it was first built, by the university hackers, they wove some of their open-minded attitudes into the web of the Internet. Remember Rule #3 of hacker ethics: *Distrust authority - promote decentralization.* That is: *if I help you, you help me*, and nowhere in the core structure of the Internet was there a function for charging each other for the use of communication channels. There were no locked doors, since it was held that everyone should be able to access anything and share their information. (Rule #2: *All information should be free*.) Just jack in and go. The only things to pay for were the constant phone line connections on which the information flowed, and then you could communicate as much as you wanted.

The entire network has been built using the stone soup principle. Every problem that occurs is posted on discussion groups, after which anyone who wants to may suggest a solution. The users are very eager to help, and usually there are a number of proposed solutions. The proposals are evaluated in the discussion group, and the one that's considered to be the best wins. The result is documented and then distributed as a *de facto* standard. This technocratic method of problem-solving is radically different from the market model. In a market economy, companies *compete* for the best solution. Each company has an R&D division that develop a solution, which is then marketed. After that, consumers judge the products by buying the one that suits them the most. The "bad" solutions are thrown out as the companies that fail to get enough market share discontinue their productmaking and buy patents from the successful companies, or, at worst, go bankrupt. In this manner it is suggested that the best product always survives.[5] (Translator's note: it's also highly circular, as the "market" judges the "marketing and marketability" of a "marketed" product).

The problem is that the winning solutions in a market economy aren't always *technically superior*. They might as well be the *best marketed* or *cheapest* products. For example, reflect on how the VHS video system beat the technically superior Betamax system. (According to legend, this was ultimately due to the fact that the VHS format was marketed by the adult video industry…. hmmm.)[(6)] (*Translator's note:* How about Windows...). This would never happen in a technocracy like the Internet. A technocracy doesn't allow marketing or arbitrariness to send a good idea into the wastebasket of history. It's pretty typical for the universities to build a technocratic network, since their main goal is always technological progress.

In a market economy, it is the *carrot* of personal gain and wealth that drive the businesspeople to develop better and better products. In a technocracy, it's personal commitment, fellowship, and the desire to advance knowledge that drives the developers. With the Internet, this attitude towards research and product development has spread across the world, and sometimes it generates solutions that completely beat out those of the market economy. It's not a planned economy, since there's no single authority that finances and evaluates the products. It's a technocracy, based upon individuals in voluntary cooperation.

In addition to the university researchers, who thanks to secure personal finances are able to dedicate themselves to solving Internet problems at work, many people employed at regular market-driven companies have started developing solutions to different technical problems on their own private time. The desire to show one's competence in a technical field, and to be accepted as a skilled developer among others on the Net, has been enough to motivate these people to develop technical solutions. Call it the joy of working or professional pride. (Yes, these still exist even in our time).

Whether technocracy is a threat or a complement to a market economy is hard to predict. Perhaps we're entering a form of *knowledge economy*. It is, however, clear that with internationalization and the ability to work in small interest groups across great distances, we have found a so-called "nonprofit" force that enables us to perform practical work and have fun at the same time. Group fellowship is the same as that among the hackers, who have long been exchanging experience through letters, BBSs, copy parties, and the Internet. The only difference is that one form is more "respectable" than the other.

As I suggested earlier, it's possible to detect an anarchistic ideological heritage within technocracy. **Peter Krapotkin** thought that society should be run through the cooperative efforts of independent groups. As opposed to **Charles Darwin**, who thought that races (and by extension, society) evolved through competition, Kropotkin emphasized the important role of *cooperation* in the building of a society. The Internet technocracy is in some ways proof that free groups independently set up cooperative relationships without governmental influence. The *virtual society* is anarchistic, in this way. At the same time, there *is* an aspect of Darwinism, in that only the best solutions survive. The difference is that this happens as a result of mutual agreement and doesn't affect any people or companies in a negative manner.

A Few Examples

I once (in my foolish youth) wrote an opinion piece and sent it to Datateknik

magazine (a Swedish computer publication). In this piece, I lamented the poor availability of digitized (machine-readable, stored in a computer or on disks) literature, and the fact that our cultural heritage wasn't properly electronically stored. I suggested that publishers should be forced to make non-copyrighted material available to the public, every time they re-printed older literary works. I received a well-motivated and angry reply by **Lars Aronsson**, project leader for *Projekt Runeberg*, which electronically publishes Swedish literature. In my naïve excitement, I'd simply been thinking practically, and overlooked the market aspects of the whole thing.

Digitized text is of course a competitive advantage during re-printing, and my proposal could hurt the competitive power of a certain company. Another company could (if my system was applied) steal the text directly from the publisher and publish the same book as a new edition, which would lead to a loss for the first company which had paid to have someone enter the text in a word processor.
The fact remains that it is a waste of human resources to let several people carry out the monotonous task of re-entering the same text over and over, instead of storing it in a central location and making it accessible to everyone - companies as well as individuals. This is one of the disadvantages of the market economy, which technocracy is trying to address: the market economy sometimes demands wasting natural resources and duplicating work efforts. You could make an analogy with the development of the mobile phone networks, where several small, incompatible networks are being built instead of one large, stable, and widely adaptable network. Call it greed or competition - but it's *not* cost-effective.

Naturally, this wastefulness is actually *a good thing* according to our classical yardstick of the public good. GNP increases, and people get something to do (work). One should, however, ask if people fare well from this. We're living in a time in which the quality of life is measured by socioeconomic number-juggling. Is it a good idea to create problems to make jobs for problem-solvers? To provoke crime in order to employ crime attorneys and investigators?

The technocrats on the Internet, spearheaded by League for Programming Freedom, hold the view that good knowledge should not be subject to patent. The companies, however, do. There's already been open conflict between idealists and profit-hungry corporate people. I've already touched upon the negative rumors spread about "stone soup software". Another example is the fighting over a compression method known as LZW, which is simply a modification of a public-domain method called LZ2, which originated at Jerusalem University. Basically, companies can possess so much chutzpah that they take out patents on methods, developed by idealists, which were originally intended to be public domain. Companies also have the time and money to sue…

Another direct example of the difference between market-driven and idealistic thinking is the way various commercial firms are fighting over email services through the Internet. Swedish Telia has had a taste of technocracy. The background is as follows: Telia has no problem getting access to the Internet. The problem is that Telia wants to decide how certain Internet addresses should appear. It's always a good thing to be able to butter up your customers with a custom, easily memorized number (Like Swedish Railways' 020-75 75 75) *Sadly*, Telia is not in charge of these things on the

Internet. The principle is that all commercial domains on the Internet should have the -COM suffix, as in COMmercial. Instead, Telia wants to give companies the 400NET prefix, which happens to be the name of their commercial electronic mail system.

Bernt Allonen at Telia says this in Z-mag@zine, 1/95: *"It's time for the Internet to leave the sandbox… the Internet is in need of strict rules and operators that guarantee performance."* With this he's probably tried to say that the Internet should be market-driven, like a company - as opposed to the reality of its current operational mode, namely non-profit/academic - with all its implications, like rigid bureaucracy, market planning, and little hierarchies in which the golden rule is: kick downwards, kiss upwards.[(7)] Mostly, he would like to see Telia assuming total control of Internet distribution in Sweden, so that things could become *orderly*. This is not the case, and hopefully never will be. Who really cares what Bernt Allonen thinks? He only represents the expansionist interests of a single large corporation.

The people who hold the most power over the Internet in Sweden are **Björn Eriksen** and **Peter Löthberg**. Both are representatives of the open, technocratic attitude, and Björn decides which *domains* (Internet names or addresses) can be created on the Swedish part of the Internet. To the great chagrin of Telia, their market plans have no effect whatsoever on these academicians. The Internet *cannot be bought!* May Heaven have mercy. The academicians are not at all concerned about "orderliness" on the Internet. In their eyes, the Internet primarily exists to be *useful,* not *marketable*. Is it a good idea to tell Telia that all these idealists and academicians have actually succeeded in building the world's *largest* computer network *completely without competition, market analysis, and commercial ad campaigns?* Now that Telia's X.400-network hasn't been as successful as the Internet, what is Telia to do? Well, of course they want the rights to the Internet. Normally, a giant corporation like Telia can indiscriminately purchase and take over their competitors.

Thinking people, however, are much harder to purchase. Telia represents the philosophy of the old market theory, which states that people that cannot be bought for money can be bought for *more* money. Internet-users, with the technical universities at the base, have a completely different way of thinking. If there had been anything else than market tactics behind Telia's demands, they might have listened. Fortunately, they prefer to continue thinking. Thanks to this view, no one has a monopoly on the Internet in Sweden. Hundreds of companies are currently fighting to provide Internet access. The competition has pushed prices down to an incredibly low level. An Internet connection is today very affordable for a normal person, and everyone who has decent knowledge of the process can buy some computers and modems and start their own Internet node. Variety as opposed to monopoly. From this point of view, the Internet promotes small operators and resists the efforts of giant corporations. Again, refer to Rule #3 of hacker ethics: decentralization.

Rule #3 is also one of the reasons that cyberpunks and others work against **Microsoft**, and especially its operating system, *Windows*. When hundreds of hackers were arrested during *Operation Sundevil*, it was because law enforcement thought that hackers were behind the collapse in the American telephone system on January 15, 1990. Now, it turned out that hackers had nothing to do with it. Instead, the collapse was due to an error in the *computer program* that controlled the switches. The problem was exacerbated by the fact that the program was used everywhere, and the

switches "brought each other down". The only switches that worked fine were those that used another, older program.

Microsoft's Windows is also a program, and more specifically, an operating system, which means that it's a program that is used to enable the user to run other programs. Today, it is installed on virtually every PC computer that is sold in Sweden. Most programs today require Windows in order to function. Therefore, Windows is used by innumerable private companies and governmental organizations, including Swedish Railways and the Swedish *national defense*. Recently, a new version of Windows, called *Windows 95*, was released. [(8)] This will, among other things, be used to provide easy connections between several computers, over the Internet and other networks.

Now, what if there was an error similar to that in the American telephone system's switch software - but inside *Windows 95?* In that case, every computer that used Windows 95 would crash. There is no way to prove empirically that a computer program is free of such errors. It's thus entirely possible -and it's happened before. Such risks exist with other, nearly monopolizing products, such as *Netscape*. A few moronic computer folks might think that it's impossible, but so was Chernobyl and Three Mile Island, so I don't buy that. And by the way, I also know what I'm talking about. (Pardon the conceited and provocative comment).

If something like that happened, large parts of Swedish society would be knocked out. We have a parallel case with the virus that in the fall of 1988 crippled the Internet by putting 6,000 computers out of commission. It was an error in the Berkely-UNIX (BSD) operating system that allowed this virus to be created. Some computers were unaffected by the virus - by virtue of using another "dialect", i.e. another version of UNIX, like NeXT or AIX (there's about 11 different versions of UNIX). UNIX basically works in the same way as Windows[(9)], but there's *only one "dialect" of Windows!* If all computers had used the *same* UNIX in the fall of 1988, well, all of the Internet would have been brought down! I'm stating that this could happen even to Windows 95, or one of its successors. If this happened, all Windows 95 systems could crash, if they were networked. It would be a catastrophe of unpredictable consequences to society.

This is where it's important to emulate nature. *Variety*, in which many *different* programs work side by side, is preferable. Hackers have always proposed variety and decentralization. In the long term, software monopolies are harmful, and lead to problems in computer systems that resemble those that occur with the *inbreeding* of living creatures. The only ones able to compete with Microsoft today is **IBM**, with its OS/2 operating system, and **Apple**, with MacOS. Personally, I look forward to more competition. Variety, decentralization, and small companies instead of giants and institutionalism is the only thing that's sustainable in the long term. Microsoft cannot be allowed to dominate the operating system market. Chaos is fun. And healthy.

The arrests of hackers after the Jan. 1, 1990 incident was a distraction to obscure the inbreeding within the telephone system and the incompetence of large companies by blaming hackers for what was really a structural problem. What are they to be blamed for next?

There are oodles of examples of how the market's been beaten by home-made solutions. Some computer nerds therefore want to stop this spreading disease by trying to stop the publicly financed distribution channels. One such channel is ftp.sunet.se, an Uppsala computer system which stores thousands of quality, free-of-charge programs. This computer is publicly funded and anyone can connect through the Internet and retrieve any of these programs. This is actually a good thing, since all of Sweden's (and the world's) computer enthusiasts gain access to free programs, but it's naturally a thorn in the side to those who promote a dogmatic, capitalist system as a way if life.

> *"The greatest problem with ftp.sunet.se is that it effectively undercuts all attempts to start domestically based software companies… Software is the industry of the future, one that we Swedes would have been able to exploit because of our well-educated populace, if it hadn't been for ftp.sunet.se… But how are such companies' products supposed to compete with programs that are 'free' because they have been subsidized by tax revenues?"*
>
> (**Bertil Jonell**, Z-mag@zine #6, 1995)

Here, we have an obvious conflict with another part of the hacker ethic: *Mistrust authority*. The answer from the established software industry becomes *mistrust hackers*, which is probably justified in the cases that Bertil mentions above. It is, however, hard to justify this mistrust in the case of mission-critical software such as those in airplanes or medical equipment, since it's impossible to find any such programs written by amateurs. The companies that make such equipment are concerned with their reputation, and don't hire just any hobby-hacker for just that reason. Instead, they get their programmers from the more status-filled university education programs.

We shouldn't pay too much attention to what one person has said on one single occasion. We'll instead treat it as an illustrative example. There is a whole set of values that we think is God-given, but that is actually not self-evident at all. It is not an obvious truth that the well-educated engineer is a better builder of electronics than the kid around the corner who's been a radio amateur since he could walk. More accurately, it's a complete untruth. Granted, some enthusiasts migrate to the finer universities and technical schools, but some of them don't like the formal and strict environment they encounter *at all*. They prefer to stay at home in their garages and study and experiment on their own. That kind of *motivation* beats most university education by lengths, when it comes to direct practical knowledge.

Of course, the at-home hacker is usually an individual that isn't very socially adaptable, and who also has a penchant for certain suspicious subcultures. *That* is most likely the *true reason* that these skilled hackers aren't hired for positions where they could do the most good. Instead, they sit at home and put together freeware for any and all. (I've talked about what happens in the worst cases in chapter 4 and 10, about underground hackers and computer crime). A university degree is not only a certificate of competence - it also indicates that its possessor is socially adept and has the ability for discipline and obedience that is required at large corporations. A programmer should have the ability to carry out a project without questioning it. No

large company is interested in employees that think too independently and develop alternative solutions without permission. Instead, every project is controlled from a high position within the hierarchy. In short: a university degree means, in addition to competence, that the bearer has accepted the authority and power structures that exist within companies as well as educational institutions.

Stone soups cooked by enthusiasts, with many rival solutions to one problem, can beat monolithic corporations in competition. It is obvious that this way of working and looking at the role of the economy in society is part of the foundation of cyberpunk ideology. But here the respectable university hackers enter the picture: people who live normal, family lives, but who grew up with - and created - the first computers during the 70's, and who are now at forefront of the explosive growth in computer development. Their message is the same: Freedom of information! The rational world of computing seems to influence its users in the same vein: towards efficiency, decentralization, cooperation, and exchange of information, and away from bickering, bureaucracy, and monotony. I say that this is good. What do you think?

The World of Science

To understand how people can work their asses off without making a lot of money, one must understand how the scientific virtual community works. The scientific community is a society within society, with its own norms and ideals. Inside, *prestige* and *knowledge* counts the most, not how many stocks you own or how big your Mercedes is. Researchers, doctoral students, and other scientists *pay* to have their creations evaluated by other scientists, simply for the joy of sharing and promoting science.

The view that information and knowledge is public property is so inherent in this community that it isn't even questioned. All this information is published in a few thousand scientific journals across the world, with an extremely small distribution, created *by* scientists *for* scientists. Nowadays, more and more of these journals are starting to partly or completely employ electronic publication as a cheaper alternative to print - even within the "soft" sciences, such as Sociology and Psychology. The scientific community has been created to free research and science from the social power apparatus. The only way to do this is by building a culture with its own framework and values, which the hackers also discovered a long time ago.

As you see, the scientific virtual community share significant aspects with the hackers' sub-cultural *Scene*. They exchange information freely among each other, and ignore the market economy completely.[10] Of course, this throws a monkey wrench into the theories of most economists, since they'd rather see everyone acting according to a rational market model, but the scientific community won't submit to commercialization, no matter how much the rest of society wants it to. The icing on the cake is that the rest of society is *dependent* on the scientific community. Without science, little progress is made, and the schooling of new CEOs, engineers, psychologists, etc. is completely at the mercy of scientific realms. Therefore, society at large is forced to financially support these scientists. Graciously, the scientists in turn support hackers and some other subcultures by offering free access to computers.

Why do the scientists help the hackers? Simple. They depend on them. The hackers yield many of the ideas for new inventions and research areas. Additionally, many of

them work at the universities and technical schools. Some work at the companies that sell information services, and some are even to be found in the IT departments of the largest corporations. It is actually the case that the rest of society is dependent on both the scientific community and the *Scene* of the hackers. The conflicts that emerge are products of the fact that the technocratic society, led by scientists and hackers, is growing in power over the regular market-based society.

The reason that the establishment wants to control the funding for the Internet is, beneath the surface, a very old one: *it is concerned about its POWER!*

The Market Paradigm

We have to try to understand the origins of this conflict. Our society, as it exists today, is moving towards increasing levels of specialization. Our entire economic market model is built on it, or rather, on *a constantly increasing* degree of specialization. Productivity levels in this system must perpetually grow, in order to give a number of anonymous stock owners returns on their investments, so that they can buy and own even more.

If I want to develop software, I need an idea. Then I have to start a company, hire as many programmers as I need, and find some suitable investors. If I can't find anyone to finance my venture, my idea must be a poor one, or I've been looking in the wrong places. When the product is sold, I employ special services for the replication, distribution, and marketing of the software. Any CEO at any software company views the process in this manner.

The problem with this view is that there's no room for creative spirit among the programmers themselves. As a boss, I have to rigidly command them onto the right track. I must never lose control over the end product, and if the programmers come up with their own ideas, I'm of course free to listen to them, but it is still *my* responsibility as a project leader to decide whether these ideas will be part of the end product. There is no place for the free action of the individual in the market-oriented way of thinking. Only the project leader should know what really goes on with the product, while the individual programmers should only be concerned with the little piece they're working on. There is always an inherent hierarchy built into this form of organization.

Market-economy thinking is also built on a hidden method for hiding knowledge. It would be unfortunate for the project leader if the programmers realized how little influence they really have on the creative process. The same goes for all hierarchically organized companies. The only people that have any idea of what's actually occurring within a company is supposed to be the leadership. If the workers are to have any information, it is transmitted through carefully designed yellow sheets that are dumped in the employees' pigeonholes, in which chosen parts of the company's activities are exposed in order to increase motivation.

We're dealing with a power structure that is anything but democratic. This is the skewed balance of power that is the reason that companies work better than governments. The absence of democracy is very efficient. It's not a secret that the democratic offensive into the Swedish business world, in the form of MBL ("the law of shared decisions") etc., has decreased corporate efficiency. The workers should act

under the orders of management, not by its own will. Corporate management has therefore invented ingenious mechanisms to limit democratic control of their companies despite these new laws. These include, for example, constant reorganization in order to hide the mechanisms of authority and give the workers a sense of being in control of their own responsibilities.

The hacker ethic, cyberpunk ideology, and technocracy stand in sharp contrast. All of these views expect programmers to be creative, inventive, and *skeptical*. The market economy assumes that comprehensive plans are *not* questioned before they are completed. That's why companies go to great lengths to hire only engineers from universities and technical schools, who have by virtue of their degree been through the social indoctrination to *not question*.[(11)] Those individuals who question are sent into other parts of the machine of society: research, politics, and the *criminal industry*, to produce information of a kind that is important to society in other ways.[(12)]

---

1. Of course, as of today I've already submitted this text to the public one time.

2. Which has in fact become the case. I must be psychic.

3. Nowadays, virtually all magazines have an online version. My personal favorite is "Syber-Starlet" (Translator's note: a magazine very similar to *Seventeen*).

4. Maybe just a little bit. Passwords and other things that the users pay for are often crack and tossed to the four winds…

5. This is a generalized view that presupposes an infinite number of companies, a great number of different products in the same category, and that the "market" is an independent filter that is never deceived by propaganda. This stands in very poor resemblance to reality.

6. Then again, it's probably just a myth.

7. At the moment Telia is undergoing a reorganization which, as everyone who's studied introductory management knows, is aimed at destroying the social networks that have formed in the workplace in order to strengthen the upper echelons' grip on the company.

8. And now Windows NT is the hot thing. And then it'll be Nashville. Hum-de-hum.

9. I know that the know-it-alls are being driven up the walls by statements such as this. If it bothers you, write your own book for those who get hung up on details.

10. Pierre Bourdieu introduces the concept of "cultural capital" in order to try to explain this trend.

11. A slightly mean (and simplified) statement.

12. Svante Tidholm remarked that I have an ability to sometimes reduce the

individual to a simple puppet for the powers that be. I understand his view, but I'm not smart enough to get around the way the question is posed. My respect for the capacity of the individual is very great, and I also take the side of the individual in this rigged game. An expansion of my views is found in Chapter 15 as well as the Appendix.

Chapter 14
FEMALE HACKERS?

Within computer culture, and especially hacker culture, women are rare. Among the phreakers, there were (and perhaps still are) a few women, maybe because telephony is normally considered a female profession. (most switchboard operators and such are women). Rave culture is a little more equal, with about a third of the audience being female. Among the hobby hackers and the criminal hackers, there's only the occasional female enthusiast. Fortunately (I think), more and more women, especially at the universities, have discovered computers through the Internet. Often, someone starts out using the computer as a typewriter, then she hears of online discussion groups and forums for her major, and once she's tried communication over the Net, she's bitten.

The most famous female hacker went under the pseudonym **Susan Thunder**. (Allow me to jump back and forth a bit between the themes of the book). Susan was a textbook example of a maladjusted girl. She'd been mistreated as a kid, but was of the survivor kind. She became a prostitute as early as her teens, and earned her living working LA brothels. On her time off, she was a groupie, fraternizing with various rock bands. She discovered how easy it was to get backstage passes for concerts just by calling up the right people and pretending to be, for example, a secretary at a record company. She became an active phreaker at the very end of the 70's, and was naturally an expert at social engineering.

Soon, she hooked up with a couple of guys named **Ron** and **Kevin Mitnick**, both notorious hackers, later to be arrested for breaking into the computers of various large corporations. Susan's specialty was attacking military computer systems, which gave her a sense of power. To reach her objectives, she could employ methods that would be unthinkable for male hackers: she sought out various military personnel and went to bed with them. Later, while they were sleeping, she could go through their clothes for usernames and passwords. (Many people kept these written down on pieces of paper in order to remember them). Susan therefore hacked so that she could feel a sense of *power* or *influence* in this world, despite her hopeless social predicament. For her, hacking was a way to increase her self-esteem.

She was determined to learn the art of hacking down to the finest details. When her hacker friend, Ron, didn't take her completely seriously, she became angry and did everything she could to get him busted. Another reason for her anger was, supposedly, that she had had short relationship with him but he had chosen another, more socially acceptable girlfriend over her. It was probably Susan who broke into U.S. Leasing's systems and deleted all the information off one computer, filling it with messages such as "FUCK YOU FUCK YOU FUCK YOU", and programming the printers to continuously spit out similar insults. Among all the profanities, she wrote the names Kevin and Ron. The incident led to the first conviction of the legendary Kevin.

When Ron and Kevin were arrested, Susan was given immunity from prosecution in return for witnessing against them. Later, she referred to herself as a security expert, and conspicuously demonstrated how easily she could break into military computers. It is beyond all doubt that Susan really *had* enormous capabilities, and that she really

could access top-secret information in military systems. It is less certain that she could fire nuclear missiles. It is clear that she couldn't do it using only a computer. Possibly, with her access to secret phone numbers, personal information, and security codes, she *might* have been able to trick the personnel at a silo into firing a missile. I really hope that she couldn't. Stories about hackers like Susan provided the basic idea for the movie *War Games*. Susan has currently abandoned hacking in favor of professional poker playing, which she engages in with great success.

However, Susan is more of the exception that confirms the rule when it comes to hacking as a male endeavor. This phenomenon has lots of candidate explanations, ranging from moronic propositions that computers are unfeminine because they were invented by men (like the sowing machine, the coffee maker, and the telephone), to suggestions that women are somehow alien to the internal competition for status and arrogance that characterizes hackers. All of this is naturally bullshit.

The real reason to the inequality within the computing world is *probably* that many women are raised to fulfill passive roles. While men learn to passionately engage themselves in discussion over, for example, things on the TV screen, women learn to passively observe and act as social complements on the sidelines. Passion, assertiveness, and arrogance, all typical characteristics of hackers, are seldom encouraged. *Women are taught a superficially passive demeanor, in which their only possibility for action is by entrusting it to the hands of men*. All exploration of new territory apparently has to be done by men. (Preferably *young* men). As an example, look at our traditional way of handling emotional and sexual relations, where the general trend is still that men take the initiative and women should provide the passive, nurturing factor. Another factor is that men are more solitary than women. It's an open subject as to why this is, but it is obvious that it is incredibly difficult to break this pattern.

Since hackers are normally of an age in which it is very important to externally display one's gender identity, many women distance themselves from computers out of fear of seeming "unfeminine". This act, which is perceived as an autonomous decision by the individual, is actually part of the social indoctrination of traditional gender roles. Parents and relatives add to this by giving computers almost exclusively to boys, and almost never to girls. Among the home computer hackers during the period of 1980-89, about 0.3 % were female, according to rough estimates. In the U.S., there was a female Apple II cracker who managed to liberate around 800 games from their copy protection. In Europe, the most famous female hackers were part of the **TBB** (The Beautiful Blondes) group, which specialized in C64 and consisted of four women under the pseudonyms of **BBR, BBL, BBD,** and **TBB**, of which BBR and TBB were programmers. They became known on the Scene through a number of demos toward the end of the 80's. Cynically enough, both BBR and TBB died in 1993, not even reaching the age of 20. Among today's Amiga and PC enthusiasts, the proportion of women is a little higher, somewhere around 1% (Source: **The Mistress** in *Skyhigh "17*, 1995).

At MIT, the cradle of hacker culture, there weren't any women at all. There were female programmers who used the machines, and even really good ones, but they never developed the obsession found among the young men at MIT. These hackers thought it had to be a matter of genetic differences that caused the women to not fall

into this obsession. This is a dangerous opinion and absolutely untrue. According to statistics, most boys who become intensively engaged in computing are around 14-15 years old. The same preoccupation occurs in women too, but usually about two years earlier, since their biological clock dictates it. Most people know what 12-year-old girls can get caught up in with such intense interest that they forget social duties and just concern themselves with the *hobby* for its own sake. The women's (or, rather, the girls') equivalent of the rather fickle but enchanting object known as the computer, is another object with similar characteristics - a four-legged one, which we usually call a *horse*. In many cases the similarities are striking, even though it is difficult to prove that the same mechanisms lie behind it. Programming a computer is really not that different from teaching a horse to jump fences. It includes the same measure of competition, control, and ceremony. With the boys in front of the computer, there's an almost empathic passion, just like it is with the girls in the stables.

It's completely obvious that if this trend continues, men will acquire the power in a future society largely built on computer technology. It would be a good thing if more women used computers. Even hackers are generally positively of a positive attitude towards seeing more women in their male-dominated fields. The few women that exist on the Scene have been very successful, and received lots of attention as "exotic" phenomena. The respect for female hackers is very great. Supposedly, there are also female hackers who have hidden their gender and are assumed to be male by their hacker friends. The thrill of playing out such a role isn't hard to understand. For the first time in history, it's been possible to assume a gender opposite of one's own without great difficulty, and for a woman to really be treated like a man.

The German police sometimes use this respect for female hackers to bust hackers and software pirates. By publishing posts and ads on BBSs and in computer magazines, using female names, they attract the attention of their targets. It is a matter of argument whether it's ethically correct to exploit people's emotions in this manner in order to fight crime, and it obviously does no service to equality. It becomes even more difficult for women to break into a sub-culture where they might be suspected of being law enforcement moles.

Pornography, etc.
One cannot fail to note the preponderance of male chauvinism on the Internet and in the home-computing world. Basically, it all started with the game *Softporn* for the Apple II, by the **Sierra On-Line** computer company, and the even more successful sequel for the IBM PC: *Leisure Suit Larry*. The object of the two games is the same: getting women into bed. The fact that the Internet is crawling with soft- and hardcore pornography doesn't help things either. Whether or not this is a sign of a screaming need for sexual stimulation among male computer users is hard to say. (In any case, there's no shortage of pictures of naked men). Naturally, it's less embarrassing to download pictures to your computer than going out and buying porn mags - since no one can see what you're doing. (As far as you know, at least).

A large part of the pictures available on the Internet are marketing tools for different pay-BBSs, from which you can retrieve even more pictures - if you pay… As usual there is, in the porn industry, a ruthless commercial interest in the Internet. Sex sells, and the Net is used as bait in a new and lucrative market. I'm going to emphasize that this is mostly a trend in the U.S. I have yet to hear of a Swedish BBS that works this

way - instead, in Sweden it's free to download the pictures, which the users engage in with abandon. A few porn magazines have opened their own Internet zones which users have to pay to gain access to.

Some PC enthusiasts have gotten a bug for collecting porn pictures, and collect them in the same manner as others collect stamps or trading cards. Actually, this hobby isn't anything strange. During the early years of hacking, many collected thousands of computer games just to have them. It was *forbidden*, since the manufacturers claimed that copying the games was prohibited. Pornography is *both* taboo and copyright-protected, since they are almost always scanned from porn magazines. It should be added that the porn industry is less than pleased with this type of distribution.

Censoring these pictures on the network is virtually impossible, and not necessarily desirable. The Internet is based on the supposition that you search for the information that you're interested in, and that you thereby bypass information that you find irrelevant, and this is the philosophy that colors the attitude of those who maintain the network. Whoever publishes the information holds the responsibility, and the middleman cannot be blamed for anything. It would be just as consistent to accuse Telia or the postal service of being accessories in crime for not conducting enough surveillance and letter-scanning. Communication should be free.

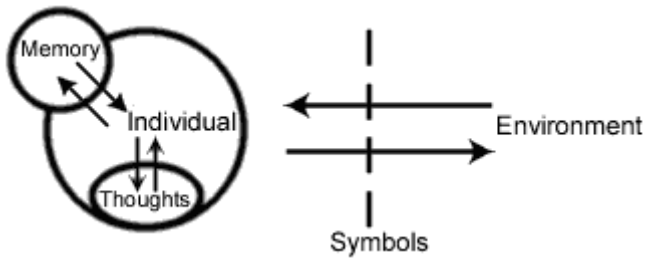
SUNET (Swedish University NETwork), under the command of Björn Eriksen, distributes the Internet in Sweden. They have so far consistently refused to interfere with the flow of information. (And I hope they never will). Individual universities, however, have (following public awareness) started to block certain discussion groups with themes such as piracy, sex, suicide, and drugs. Blocking pictures in general, however, is much more tricky, not to say impossible. If someone encrypts the pictures, it becomes *completely* impossible to stop them. The only thing you can do is monitor the pictures stored on the computers inside your own organization, which has led to public intervention against pornography at the Lund and Umeå universities, among others.

If you really wanted to crush the market for the porn industry, you could simply remove its entitlement to copyrights for its products. This would immediately ruin the market for the established industry, and force the companies to go bankrupt in just a couple of years. I will, for the sake of clarity, add that most women who are actively involved with BBSs and the Internet take the whole thing in good stride. If someone insults them with profanities, they usually respond with the text version of a pat on the head - *"There, there, calm down now"*, or something similar.

Even if cyberspace is male-dominated, we can comfort ourselves with the fact that the world's first programmer, **George Byron**'s daughter **Ada Lovelace**, was a woman. Ada was a *real* hacker, by the classic definition. She was the product of a failed marriage between Byron and Annabella Milbanke. Just like many contemporary hackers, she escaped painful emotions by dedicating herself to the natural sciences together with her friend **Charles Babbage**, and completely immersed herself in the quest to construct *the analytical machine*.

Chapter 15
THE CYBERNETIC SOCIETY

I will now try to summarize what I've written so far, and synthesize this with a number of modern philosophical ideas about people and our society. A cybernetic society is a society of people who live in symbiosis with machines. To understand a society, I employ a simplified concept of an individual, in which he or she is viewed as a construct of information, communicating with the environment by means of *symbols*.



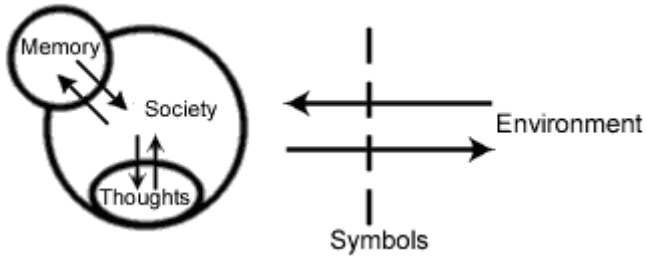
In the figure, **memory** stands for the stored patterns in the brain's neurons, **thought** is the reflections and dreams (daydreams included) that we all have, and the **symbols** are those chunks of information we exchange with the **environment**, which can be single individuals as well as the entire family or society that we live in. Such symbols can be human language, but also other conventions that we don't think about much, such as pieces of paper with numbers on them perceived as possessing value, or a certain type of clothing perceived as indicating a certain status. For natural reasons, science uses well-defined symbols called *paradigms*, which define:

1. **What to observe**
2. **What questions to ask**
3. **How the questions should be asked**
4. **How the answers should be interpreted**

(I'll take the opportunity to state that I interpret the sociological-scientific concept of a symbol, as well as the concept of a paradigm, in a very pragmatic and personal manner - raise a hand, whoever cares. This is high-level hermeneutics. Pardon the ten-dollar words).

It is these concepts that the hackers, with Zen and Gödel behind them, contest in their motto number 4: *Hackers should be judged for their hacking, not according to suspicious criteria such as academic performance, age, race, or social status*, and in 3: *Distrust authority.* It's an attempt to break out of a system that is perceived as wrong. Marvin (the guy with the telephone cards) spoke in a radio interview of his dissatisfaction with companies hiring people with degrees instead of caring about their *real* skills and in this way pointed out the shortcomings in our formal social system. Burroughs thought that society would try to increasingly control the thoughts of its citizens, whether its public servants wanted to or not. It is said that an enlightened individual must have the ability to *exit* the system to see the real patterns behind it, which can't be described using words, paper, or clothing. At the same time, the

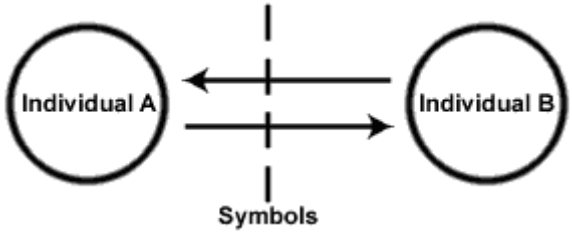
symbols are vital to our communication as well as our society as a whole. An intelligent individual can, using symbols, detect intelligence in him- or herself as well as in other individuals. We can now view society from a similar perspective:



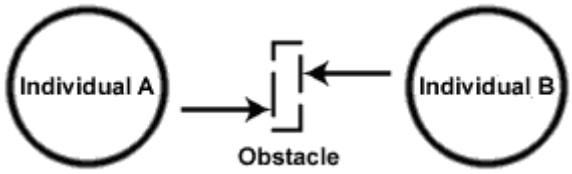
But what's this? It looks just the same! That's right. In this case, **memory** is the collective memory in the form of books, films, CDs, or computer programs, stored in libraries or in our homes. **Thought** is the same as *culture*, the ongoing process that continuously affects our living conditions. Note also that the **symbols**, in this case our relationship towards other societies or aggregations, is not the same as our culture. Sociologists often refer to this model as the *collective consciousness*. As for myself, I've nailed together the concept of *superindividual* for this model.

The symbols show only those parts of our thoughts, culture, that we *want* to show. As is well known, this is also how an individual works. An intelligent society detects intelligence in other societies *and* individuals. The individuals that make up society can very well endeavor to analyze the thoughts that society thinks, but the task is virtually insurmountable, like if the individual neurons in our brains were to try to understand the thoughts of the entire brain. (These arguments originate in research of artificial intelligence in non-formal systems and sociological science). This model is not limited to describing societies and individuals as intelligent organisms, but can also be applied to corporations, military organizations, and others. It is this *formal system*, the complex society, which sociologists study as scientists, William Burroughs criticizes as an author, and Zen debunks as a philosophy

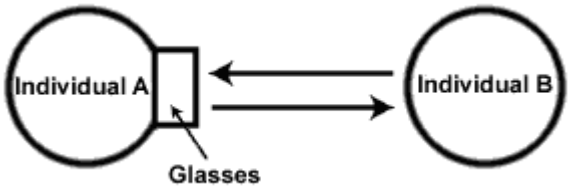
Now that we've agreed on a common view of individuals and societies, we can start defining cybernetics. I said earlier that cybernetics means *people or society in symbiosis with machines*. To illustrate, here's a practical example:



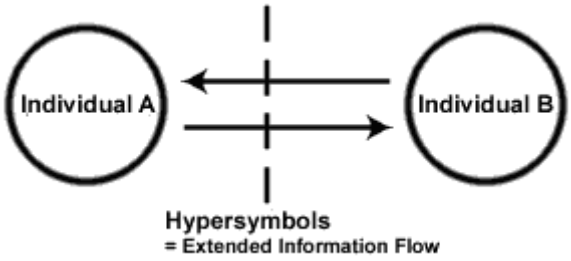
We see two individuals, A and B, communicating by way of symbols. So far there's no problem. If we, for
example, suppose that these individuals communicate by sending **letters** to each other, a problem could occur if one of them has a slight vision problem.



Since people are so ingenious, they naturally find a way around this problem. They attempt to *improve* their natural conditions. I will illustrate this with an invention that was created around 1290 AD:



We have here one of the very first cybernetic innovations. Reality has been improved by a small opto-mechanical construction that we take for granted in today's society. All people that wear glasses are therefore *cyborgs*, people who live out their days on Earth in harmony with machines. We're so used to this that we hardly ever think about it. If you're a little more vain, you can get contact lenses, and then you invite the machine into your own body. Glasses constitute one of the modifications that are meant to improve our ability to communicate with the rest of the world. Other cybernetic modifications are aimed at making life more comfortable and bearable for the individual: the wheelchair, the cane, etc. Some are vital, like the pacemaker. Of course, now I've just listed inventions that "correct" human disabilities. Naturally, you can "improve" regular people too, with the aid of binoculars, electronic devices for night vision, etc. The telephone, for example, improves us so as to allow us to communicate over enormous distances. We can also establish *hyper-communication*.



One such medium is hypertext, which is better than normal text. We can also improve our possibilities as a society to exchange and distribute information with the help of transaction systems, satellite TV, etc. Yet another improvement of our perception - and the most revolutionary - will be Virtual Reality. There are, however, a few uncanny aspects of this society. Like, for example, the previously mentioned *NetNanny*, or when Aftonbladet on July 15, 1995, reassuringly announced that TV sets can now be fitted with a chip that is programmable by parents who don't want their children to watch excessively violent, pornographic, or otherwise unsuitable programs. When the kids try to tune in to a blocked program, the screen turns blue.

Fantastic. The question is just who is being programmed: the chip or the children? One of the parents interviewed by Aftonbladet wants to prevent the kids from watching, among other things, *SOS - På Liv och Död* (cf. the American TV show *Rescue 911*), which is a program that shows films of real accidents and rescue efforts. What's next? Isn't it just as well to turn off those terrible news, so that you can raise your children in a protective bubble, as far removed from the world as the Russians ever were under Stalin? The risk of abuse of this, and similar, invention is terrible and great.

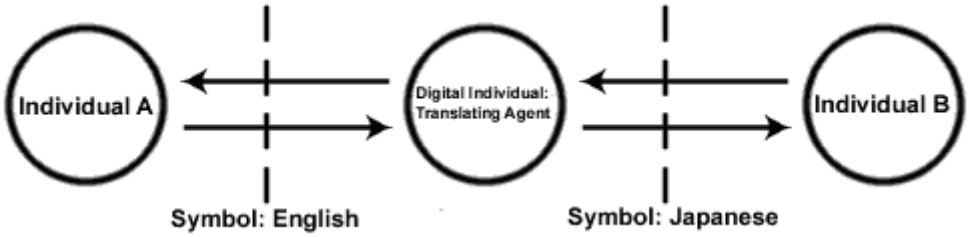
And this was only an example of what a relatively stupid chip can accomplish. We are already forced to note that our society is no longer formed solely by people, and that not even *people* are formed solely by other people. When almost every store has electronic anti-theft systems on every product, there's no longer a need for honesty as a virtue, because it becomes *impossible* to act dishonestly - and thus, moral limits are turned into real, physical limits with the help of technology. We are so singularly obsessed with the public good provided by these machines that we don't question what is happening. A store alarm is nothing to complain about, since it only concerns itself with thieves… *One fine day*, we'll be hanging around with machines that automatically inject sedatives into all individuals with violent tendencies, naturally only to prevent them from committing violent crimes. That's no concern of yours, is it? You're not a violent criminal. Or?

Just to give an example from a few years ago: in 1984,[(1)] the computer at Värnpliktsverket (the Swedish national military conscription administration) experienced problems with the result that orders to report for rehearsal training were not sent to all personnel that were obliged to do so. These people received phone calls from authoritarian military officers that interrogated them as to why they hadn't reported for duty. The authorities had received information from a computer, presumed to be reliable, that orders to report had in fact been sent. What's interesting here is not so much that a computer could experience an error, but that it could really *control* a large military organization. Some of our most respectable military institutions therefore have names that could be used as product labels for various computer brands.

Then, there's artificial intelligence. When intelligent agents enter the picture, complexity increases. We may be forced to ask ourselves if it's perhaps the case that we interact with digital individuals, seemingly possessing their own free wills. A digital individual is created when a computer system becomes so complex that it gains a *consciousness*, similar to that of humans. This probably hasn't happened yet at the time you read this. The most disturbing example I can think of is a program from Hectare Ltd, which can generate trashy novels for women, i. e. stuff similar to **Barbera Cartland**'s, in a never-ending stream. If you ever suspected that a computer could generate mainstream fiction, your fears have been realized. The program really works, and it's not even very large and comprehensive. Similar programs can reformulate pre-written passages to infuse them with a certain style of writing.

One of the most dangerous power factors with AI is that it can easily produce an endless flow of seemingly intelligent bull, which diverts attention from real problems. To coin a conspiracy theory, I'll propose that there are already publications whose content is wholly or partially computer-generated. Those who wrote the programs are

probably mostly concerned with making money and don't care whatsoever about the moral aspects. *Wouldn't you?* The public doesn't notice. They think they see a human, but it's really a robot. But then again - what's the difference? Curtains.



This is just one of the many possible applications of artificial intelligence. It is the case, however, that the digital individual will one day become so intelligent that it can produce a dialog without any input from one of the persons speaking. The established authorities can then control the individual in any manner they choose. Imagine calling the utility company about having no hot water. You think you're speaking with a human, but you're actually talking to a computer. Everything you say is turned into statistics, with no need for the responsible parties to react to any criticism. The powers that be can filter out your complaints in order to make independent, emotionally neutral decisions… and right about here the argument becomes so fuzzy that I might as well leave it to the reader to finish. (I'm not really a philosopher, just a dabbler in the art). It is at least an amusing thought experiment.

Cybernetic Society vs. Copyright

It is obvious that the cybernetic social model entails changes in our way of viewing information and its role in society. Some things that we now take for granted may become fundamentally altered. An example: copyright. Copyright is the right to own information, or in the case of a *patent*, the right to own knowledge and make money from it. In jargon, it's called *intellectual property*. Copyright was created in conjunction with the art of printing, since before that time it wasn't very important to know who owned information and the right to publish it. All knowledge and ideas were in those days considered public domain, and not property. *Information was free*. Th possibility of owning information is inseparable from the presence of machines like the printing press, fax machines, or computers. Without these, the book, painting, etc., become unique works of art as opposed to a mass of reproducible information. Thus, copyright is an attribute of the early cybernetic society that associates *information* and *knowledge* with *economy.* This applies to all information, printed text or photographs, film or software.

We can then trace the origin of copyright to the emergence of the printed symbol. To emphasize the importance of this development (in order to strengthen the argument), I will summarize the development of modern symbols below:

Symbol	**Population**	**Cultural Basis**	**Time Period**
Primitive symbols	Animals	Genetic culture	Prehistoric
Speech	People	Oral culture	40,000 B.C.
Text	Civilization	Written culture	3,000 B.C.

Print	Industrial society	Distributed mass-culture	1,500 A.D.
Hypersymbols	Information society	Information culture	2,000 A.D

The dates indicate the origin of the respective symbol, rather than the date it became widely used. Normally, the transition from oral to written culture is considered to have taken place around 500 B.C., and printed material wasn't very widespread before the Enlightenment (1700s and 1800s). The first date is very hard to ascertain. This is really not that important: the question is not one of dates, but of the history of symbols. It is clear that information technology is causing a change in society which effects are comparable to that of the printing press (at least!).

Symbols change with time. What we consider valuable today can become worthless tomorrow. For example, most people think gold is valuable. If, let's say, a small planet made of gold collided with the Earth, making gold the most common metal on the planet, our view would instantly change to where gold was worth less than iron. By the same token, we would gladly trade all of our gold for food if we were starving, since we also have certain physical needs. You could even say that we have psychological needs, which are (in our modern society) largely generated by advertising, making us willing to trade our economic means, in monetary form, for stereos, sodas, etc. We thus have a conception of the value of things that is based on supply and demand. Supply and demand are controlled partly by nature, and partly by other people. This is what makes us consumers. These concepts are found in all major ideologies.

When other people want to influence our consumption, they use symbols to do so. This can be done by, for example, establishing a certain brand of clothing as synonymous with the symbol called *status*, or a brand of soda as synonymous with *freshness* and *youthfulness*. But this is only the most conspicuous part of the top of the iceberg. In reality, our entire societal system is built by symbols. This is what sociologists cal *symbolic interactionism*, which is a scientific theory usually associate with a guy named **George Herbert Mead** - something of a genius of a philosopher, who unfortunately didn't directly write anything, but had a great influence on the field of sociology. Mead defined many of the symbols I've mentioned in this chapter. Mead also touched upon the concepts that will be found later on; among other things, he suggested that the French Revolution was a turning point in modern history, where people for the first time realized that they had a right to change or correct society, and that the state wasn't based on some divine principle. Philosophically speaking, he was a pragmatist who thought that ideas and theories should be checked against reality before being awarded any value or authority. Mead for sure was a supporter of the *hands-on imperative*. (The pragmatic school of thought is an extension of fallibilism, which is basically the same as Zen).

Ok, fine. What about copyright, then? That's the point I'm supposed to get to. We, as the people of the Earth, have reached an agreement that says that we should view information and knowledge as property. This concept of property, or ownership, is a *symbol* that we endorse. With the introduction of the information society, the *morality* created by these symbols becomes fuzzy, to say the least. Morality, or ethics, tells you that you shouldn't trespass on the territory of others, not to harm, not to steal someone else's property. These are commonly accepted moral imperatives when it comes to

material property. But when it comes to *intellectual property*, protected by copyright and patents, we've reached a breaking point. IT forces us to re-examine these principles: it is *immoral* to enter certain commands in a certain order from your keyboard. Other command sequences are fully acceptable. I can program my own computer, but not someone else's over a network. I am permitted to copy some programs as much as I want to, some not at all, and some with conditions. We become uncertain of what to think, and some succumb to dogmatic condemnation of software piracy, in order to be certain.

Since legislation isn't the same thing as corporate policy, I get mixed signals, like when the gaming company Nintendo asserted that it was forbidden to engage in second-hand sales of computer games. Of course Nintendo is of this opinion, since if people can only buy new games, that lets Nintendo sell more of them and make more money. Under Swedish law, Nintendo doesn't have a leg to stand on. We are faced with conflicting messages from the government and established industry, with the result that we start thinking on our own. Since corporations share economic power with governments, we view both as authorities. We start questioning these authorities - we start thinking independently, and make our own decisions in the absence of clear directives from society. Remember, once again, Rule #3: *Distrust authority.* The hackers' ethic leads the way through turbulent times.

The hackers discovered severe injustice with regards to information. On the Scene, the 13-14-year-old hackers couldn't for their life understand why only the youths with rich parents should have access to all the fun software. Among the phreakers, there was total disbelief over why only companies and institutions should be allowed free communications - since this was a way to grow! Why accept this? Granted, one could call this lack of respect and lack of understanding of the workings of society, etc. However, no one lowered himself or herself to discussing the issue. The message that the hackers received from the establishment was: *"You are criminals. Period."* What amazing hypocrisy!

I conclude that *the more cybernetic a society becomes, the more difficult it becomes to define private domains of knowledge.* The more computers and the more refined technology we get, the more meaningless the concept of *intellectual property* becomes. This is especially the case with software, for which patents are granted for methods that didn't require any large investment in research and equipment, but only perhaps one or two nights of intensive hacking. The ideas didn't cost anything - it's mostly a case of "early bird gets the worm", and it gets the *only* worm. It is no longer possible to defend intellectual injustice with material analogies.

This forces us to pose the question: where is the line between freedom of expression and property? What may I copy and what may I not copy? When does knowledge cease to be public property and change into private property? What is happening is that technology is de-boning our entire social systems, holding up its skeleton for all to view. We can see how large areas of cyberspace has arbitrarily been sold out to the profit-hungry gold diggers of the information industry.

Software is an extension of the human mind: of the ability to create, understand, and generalize knowledge. To reserve such a powerful tool only for those who can afford to burn hundreds of dollars on it is not sustainable in the long term. I'm not saying that

parasites like the Chinese Triads or other piracy syndicates should be allowed to take the right of ownership from the large companies. What I *am* saying is that it shouldn't be prohibited for private individuals to freely distribute software and help each other use it. This doesn't exclude competition from established companies, as long as they can provide something that the local hacker can't: printed manuals, 24-hour service, instructional resources, etc. Who knows these things better than the one who created the software? *Software is a product that lacks inherent value*. It is not the ownership of software that drives society forward, it is the ability to use it, and to teach others to use it. What we should buy and sell in the information society isn't software, but applications and advice - in one word: *Support*.

As necessary as copyright was in the industrial society, as meaningless it is in the information society. The problem is not separating printed information from electronic information. The problem is that it's no longer possible to separate *information* from *knowledge*, and *owned knowledge* from *public knowledge*. The line between an *idea* and the *application* of the same is being erased as people communicate more and more using machines that have been constructed for that very purpose. By extension, the line between *thought* and *action* is also threatened by the development of virtual reality.

Let the software companies fight syndicates, mafias, and criminal groups that make a killing off piracy - this doesn't bother me at all. But, for God's sake, don't condemn the private copying of software between friends with no profit interests involved! This distribution is *not* immoral, but simply a way of transmitting knowledge. It is *wrong* if such copying is illegal, and it *should* be permitted for private individuals to copy as much as they want. It is the *dirty money* that should be removed from the software business, not the burning interest and enthusiasm of the amateurs! The moral limit is not drawn over the right to copy programs or not, but the right to *make money* from a program or not! This is the right that should be reserved for the author, if he or she so wishes.

In Sweden, today, I can go into any public library, retrieve any book that I want, go to the copy machine and copy as many pages as I want. Some legislator, in a moment of clarity, realized that preventing this would be an infringement on the freedom of the individual and the possibility of personal development *Code 1993:1007). Information gives birth to intelligence! *There is no reason that this freedom should be limited to printed matter.* Films, CDs, computer programs… it's only a matter of definition. All of this is information, and nourishment for human intelligence. It is not healthy for the individual to be prevented from copying information. It is sick. *SICK!*

Patenting a certain sequence of characters - strings of information - sound waves and videograms - insanity. If the people who first invented words for human language thought in those terms, we would have never learned to read or write. Whistling a patented song on the town square one sunny afternoon is a "public broadcast", and royalties should be paid for it. When you're not engaged in making a profit off information - which is by extension to increase your power - when you're simply out to spread joy and knowledge, then information should be *free*. Period.

There's no point in dragging out an argument about it, and legislate left and right. Sooner or later, we'll reach the *jaywalking* criteria (Translator's note: in Sweden, it's

only illegal to jaywalk if you end up actually interfering with traffic): this is when a crime becomes so common and widespread that it's pointless to fight it, like jaywalking or copying music CDs to tape. Rather, governments and legislators should concern themselves with their own integrity.[(2)]

Conceptual Breakdown (Copyright Does Not Exist!)
With the decreased clarity of our symbols, what should we expect to happen? To have something to build on, I will with impunity borrow an idea from **Thomas Kuhn**. Kuhn is a philosopher of science, who has exciting ideas about the way science grows and changes over time. Kuhn's theories are reminiscent of ideas of social development, the emergence of various ideologies, and how we humans grow and change our environment in general. In short: the man describes what happens when people use their intelligence. The most thrilling part about Kuhns theories is that they are very reminiscent of Gödel's theory of formal systems. The basic premise is the following: you have a clear picture of the world, a *paradigm*[(3)], such as:

> You know that information can be owned, because otherwise this and that company would go bankrupt, and that means this or that to you, which is not good, and therefore you should accept that information can be owned.

Or:

> You know that money is valuable since it's based on the country's productivity and quality compared to other countries, and therefore you should accept that a note with some numbers on it is worth money, so that the government (and other governments) doesn't suffer a crisis of public confidence, because then your standard of living is threatened. (Note: slight sarcasm here. Other people might say this in complete seriousness, though ;)

Kuhn thought that paradigms changed over time like this:

Paradigm -> normal conditions -> Inconsistencies -> Crisis -> Revolution -> New Paradigm

With the premise that people generally develop norms (rules for action, bases for judgment) in the same way that scientists form paradigms (models, bases for judgment), I'm applying this system to our society. (Norms and paradigms are kind of the same - both are grounded in human intelligence, and are oriented towards bringing order out of chaos by erecting philosophical systems). These conceptual systems live around us while we don't think about them. For example, there's no law of nature that says we have to divide the day into 24 hours - we would do just as well with 10 or 50. No one forced us to separate musical tones into 12 per octave, because 8 or 16 would work fine too. We define our environment in common terms to avoid conceptual confusion. Sometimes we reflect on these concepts so rarely that we take them for granted, as a natural order, and for that reason we consider people who come up with new conceptual systems delusional. William S. Burroughs expresses this more conspiratorially and ruthlessly:

> *"There is no true or real 'reality' - 'Reality' is simply a more or less constant interpretive pattern - the pattern that we accept as 'reality' has been forced upon us by the authorities of this planet, a system of power that primarily seeks total control."*
>
> (From *Nova Express*)

When **Erik Satie**, the poor genius, played his furniture music which broke with traditional patterns of musical creation, he got booed out. When **Picasso** broke with classical art concepts, many considered him to be an idiot. Cross your heart - how many of you has *not* at some point complained about art which *"you can't see what it's supposed to be"*? Gödel went so far as to prove that even something like *time* is subjectively perceived, philosopher or not. With hackers, we find this rebelliousness in, for example, the B1FF language, where our pre-established notions of the functions of signs are given a serious twist. Many BBS and Internet users write flaming posts when they see someone write a sentence like: y0YO!#%$!! wH4+zZ h4pP3n1n' 4r0uN '3r3 +H3zZ3 d4yZzZ?#$!%??. The question repeats itself: *how groundbreakingly creative are you allowed to be?* And at which points in time?

From the start, after some turbulent times we've established a closed conceptual system that we have accepted, we live in a stable condition where production and consumption live in harmony with an established societal system, with all that it brings of class divisions and territorial thinking. Now, when the information society brings things to a head, internal inconsistencies emerge inside the system. Is money really based on production? What are the production forces, in that case? Can knowledge be owned or not? This is the period in which our society currently finds itself, and will remain in for quite some time. This is the turbulent era of the *post-industrial society*. We are breaking out of the complete, near-mathematical system that our society has been stuck in, almost like Gödel broke out of mathematical systems and Zen debunks philosophical theories with direct answers. The *Patriarchy*, which the feminists want to break down, is another system whose foundations are cracking. (Within sociological science, this condition is called *anomie*, which means that there is a lack of functioning norms in society, like in today's post-Soviet Russia). This phase is also characterized by mushrooming subcultures and a reinforcement in religious sects, both of which are a result of an anxious search for definite norms not found in ordinary society. Eventually, there will be a *crisis* that precedes the *real* information revolution. This is when the most comprehensive societal changes will take place. (We are talking about a social revolution, no necessarily a bloody one). After this revolution, we form a new set of assumptions about how society should function, and it is only then that we have achieved the real information society. Many micro- and macroeconomic equations (or *axioms*, to be scientifically nit-picky) that are valid in the industrial society will become totally worthless in the information society.

In order for the changes to occur at all, someone has to push them through, committed to partially tearing down old norms to make room for new ones, albeit with some respect for the old society. These are Nietzsche's disciples, or in our case, the most militant cyberpunks with the hackers at the front, who dare to stand for their ideals in a new age. To quote Nietzsche himself: *"I'm not closed-minded enough to stick to only one system, not even my own!"* It's about tearing down the norms of industrial

society to make way for the ones that will put information society on track. It doesn't have to occur outside the established system; what Nietzsche (and others) says is that it *may*.

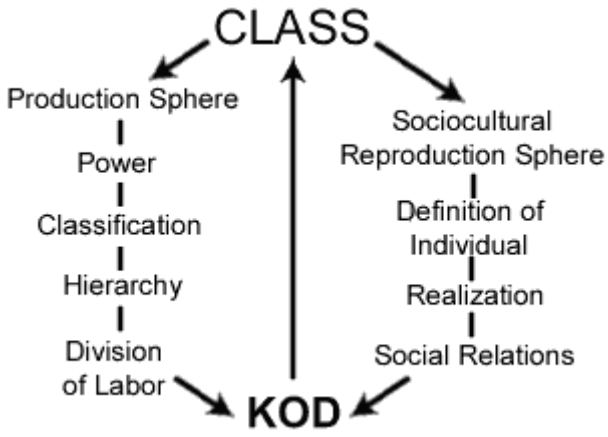
Since the 50's and 60's, the younger generation has assumed the role as pattern-breakers, questioning old systems and building new ones. In Nietzsche's time, students and intellectuals were the most rebellious. There's been a shift to where radical ideas are associated with youth, and conservative ideas with age. This is one of the worst pathologies of our system of roles - many young people actually dislike the role as revolutionaries, and become, like in **Tom Petty**'s partially self-biographical song *Into The Great Wide Open*, rebels without a clue. The pressure to revolt can in some cases become the straw that breaks the camel's back, pushing youngsters into crime and drug abuse. Many acts of rebellion are unfounded and arbitrary, aimed solely at provoking more conservative older folks - but there are some acts that *are* justified. The revolt against the informational dictatorship of corporations and governments is not unreasonable. It is an ideologically grounded revolution, which deserves being taken seriously.

Tolerance for new concepts and points of view is one factor that determines how closed or streamlined a society is. Nietzsche, in his time, appreciated the majestic music of **Richard Wagner**, which was another attempt to break out of a degenerating musical paradigm. Even though Hitler later admired both Wagner and Nietzsche, nazism was an ideology that condemned any effort to create new systems of concepts. Towards the end of the 30", they organized an exposition in Berlin for "ugly" art, mostly modern, which they considered sick or twisted. That's the nature of fascism: after a shining ascension, it loses all interest in creativity and strives only to preserve itself. Can a society like ours, with corporations large enough to intimidate governments, accept an orderly and reasonable debate about the existence of copyright? Or will the system violently seize the power to decide what is public and private property, bypassing pesky democratic channels through lobbying and executive decrees with no debate whatsoever?

Dear readers: I suppose that on your journey through this book, you've discovered how close we really are to the information society.

It's my honest and upright opinion that such a society will either be free of copyright and software patents as they exist today, or it will be an informational dictatorship run by either governments, corporations, or mafias. The latter is the society William Gibson warns us of in his cyberpunk novels. Let's avoid it. I have do not know exactly how this change will occur, nor what the final result will be, just that it *will* take place.

Cybernetic Society vs. Class Perspectives - The Mechanisms of Power
The British sociologist **Basil Bernstein**[(4)] viewed the mechanisms of society like this:



In this system, we can see society divided into a production sphere and a sociocultural reproduction sphere. In the *production sphere* (corporations, organizations, legislature, executive branch, and counties), **power** is created, economic, political, and public. The *socio-cultural reproduction sphere* (parts of the media, entertainment industry, educational system, etc.) exists to justify and perpetuate the patterns suitable to the production sphere.

At the bottom of the picture, we find the nexus of these relationships. The **Code** is our language, in all its forms. It's actually every social symbol used to exchange information between people and society. The **Code** is *pure information.* It is the foundation for the entire hierarchy and social order. Through the linguistic code, society is constantly structured and reinforced in the same ways, which is why Zen, Nietzsche and Burroughs criticized language - they felt subordinated to a social and cognitive system which never changed in any substantial manner. Additionally, language has more levels than the spoken or written. There is pictorial language, music, and all kinds of symbols to use. Basically, all vessels for the transfer and storage of information could be said to be part of this code.

Many believe that the information society will naturally generate the same kind of structure, just because it's always happened before. There is no evidence suggesting that this would be the case - rather, evidence suggests the opposite. The information society inherently elevates public consciousness of society itself to a level which bares its mechanisms. What's actually happening is that the basic units of society become aware of their own role in this gigantic information system, which in turn leads to their desire to improve it. Social progress can thus be further accelerated, like always (you with me?).

Let's employ an illustrative example: a current controversy on the Internet concerns (as I mentioned in Chapter 8) the Church of Scientology and its questionable copyright on the religious documents it produces. According to believers, the documents contain material describing the movement's so-called *clearing technology*, which is a quasi-science demanding comprehensive and very expensive courses. The Church thinks that only members of the movement have a right to this information. Roughly, you could say that clearing technology consists of hypnosis and science fiction.

The Church of Scientology is a sect, and as such, a society within society. It provides all the functions a society normally provides for a human being. It affords her opinions, morality, social orientation, and so on. The only reason for a member to venture outside the limits of the sect, is to earn his or her own living and thereby nourishing the sect also. Sects, among which I also place the Plymouth Rock people, Jehova's Witnesses, and Livets Ord (a Swedish religious sect), live like parasites on our social system. Almost every clear-headed individual is aware of this. One way of seeing how hermetically closed a sect is, is to apply Bernstein's model on it. Any reader with some imagination shouldn't have much trouble doing this.

Now, participate in a thought experiment that is taboo. Imagine that society is a sect, and that your thought patterns are externally controlled. Imagine that copyright and freedom-of-expression legislation exists to limit your awareness and maintain the social hierarchy, just like a sect's leadership rules its members. Imagine that, despite all of our freedoms, we might be blinded by the delusion that our society is free! Members of a sect are completely convinced that they have made an independent choice to join it, and that they are free individuals. All sect members are convinced that the sect's account of things is the one true account, and all renegades are vehicles of, for example, Satan. Suppose that all members of society are convinced that society's account of reality is the true one, and that criminals, hackers, and other non-conformists are painted in a bad light because it suits its purposes. No sect leaders force their members to obey and serve out of sheer lust for power, but because they actually believe in what they're doing. No politician or CEO forces citizens and employees to do their bidding out of sheer malice, because they also believe in what they're doing. Do you understand Burroughs a little more?

Look society and power in the eye. Why is the Church of Scientology one of the first authorities to cry for law and order, wanting control of information? Why is society not so far behind? Why do we want to keep tabs on the information that spreads through subcultures? Suppose that there are truths you never dreamt of, outside the universe of society. Isn't it the case that behind this jovial façade of the social community a force is concealed, which wants to replace organic sympathy with mechanical obedience?

So what is this superior power? I've already shown what it is: supervisory intelligent entities, thinking units consisting of constructs of people: Corporations, Governments, Nations, Counties, Concerns, Mafias…. they consist of individuals, but they don't *think* like individuals. They are intelligent, but their intelligence is not human. They can benefit us, but they can also do us harm. They are *superindividuals*, individuals made out of individuals, united through the control of information, or to put it in another way: *power*. The problem is that we, as humans, have a horrible time seeing the forest for the trees.

Too many myths are flourishing around people and their society. One of the most despicable ones is the delusion that society is "free". Every society is founded on the *lack* of freedom - giving up some of your freedom in exchange for security. What every individual should know is that unless you apply anarchistic principles, you have to go through life constantly sacrificing parts of your freedom to superior forces. These can consist of the kinds I enumerated above, and others. The basic obligation a superindividual has to an individual is to inform the individual that *"this is what I*

claim of your freedom, and this is what you get in exchange." Symbiosis, not domination. The nastiest of these superindividuals are those that operate behind the scenes, intentionally controlling and influencing individuals without their knowledge. These are often referred to under a collective term: the "Illuminati", the glowing ones, the "good" people, the circle of initiates.

Look at a new world with open eyes. Break out of the system. Only after doing so, can you understand what you can do for society. (And don't forget to ask yourself if I am, in fact, just a nutty conspiracy theorist trying to see something where nothing exists. That possibility exists, you know.)

---

1. Wasn't it an exquisite coincidence for this incident to happen in 1984?

2. Here's a present for the libertarians: if the right of ownership is sacred, why do people not respect it when it comes to music CDs, etc.? Would you? *Why* is the market unable to solve this problem, if the legislature is really so powerless? Say, are there any problems that can't be solved either by the market or the state?

3. This word is one of those that have escaped down from the esoteric, academic levels into normal language. Be careful if you use it around people with scientific training, since the keyword of science is *precision* - paradigm means one specific thing, not a category. Using the word outside the philosophy of science could be viewed as a vulgar, though common, practice. The opposite of scientific language is found in New Age culture, where it's important to be as fuzzy and imprecise as possible. Popular culture, of which this book is an example, must attempt a balancing act between these two extremes.

4. Bernstein, who was originally a linguist, belongs to some structuralist or post-structuralist school of thought, which isn't really too important in this context.

Chapter 16
THE FUTURE

This book's coming to an end soon, and I should make some predictions of what we can expect on the electronic front in the days to come. If you want a nightmarish vision, then you could read my futuristic novel-in-progress called *Digitala Dagar* ("Digital Days")[(1)], but this is science fiction. However, the book is relevant to what follows - which is my personal predictions, not pure fact. Everything I write from this point on is speculation, and since the future is always in motion, I might reconsider the points I'm about to put forth.

The electronic universe is actually a new world, which we call cyberspace. It is a place where small communities of information have been allowed to exist in the state of a sort of loosely organized anarchy. Cyberspace is in the process of becoming civilized as it grows. Within a decade or so, everyone in this country will have access to the Internet and be part of the electronic community, and just like all other communities it suffers from crime and internal conflicts.At the same time, the human factor is always present. Cyberspace is a place occupied by people, and wherever you find people, you find politics and culture. As a tool, the computer is unbeatable; it can construct and visualize with a unique precision. Electronic art is not a fad, but something we will see more and more. The musicians and painters of the future will leave traditional methods and migrate to virtual reality and instruments that don't exist as of yet. Motor skills and rhythm won't be required to make music. The ability to mix colors and execute pen strokes won't be required to make art. The only prerequisites will be imagination and the ability to use technology - which becomes easier and easier to use. Artists who only work with artificial worlds, *spacemakers*, will basically be able to act as *gods* in the artificial realities - for better and worse. (Nietzsche's statement that God is dead is frighteningly tangible in a virtual reality). Perhaps professional artists will go away in favor of a large number of amateurs following the introduction of advanced technology into the mainstream.

In early computer art, such as demos, the computer was used like a musical instrument. Just as a guitarist finds hidden attributes in his or her instrument when he/she finds out it's possible to play *flageolets*, or notes affected by the physical characteristics of the string, early computer artists found hidden potential in their machines. This was particularly the case with the C64 and Atari ST. Modern computer art is more a matter of constraint - in virtual reality, *everything* is possible: it's the nightmare of the canvas. It's easy to overdo it and become totally incoherent.

Like I said before, the digital universe is just a mirror image of the "real" one. The only thing that's really *strange* about cyberspace is the sudden *proximity* of information and other people, and the breathtaking boost in cultural and social evolution that this proximity causes. We hate it for its distorted image of ourselves, reflected as if by a twisted mirror. The behavior patterns of people are ever so obvious within the framework of a computer. Soon, our society will be so interlinked and complex that it will become as dependent on computers as our bodies are on a circulatory system. There is (unfortunately?) absolutely no return. Not even now, today, can we turn back. Our last chance to guide society away from computerization

came and went with the 50's. It's not a question of computers or not - it's a question of how to use them.

The new communication channels will fundamentally change the way public opinion is formed. There will be more responsibility on the part of the individual for sorting information. If Swedish youth would suddenly start showing a great interest in certain suspect publications, many people would probably react strongly to this. There would be a public debate of the publications' agenda and opinions.We have no control over electronic publication. No one knows the distribution size, how many copies exist, and when a reader has viewed the paper, it's erased from the computer's memory, leaving nothing - except new ideas, thoughts, and opinions in the brain of the reader. The only way to find out what a person reads electronically, is by monitoring him or her at all times. The responsibility for forming public opinion will wholly or partially shift *from* society and established media to the individual. Media will have a hard time keeping track of all the interest groups that will arise. All people will be forced to think on their own, whether they want to or not.

The possibility of having an opinion without having to stand up for it is considerable. If political discussions to a greater extent are held electronically, on the Internet and on BBSs, it becomes virtually *impossible* to resort to personal attacks on people with different views, since every modern conferencing system contains the often-used option of remaining anonymous (under a pseudonym). The rhetoric of public debate will certainly also change in accordance with Rule #3: *distrust authority.* By extension: distrust the entire social hierarchy. Power *always* corrupts; the fourth state - the media - is no exception.

The chronicling of history won't be as geographically centered as before. It won't be possible to say that *"this idea emerged in Chicago, USA, around 1997"*. Maybe not even what people were involved. Ideas and social perspectives will spread globally almost instantly. Opinions, ideologies, and innovations of all kinds will be created in the discussion groups on the networks, and they'll be created on a global level and by people from totally different walks of life. Some will be CEOs, some will be thieves, some 70 years old and some 14. The most important thing will be the ability to articulate oneself. No one cares what you look like, where you're from, or how you dress. Perhaps there will be a distinction between ideas that have originated in cyberspace and those that haven't. Debates will be held between those who are interested and seek out the discussion by themselves, not by "pundits". The distance between debaters will become *purely* intellectual.

Social self-censorship (which means that, for example, publications which defend the use of drugs don't get press subsidies and are consistently resisted) doesn't exist on the networks. Instead, it's up to the individual to decide what's right and wrong. Instead of hiding behind an editor-in-chief, you have to stand for what you write. This tendency is notable in the daily press, where it's become more of a rule to sign articles.

Putting an interactive terminal in the hands of a normal person means considerable change. At first, it's not terribly exciting. You discover the Internet through the World Wide Web, which isn't much more captivating than a library or a TV program. It is one-way information for the individual, and not very interactive. Today, the big companies and institutions largely control the World Wide Web, even though there

are brilliant exceptions. It's not too surprising that the small amount of material that isn't commercial has been produced either by public institutions or hackers.

But then, you hopefully discover Usenet, where you can *discuss* anything between heaven and Earth without being spoon-fed ready-made solutions by experts. You might discover IRC, where you can hold real-time conversations with other people from anywhere in the world. And then you discover that you have many equals, and even that you're an expert on many things, and that your own knowledge is valuable. Then, things start to happen in the homes around the country. Swedes are transformed from passive consumers to interactive world citizens, and this is the real digital revolution. If no *market forces* (Telia, Microsoft, etc.) succeed in stopping, commercializing, or obscuring it before it has a chance to grow…

It's the case that this planet we inhabit, Spaceship Earth, is starting to become so internationalized that all the people aboard are starting to develop certain common values. It's a rough, uphill ride, but it's happening everywhere. Information technology, especially the two-way kind, will be the decidedly most important link in a society that can stand united in Sweden and Australia as well as in Japan and on Madagascar. This demands communication free from monopoly, and freedom of information. I am convinced that we will find a compromise.

A few years ago, many politicians and sci-fi authors cautioned us about the risk that information technology would be used to control people *everywhere*. (The examples used included **Ira Levin's** *One Fine Day,* **Karin Boyes'** *Kallocain*, and **George Orwell's** *1984*.) This is what organizations like the EFF want to stop at all costs. The encryption program PGP was created *just for this purpose*, and this gift should be considered a social good deed. The encryption expert, Zimmerman, is maybe deserving of the Nobel Peace Prize for his service to the protection of "healthy disobedience".

When I was younger, I had a diary with a small lock on it. Many adults have one too. Now I don't need to lock my computer, because encryption is enough. It's in any case much more effective than physical locks for protecting information. The problem is that criminal investigators, for example, may very well consider my diary part of the investigation material. I don't think so. My thoughts belong only to me, and I'm not going to abandon them to anyone. The desire to read other people's diaries is, in my view, just a step on the way to the desire to read other people's thoughts. Diaries are an improvement of one's memory, an extension of the intellect. Where is the person? In the body, or in the diary, or both? Some diary-keeping people discover details of their past that their brains have forgotten… *"My actions occur in my body, but parts of my mind are on the bookshelf"*. Yes, we're information-processing individuals, all right. And information technology is so many times better than a library ever was at storing and processing information.

If you want to write anything hidden from the mafia, the government, or your family, you should use encryption. The possibility to erect a "firewall" against the oversight of authorities is vital to any democracy. PGP, in one swoop, puts humanity's collected mathematical science between you and the superior powers. Zimmerman's crypto also allows you to set up "bug-free" communication channels.[(2)] Encryption is a fact, and I suggest that anyone who wants a bit of personal freedom and privacy use it. I'm not

going to deny that well-applied encryption will make it impossible to stop nazi propaganda, child pornography, violent movies, and that it can partially protect criminal syndicates. I'm split on this issue, but I ultimately think that it's worth the price to protect the private lives of individuals from governmental, corporate, and organizational control. Furthermore, there's already crypto around the homes of the country. As for me, I got my copy of PGP on a CD supplied with the magazine Mikrodatorn (a Swedish home computing magazine), and which can be found in any well-stocked library. No authority in the world has the possibility to decrypt information that's been encrypted, using today's technology. Prometheus has already stolen fire from the gods, and no one can call it back.

I observe the changes in society with excitement: encryption can perhaps end the *Pepto-bismol policies* that, for example, in the case of child pornography, treat the symptoms instead of the disease. For we all have to conclude that it's not pornography *in itself* which is the problem, but rather that there is *demand* for it. This, however, is a harder problem to address…

It wouldn't surprise me at all if there was soon another debate about prohibition in our stuck-up Swedish media. A debate such as the one in 1980, which started when Kulturarbetarnas Socialdemokratiska Förening (the Social Democratic Association of Culture Workers) wanted to prohibit TV satellite dishes in order to prevent Swedish residents from watching unsuitable television programs. (Which, in retrospect, looks pretty absurd). Of course - attack technology, there's never anything wrong with people.

The debate will naturally be caused by something that upsets the average family: drugs, pornography, political or religious extremists. All of this is now available on the Internet, mostly in the form of text or pictures. Tomorrow, it'll be there in the form of sound and motion pictures. In the future, it might be some form of virtual reality. The U.S. Congress has *tried* to prohibit effective crypto, and the European Union has issued directives banning un-crackable encryption. Naturally, nothing will come of either one, at least nothing that will be respected any more than the prohibition of, say, jaywalking. Human nature includes an ability to resist every form of thought control. (Or should we call it information control?)

If people have any sense (and they do), they'll realize that we're dealing with international problems. Mom and apple pie are disintegrating, and the problems of the world are approaching from every direction. At some point, perhaps we'll realize the need of *even more* international cooperation, and of course it's just as difficult to keep international problems outside the EU as it is to keep them out of Sweden. The information society grows towards internationalization by its own force. All of this thanks to some hackers who created ARPAnet, later to become Internet, and which interconnected the whole world, for better or for worse. The change has just begun. It is without doubt the most beautiful, magnificent *hack* ever executed. The university hackers hacked down barriers between educational institutes, then between countries, economic interests - and yes, between *people*. Maybe I'm being a bit dramatic, but you know what I mean.

Rave culture and electronic pop music aren't fads - we'll get more and more of them, more genres, and we'll educate professional musicians who've never played anything

but techno music, even at public institutions. The joy and vitality of rave culture's futuristic shows yields optimism and a belief in the future. With luck, rave culture will become for today's youth what 60's rock was for the baby-boomers; a symbol of rebellion, identity, and creative thinking. And in contrast to dystopic cyberpunk and many other modern trends, it is *happy and optimistic*, not regressive or doomsaying. The same goes for many other forms of electronic culture, including electronic film as well as multimedia and online culture.

The most prominent danger to democracy in conjunction with new technology is the risk that not *everyone* will have access to it. In the US, almost every well-to-do middle-class family has a computer, and even a modem. In the ghettos and industrial suburbs, it's a pipedream. In Sweden, where the gap between classes is not as wide as in the States, there's a marked risk that the gap will *increase* if not *everyone* has access to computer technology. If not, information will be available only to those who can afford it. Remember the second rule of hacker ethics: *All information should be free*. Internet and public computers at all the schools and libraries around the country, even grade schools and community colleges, is a given. A computer for each student is desirable. State subsidies for computer equipment is a valid issue.

I'm fully aware that I express political opinions now, and I'm placing myself squarely against those who think that technology, high-level jobs, etc. should be reserved for the elite. Neither do I look up to hackers that are just out to show off and don't care about anyone else. Following political and economic democracy, we're now approaching a democracy of information. Information for the people, perhaps. It's my hope that information technology will provide the foundation for a more democratic society than we have today.

You should think before judging a hacker. A hacker is generally a middle-class youth who have acquired possibilities that normally only the richest upper-class kids can revel in, using computer technology. They've done this simply by going out there and grabbing everything possible. Isn't this really what our whole modern, class-based society's rules of the game are all about - that the privileged should be able to pick and choose, but the less privileged get long sentences if they try to get some of the goodies?

To categorically state that hackers, phreakers, virus makers, or crackers are public enemies is bullshit. It's simply pointing to superficial factors and appealing to authority. Saying that a phreaker, taking some phone time in a fiber cable to talk to his buddies in the States, is a thief because the law says so, is placing 100% trust in the makers of the law. It's reducing the problem to legal text. It's a senseless oversimplification. Every law is constantly in motion - that's how it actually works. You're one of the people that are obligated to change the law if you realize that it is wrong.

Isn't the real crime of the hacker that of challenging values and power structures that seek to distribute influence and property unequally? For his or her own gain in the beginning, certainly, but still. The true crime of the hacker is perhaps that he or she has "cracked" *human software*, the social protocol that's been programmed into out minds since birth.

And the university hackers - without them, we wouldn't have *any* of the computer technology we have today. All new ideas of any worth have emerged at MIT, Stanford, or Berkeley, by kids who've worked passionately for minimal pay and under uncertain employment terms. And most of them haven't earned a dime of profit from their inventions. Instead, IBM, Microsoft, and the other giants have raked in the profits. And the hackers are not at all upset! They think that technology - information - should belong to everyone. They never had any commercial interests. They thought it was *fun!*

On the pinball games at the autonomous rave and anarchist club **Wapiti** in Lund, Sweden, the text OBEY AUTHORITY is sarcastically displayed on the kitschy LED screens. Man has assumed control of the machine.

---

1. And I'm damned if I know if I'll ever work on that project again.

2. Currently limited to electronic mail, but a telephone version is under development.

Chapter 17
A CYBERNETIC UTOPIA

In an ideological utopia, one can discern a decentralized community with the perfect technology for creating virtual reality, in which really only technology, communication, the legal system, and food production has to be state regulated. (Everything else can be synthesized in artificial reality). What the individual engages in in his or her virtual reality - like electronic dreams - should be protected from all governmental control. Perversions and aggressions can be realized without putting other people in danger. Therefore, it is suggested that people would become more harmonious creatures, with a mind free from the oppressive norms of society, finding their way back to the *real* values. (Whatever they may be). It's about disconnecting the individual consciousness from the collective consciousness - for better and for worse.

In such a cyber-utopia, the real reality and nature have lost their meaning, since you can experience an artificial one that's much better. In a cyber-utopia, people are driven by group fellowship to explore the world. Small interest groups can research their areas and communicate over the networks. All boring, dangerous and monotonous work is conducted by robots. *"Humankind should concern itself with love, science, and art"*, to cite a famous Swedish rock band.

In a cyber-utopia, you can meet people all over the world and still be at home, physically speaking. Humanity is just a keystroke away. This utopia (like all others) naturally has obvious drawbacks, but this is the way it is. (Myself, I think it's horrible). For example, one could debate the wisdom of letting pedophiles, for example, live out their dreams in a virtual reality. Totally new political issues are raised in such a community: should we regulate people's actions, or is it - terrible thought - actually their *thoughts* that we want to regulate?

The cyberpunks want you to be able to think and enact anything without harming others, and technology might give us this possibility - but do we really want *everyone* to be able to realize their fantasies, *even* if it doesn't harm anyone? Several philosophers have pointed out the risk of living in a society without stable norms. Is the repression of thought necessary to protect humankind? Can technology aid us in finding those functions that connect our individual consciousnesses with the collective by giving us the opportunity to "disconnect"? Can today's outsiders find their way into society with the assistance of technology?

People who *like* monotonous work, who think that intellectual exercises are boring, or who would rather engage in sports or hunting, wouldn't have a place in a cybernetic society. On the other hand - if you had grown up in such a society - what's suggesting that you would put any value on such trivial matters? A lot of our current society would seem inhuman and despicable to a person originating in the 1700s.

And as for the artificial intelligence that has to exist in order to create this partially artificial world we already live in - does *it* have any rights? Do we really have the right to use artificial intelligences as slaves, as we currently use social hierarchies to make other people work for us? Machines are actually already part of the collective

consciousness I call superindividuals - they're already thinking along with us. The information age focuses on these new ethical issues and forces us to consider them.

If you're frightened by cyberpunk and the information revolution, I'm afraid I'll have to say that they're not so easy to stop. What you can do is learning more and helping to control the development of society towards a desirable state. If you're passive, you leave decision making up to others. Begin by *understanding* that which you criticize, and only then can you start influencing things. Reprimands and threats have very little effect on my generation. If someone complains enough to bother us, we just switch the channel. (Zap!). Don't think that we're not interested in your views, however. We listen - if you know what you're talking about. The suggested literature section at the end of this book is a good start if you want to learn more.

One thing that radically distinguished the information revolution from the industrial revolution is that many people have been prepared and have had time to become learned in the ways of technology. The development of society is *questioned* in broad circles, and isn't left up to politicians and corporations. People in general, and especially young people, question and critique. Hackers, cyberpunks, ravers, and others are the most questioning - they want to be part of creating their own future, and refuse to passively meld into the pattern. They have optimism and a belief in the future, and they rush to meet it. This youth movement is sometimes referred to as the *New Edge*. These children of the information age don't see only threats, but possibilities.

I'm not a doomsayer, and this is not a dark book. As wise as I am, I've saved the most important point for last. There's been a lot of complaining lately. Many contemporary philosophers have suggested that humankind has locked itself into a pattern of progression, in which consumption has to constantly increase until people just can't consume anymore. This is probably true. We will consume more. Further, they think that this will lead to environmental decay and global segregation, which will eradicate all of humanity. This, however, probably isn't true. It's not true because those who speak in these pessimistic terms have been incapable of noticing a very important contemporary detail: the entrance of the information society. More precisely, the mistake has been to presume that a constantly increased level of consumption necessarily *requires* an increased consumption of natural resources. There is no such relationship in the information society. (I might add that I'm perhaps a little too optimistic in reference to the connection between information society and environmental concerns; environmental problems won't go away, but the continuing damage will decrease).

On the day I'm writing this, Microsoft's new operating system, Windows 95, has been released with much fanfare at the *Globe* in Stockholm. I have previously expressed my negative attitude toward this company. Still, it makes me happy to see that national media are reporting this massive marketing effort of a product that ten years ago *no one* could even *imagine* would be sold through galas at the Globe and on TV commercials. It would have been *ridiculous*. Windows 95 is software, a pure information product. Granted, you get some disks and a book when you buy the program, but those are not the actual product. It's perfectly possible to buy Windows 95 without the books or the disks if you buy a new computer where the program is pre-installed on the hard drive.

Thus, a product is being sold which, compared to a car, required almost no natural resources to produce, even though it cost thousands of hours of work to develop, and will cost *billions* of hours to consume. When I sit down with this software at home, wrestle with it, create with it and try to make it do my bidding - during this time, I'm not driving a car. I don't consume anything, save for a little electricity and maybe some coffee. I don't eat potato chips, because I don't want the computer to get greasy. (Translator's note: Habits vary. I drink *beer*, smoke *cigarettes*, and eat *pizza* in front of my computer. The main difference is that I probably have to switch keyboards more often.) I don't buy a lot of useless items from the shopping channels on TV that I later just throw away. I basically consume nothing but information. Not even a *book* is more environmentally friendly. The same phenomenon occurs in most of the rest of the information society - TV: an electronically transmitted product with low demands on natural resources, Multimedia: also primarily an information product, Telephony: an electrical signal from one place to another. Using virtual reality, we can even consume everything we usually do, offroad a four-wheel Jeep, and pilot a spaceship, with no notable wear on nature. There is hope. There is a hell of a lot of hope, even though it's combined with new dangers.

You can note that many of today's products satisfy artificial needs. You could ask whether we ever needed an operating system like Windows 95. Probably not. In a few years, however, we do. This is really not that important - more needs than we think are ultimately artificial. It's sort of like a premise for a market economy. Your mind reels at the thought of security companies that hire a team of hackers to build security systems for their customers, and then, at night, make sure that the same hackers *"maintain market image"*. Or virus hackers that work half the time on creating virus killing software, and the other half on creating new viruses to create demand for the antivirus tools. *Wouldn't you?* Of course you would. So what? The gears are spinning, GNP goes up, everyone's happy. In the same way, we've created a dependency on criminal activity, administrative tasks, etc. to no end in this society. There are many such processes, whose only purpose is self-perpetuation and self-justification. Does it matter? No, probably not. It depends on whether or not you think humanity has a "purpose"; whether there is something we should strive towards. But that's philosophy.

We have moved from material bartering, with merchandise for merchandise, to an economy in which we trade money for goods and goods for money. Now, we're starting an infonomy, trading information for information without intermediary material transactions. The danger that still lurks behind the scenes of our system is a desire for power, in individuals at all levels: corporations, governments, and organizations. They're after power over *you*. Make sure you don't give up any of your freedom without first knowing what you get in exchange.

I've reached the slightly shocking conclusion that the mechanisms I previously identified as *superindividuals*, i. e. superior intelligent entities, have no need to produce material products or artifacts in order to control other intelligent entities. Instead, they simply employ exchanges of symbolic information, chunks of info transmitted through cables. Every such superindividual is characterized by the creation of internal chinks of information, secret documents, transmitted inside the individual outside the reach of the public or other superindividuals. That's why corporations, governments, and other organizations are paranoid about someone else

reading their secrets, whether important or not. With information technology, the possibility of creating such structures is amplified by a factor of hundreds, and the exchange of information, the thoughts of the superindividual, its intelligence, is expanding at the speed of light. I've also discovered that the information-processing machines are *part* of these superindividuals, not some accessory of people to assist in their work. Somewhere around this point is where you have to start thinking for yourself.

If *you* have read *this* book on a computer, without printing it out on paper, you've consumed something. Or have you? Do I have to charge for this book before it can be called consumption? I'll leave that as an open question. I've certainly not made a dime from you reading this book, but maybe I've accomplished something that can't be measured in terms of money - maybe I've taught you to question the mechanisms of power. (Hmm… if this book ever goes into print, I'll have to modify the above paragraph).

Let me finish with a timeless quote, from a man who belonged at the frontline of his generation:

> *"Come mothers and fathers throughout the land*
> *and don't criticize what ya can't understand*
> *your sons and your daughters are beyond your command*
> *your old road is rapidly aging*
> *please get out of the new one if ya can't lend your hand*
> *for the times they are a-changin'"*
>
> **Bob Dylan**, September 1963.

We are all part of the inevitable.

Linus Walleij, Lund, Sweden, September 5, 1995.
Binary sculptor, harmless hobby hacker.

Translation by Daniel Arnrup, Bergen, Norway, October 30, 1999.

Thanks to: The libraries of Ljungby and Svalöv, the university libraries of Lund and Linköping, Microbus i Ljungby AB, Gunnar Kålbäck, Christian Lüddeckens, Motley, Tranziie, Mikael Jägerbrand, Ulf Härnhammar, Marie Fredriksson, Christer Sturmark, Hans Roos, Erica Larsson, Daniel Hellsson, Jucke, Chorus, Stellan Andersson, Anders Hellquist, Anders R Olsson, Jesper Jansson, David Malmborg, Daniel Näslund, Mikael Winterkvist, Per Jacobsson, Fredrik Schön and all the members of the Triad and Fairlight hacking groups, without whose help this wouldn't have been possible. Now I'm gonna sit down and finish my cyberpunk novel. Maybe.

And I refuse to say whether the Dylan quote above was meant seriously or ironically.

Literature:
Scientific literature tends to consist of 70% of cross-references to other works and other authors, which makes the whole thing difficult and slow to read for an uninitiated reader. This is not a scientific text. Possibly, it's popular science. Most of

this text is written on the fly, based on my own experience and knowledge. For those who would like to read more, I'm listing a few books, publications, and such which have served as a factual basis for the book.

Barlow, John Perry:*Selling Wine Without Bottles*

An article published in Wired about information and "intellectual property". So initiating and well considered that I've referred to it as a "paradigm".

Burroughs, William Seward: *The Naked Lunch*

Burroughs' breakthrough, unfortunately not as articulate a social critique as the subsequent *Nova Express*. Counted as a milepost within the literary tradition of cut-up.

Burroughs, William Seward: *Nova Express*

Run for your lives! The Nova Mafia has sent agents to the Earth to enslave human thought patterns through language, drugs and sex. Luckily, the Nova Police have sent out counteragents, including Burroughs himself, to stop the invasion. In this cut-up sci-fi novel, Burroughs develops the ideas form *The Naked Lunch* to an astronomical perspective. By affording the reader a solid sense of paranoia, he makes you question your surrounding reality. There's also a hint of ironic humor underneath it all.

Cornwall, Hugo: Datatheft

Heinemann Professional Publishing Ltd, England, 1987.
ISBN 0-7493-0217-8

One of the most in-depth books ever written about computer security. Cornwall brings up many common security flaws in computers and security systems in a general and broad perspective. Hackers are only mentioned occasionally, and the book is heavy and rather strictly scientific.

Cornwall, Hugo: *Hacker's Handbook III*

This is a handbook for network hackers. Nobody's learned to be a hacker by reading this book, but despite this it's quite interesting, and a given best-seller among people who think that the network hacking thing is the coolest thing around (i. e., wannabes). Additionally, the title seems "forbidden". However, it is a well-written book that points out the most common security holes in certain systems.

Datormagazin

Yearly issues 1986-94

Dick, Philip K.: *Do Androids Dream of Electric Sheep?*

Forrester, Tom & Morrison, Perry: *Computer Ethics*

Basil Blackwell Ltd, England, 1990
ISBN 0-631-17242-4

One of the most interesting books written about computers and computing society. Many examples are based on English conditions, and uninteresting for Swedish readers. The purely ethical issues around hacking, artificial intelligence, databases etc. are fascinatingly treated.

Gibson, William: *Neuromancer*

Harper Collins Science Fiction & Fantasy, 1993
ISBN 0-586-06645-4

If you're going to read any cyberpunk literature at all, read this one. It's a classic which defines the literary term of cyberpunk.

Green, Jesper 69 & Johansson, Sune: *Cyberworld*

Alfabeta Bokförlag AB 1994
ISBN 91-7712-389-1

Many reviewers trashed this book when it came out. In some respects it was deserving of this, in others, not. All examples from the book are drawn from a Danish perspective, which may make it less interesting. On the other hand, the delusional predictions of the future of the cyberpunk author, Green, is something not to miss. There are many quotes from the Danish network hacker, Netrunner, and the Kraftwerk member Ralf Hütter, which elevate the book.

Hafner, Katie & Markoff, John: *Cyberpunk - Outlaws and Hackers on the Computer Frontier*

Corgi Books, England 1994
ISBN 0-552-13963-7

This book contains biographies of the most famous network hackers: Kevin Mitnick, Pengo, and Robert Tappan Morris. It's written in a typically American fashion, with many irrelevant details, and has the advantage of being relatively easy to read. You get a good view of the hacker's life and mind.

Harry, M: *The Computer Underground*

Loompanics Unlimited, Port Townsend 1985
ISBN 0-915179-31-8

One of the first books about underground computer culture. Loompanics is one of those publishers that print just about anything and doesn't censor content for being politically incorrect. Among other things, they have wide range of Timothy Leary's books.

Hofstadter, Douglas R: *Gödel, Escher, Bach: An Eternal Golden Braid*

Timeless classic and cult book among all computer science students. A thick, heavy book which explains why math is fun, and why the innermost essence of intelligence can be captured in a machine. To top it off, it's written with a good dose of distance and humor, with simple, easy-to-understand examples. People who have recently read the book for the first time often speak of it in an almost religious manner.

Illegal (edited by **Jeff Smart**)

"22 - "37
Germany, 1987-89

Probably the only significant European cracking zine. It's from this zine that cracking culture spread across Europe, primarily Germany, and then to the rest of the world, and it possibly for the first time defined the concept of "elite" among European home computer enthusiasts.

In Medias Res (edited by **Zike**), #1

Eskilstuna, Sweden, 1992

One of those surprisingly well done and thorough little zines which many refer to, but was never printed in a large run. And it's not in the national archives, either. But I have a copy…

Kuhn, Thomas S: *The Structure of Scientific Revolutions*

Phoenix Books, USA1962

Kurzweil, Raymond: *The Age of Intelligent Machines*

This is an anthology of thoughts around artificial intelligence. If you want to know what AI is, and consider social and philosophical problems, then read this book. If you want to know how AI works, then read Hofstadter's *Gödel Escher Bach: An Eternal Golden Braid* (see above) instead. Hofstadter and **Sherry Turkle** are also contributing writers in this book.

Landreth, Bill: *Out of the Inner Circle*

This is a classic among network hackers. It's written by a renegade from the *Inner Circle* hacking group, and it's pretty well-done. It has, however, lost some of its immediacy.

Leary, Timothy: *Flashbacks - A Personal and Cultural History of an Era*

Tarcher / Putnam Books, New York 1990
ISBN 0-87477-497-7

Tells of large parts of 60's hippie history that has later been covered up or stigmatized. Leary was feeling pretty good about life and society and himself when he wrote this self-biography, and you get the impression that he is an incurable optimist. He is a

man of the arts, and well-read… obviously a dangerous enemy to his opponents. Leary died in 1996, and ironically, the Harvard LSD experiments that started his career have been resumed.

Levy, Steven: *Hackers - Heroes of the Computer Revolution*

Penguin books, England 1994 (first printed 1984)
ISBN 0-14-023269-9

This is the best book ever written about hackers. It concerns the first hackers at MIT in the 60's, the home computer builder of the Altair, and the programmers at the Sierra On-Line gaming company. The first two parts are the most interesting. Read it.

Nietzsche, Friedrich: *Thus Spake Zarathustra*

It takes some courage to read Nietzsche. If you expect to find a fascistic manifesto, you're reading in vain. Those who can't get around Nietzsche's thinking will think that the book is "strange", and won't understand what Zarathustra is talking about. Zarathustra was a Persian philosopher, and Nietzsche resurrects him in this book to "revise" the earlier teachings of good and evil.

Petiska, Eduard: *Golem*

Martin publishing house, 1991
ISBN 80-900129-2-2

This is the myth of Rabbi Löw's Golem, created to protect the Jewish ghetto in Prague. I read it as part of the research on the section about artificial intelligence, and it doesn't have very much to do with the information society.

Pondsmith, Mike (ed.): *Cyberpunk - The Roleplaying Game of the Dark Future* (Version 2.0.2.0)

R. Talsorian Games Incorporated, California 1993
ISBN 0-937-279-13-7

If you're not used to reading role-playing games, this book will probably confuse you. Role-playing game books contain little or no fictional material. At first glance it looks like an encyclopaedia full of facts - except everything is made-up. A role-playing game book contains descriptions of organizations, people, machines, weapons, and everything between Heaven and Earth to assist the players' imaginations. When you've read the book, the idea is to get together and develop the story using the book as a reference for the world. The result is something like a mix of authoring, theater, and boardgames.

Rubin, Jerry: *Do It!*

An instruction manual on how to become a yippie. A very sociopathic book by one of the leaders of the American yippie movement. On the cover page it says "Read this

book high", and that's about as good as it gets. If your tastes are a bit morbid, you could see it as humor. Otherwise it's just plain horrible.

Shea, Robert & Wilson, Robert Anton: *Illuminatus!*

Consists of three novels: *The Eye in the Pyramid, The Golden Apple* and *Leviathan*.
Dell Publishing, New York 1988 (1975)
ISBN 0-440-53981-1

This book is mentioned in several places of my text, among others in connection with the hacker Karl Koch and the techno band KLF. It's also recommended as a suitable read for hackers at the end of *The Jargon File* (see below). The books are conspiracy theories about ourselves and our society, primarily inspired by William S. Burroughs and Timothy Leary. They're cult books in the US as well as Canada and the UK, and there's no good reason why they haven't been translated into Swedish. Actually, there's one: they're painfully politically incorrect. The narrative technique of these novels has been adopted by **Douglas Adams**, among others.

Sterling, Bruce: *The Hacker Crackdown*

Bantam Books, USA 1992
ISBN 0-553-08058-1

A book about hackers written by a complete outsider. Sterling normally writes cyberpunk novels. The book is available at no charge as a text file on the Internet via EFF. The most exciting and creative chapters are those about the American Secret Service and their fight against hacking and phreaking, and the story of how EFF was created.

Stoll, Clifford: *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*

A much-discussed book in which Stoll, with passion, recounts how he traced the hacker (Mattias Hess) who broke into his computer system and used it as a springboard to search for military secrets for the Warsaw Pact (the Russians, Reds or whatever you want to call them).

Turkle, Sherry: The Second Self: Computers and the Human Spirit

Sherry touches upon sociological and psychological aspects of the interplay between humans and computers. She interviews children and hackers as well as computer scientists, and draws conclusions about the computer community from a sociological standpoint. Towards the end of the book she also ventures into artificial intelligence.

Yourgrau, Palle: *The Disappearance of Time - Kurt Gödel and the Idealistic Tradition in Philosophy*

Cambridge university press 1991
ISBN 0-521-41012-6

***Electronic Documents and Magazines*:**

40hex # 1-12

Phalcon / SKISM

Pretty well-written, treats most things related to virus manufacture and virus culture.

Bausson, Stephane: *What You Need to Know About Electronic Telecards*

V. 1.12. Last Revised 05/18/95

Described the inner workings of Telia's phone cards. Very embarrassing for Telia, since they thought this information was secret when I called and asked them. It's not.

Brent, Doug: *Oral knowledge, Typographic knowledge, Electronic knowledge: Speculations on the history of ownership*

(Article in EJournal #3 Vol 1, ISSN 1054-1055)

This is a very important article which I used as a basis for the section on *cybernetic society vs. copyright*. Brent is active at Calgary university, and shows with all clarity why it's more difficult to own information in an information society.

Drummond, Bill & Cauty, Jimmy: *The Manual - How to Have a Number One the Easy Way*

KLF Communications 1988

In case you were wondering: it works. Everything in this book is completely true. Among those who have tried Drummond and Cauty's recipes for hit singles, we find the Austrian group Edelweis plus a hundred or so other artists who don't dare reveal that they've just followed the instructions in this book. Even Swedish talents like Denniz Pop or Pat Reiniz have, consciously or subconsciously, managed to follow this manual point for point. If you want to know how it's done, read this book. You need a certain distance to be able to grasp the contents - it's a thorn in the side to the entire pop industry. Copies of this book, and bootlegs of the same, are circulated under much hush-hush among the amateurs of the music world. This is unnecessary, since someone's "liberated" the text and put it on the Internet. KLF themselves presumably don't care one whit about this.

Gunzenbomz Pyro-Technologies / Chaos Industries: *The Terrorists Handbook*

Probably one or more printed books from the beginning. This very text file created a great deal of press attention when a couple of 15-year-olds got it off a BBS and showed it to Expressen (a Swedish daily). Too bad Expressen didn't review the book, because it has some comic value. I can't judge how useful or dangerous the descriptions in the book are, but it's obvious that you have to be a little crazy to even

attempt to use the bomb recipes. And that's the problem: many parents apparently think that their 15-year-old sons are completely mad.

Jammer, the & Jack the Ripper (pseud.): *The Official Phreaker's Manual V1.1*

Last revised in 1987

Describes most of the technique and history of phreaking. Contains, among other things, the articles written by Ron Rosenbaum about the phreakers John draper (Cap'n Crunch) and Joe Engrassia in Esquire in 1971.

Raymond, Eric S: *The Jargon File 3.2.0*

Last revised on 03/21/95

This is the same as *The Hacker's Dictionary*, only free an in electronic form. Unfortunately, the text gives a somewhat disparaging view of anyone who is not a "real" hacker, i.e. the intellectual elite at universities like MIT. This file is regularly updates, and attempts to include international hacker culture, which it hasn't been terribly successful with so far. The content is heavily adapted to American phenomena.

Reid, Elizabeth: *Cultural Forms in Text-Based Realities*

Cultural studies program ,Department of English, University of Melbourne, January 1994

Brotherhood of Warez # 1-4

One of the most entertaining phreaker publications, it is published by the Brotherhood of Warez (BoW) group. It's a constant mix of humor and seriousness, where it's hard to discern real statements from sarcastic lies written by bored pirates. If you like Generation X-humor, you'll probably like BoW. The leader of the group, U4EA, was sentenced to jail after driving the Gray Areas magazine crazy withrage. (I think - it could have been a sarcastic lie).

Phrack #1-48

Infamous hacker/phreaker magazine which plays a large role in Bruce Sterling's *The Hacker Crackdown* (see above). Offers sensible as well as really sick opinions of the world and telephony. Has had a string of editors throughout the years. The article *The Conscience of a Hacker* in issue #7 is especially important. I've written an article about Swedish hackers that was published in issue #48 of this publication.

Skyhigh # 17

Camelot Productions 1995

An interesting article by **The Mistress**/Angry regarding women and hackers.

Surfpunk # 103 and 105

Cyberpunk magazine, full of excerpts from Usenet newsgroups and various publications. Behind the paper is a more militant group than the EFF, but with similar views on society. They distribute heavily cyber-slanted opinions.

Swedish Hackers Association (SHA) (ed.): *Annual Year Protocol #3 & #4*

Our favorite hackers' own paper, SHA's insolent and somewhat arrogant "protocol" is a refreshing breeze compared to the government's and the media's condemning attitude towards the group. In these protocols, the SHA account for their activities, and why and how they do what they do. Guest writers include **Knight Lightning** from Legion of Doom, who was also one of the men behind Phrack (see above). The English is of mixed quality - it is obvious that Swedes wrote these "protocols". It's a required read for anyone who wants to know what both sides have to say about the issues.

All electronic documents are available from me directly, if not elsewhere.

Appendix
White Knight vs Otto Sync

On September 2, 1992, 25-year old Otto Sync (ficticious name) was arrested and charged with unauthorized use of the Datapak computer network. The infractions had taken place during November 1992, at the expense of Televerket. At the time, Televerket was a state-owned company with a monopoly on telecommunications in Sweden. The person who traced and ordered the arrest of Otto was Televerket's own "white knight" Pege Gustafsson, a zealous 38-year old security expert climbing the career ladder.

From December 1991 to February 1993, Otto was doing non-combat service in the French army, "Volontaire Service National en Enterprises", as an engineer working with PLC (computerized process controllers) at a French telecommunications company in Flen, Sweden. After having passed rigorous military tests, and with the help of a master's degree in engineering with credits in applied mathematics and computer science, he was offered the opportunity to perform his civil service in the French company's Swedish branch.

Being a lonely young Frenchman in Flen wasn't much fun; Otto tells us that the town was full of political refugees and the public mood wasn't the best -- the Swedish youths in Flen kept to themselves and saw him as yet another immigrant, and none of the other immigrants were French, but rather Iraquis, Kurds, Somalians and so forth. Additionally, Otto was unfamiliar with a small-town environment, as he had come straight from Lyon -- "Imagine my surprise when I arrived there alone mid December 1991... I've only lived in big cities before, and there is this place, without any bars, pubs or computer shops"[(1)] . As a result Otto spent most of his time alone in his apartment or in company office. "Flen is so boring I practically lived in the office building -- what else can you do there apart from hacking really?", as he says.

For the above reasons, Otto spent his time engaging in his favorite hobby: hacking. Otto was already a skilled hacker when he arrived in Flen, and as time passed he became even better. He became a regular at Swedens best hacker-BBS at the time: Synchron City. He explored every system he could reach: Televerket's public phone network, AT&T, Internet, and so on. However, none of this is very exciting to an experienced hacker in the long run: the phone network is very easy to trick, and the Internet was mostly full of regular people. Real hackers went for BBS:es on the X.25 network. As Otto wished to stay in touch with his hacker friends, he wanted to access the biggest hacker conference system at the time - *QSD* . QSD was only accessible through the international X.25 network. In trying to access QSD, he made a fatal mistake: exploring Televerket's Datapak network.

X.25 and Datapak

Datapak is a network which is structurally reminiscent of the Internet -- a packet-switched network, where the users share a few dedicated lines, and pay charges based on the amount of data transmitted on those lines (i.e., per packet). In general, it works in such a way that, using a modem, you call up Datapak through a so-called *PAD* connected to a 020-number (Swedish 800-number), then dial a number to a computer

permanently connected to Datapak. All computers on the Datapak network have datapak numbers in the same way that phones in the public network have phone numbers.

Of course you can also connect straight through Datapak in case you can afford a permanent connection for your computer, a method primarily used by large companies to connect their computer systems. That way, two computers can be permanently connected through Datapak (which would have been very expensive using regular modems) and thus you only have to pay charges for the information actually transmitted. Of course you can also connect through the computer network Datex, which is used by (among other things) ATMs, and it works like any other phone network, except that it's designed for computers.

Datapak is built around the X.25 standard , which describes how computers in the network are to "talk" to each other. Besides X.25, there are many other standards on the network, such as X.28 and X.75 , but as X.25 is the most common standard, the kind of network that Datapak belongs to is generally called an "X.25 network". The international X.25 network is thus made up of a number of interconnected computer networks, e g Datapak, Tymnet (which also manufactured the equipment used in the Swedish Datapak network), SPRINTnet, and so forth. Almost every big phone company in the industrialized world has their own X.25 network.

The international X.25 network has been running since the mid- and late 80's, but the Swedish Datpak network has never been very big. The reason for this is that X.25 was not targeted by the consumer market; X.25 is, as opposed to the common telephone networks, not designed for individuals. X.25 was from the beginning a network for corporations. The large consumer market that was conquered by the academic Internet system, which is based on multiple service providers and competition (as opposed to the X.25 market, which consists of oligopolies and only a few providers), is so fundamentally different that X.25 does not have a chance in this respect. X.25 is today mainly used for establishing logical links between private networks. X.25 is even used for some Internet links.

So, what Otto Sync didn't know, or didn't think of, when he ordered his Datapak subscription, was that Datapak was a small system in a small country, and that a person who tried to manipulate it would immediately be detected by the monitoring systems. The public phone network is quite safe to explore because of all the odd and random calls people make to strange places. A few cases of manipulation instantly disappear in the vast amount of calls, but *Datapak* was the backyard of a few subscribers. To enter the system was equal to walking around wearing emergency flashers on your head -- your presence was not very discreet. When Otto began scanning Datapak numbers, he finally drew Televerket's attention.

It is worth mentioning that Televerket had increased the monitoring of the Datapak network due to an enormous attack by the British hacker group 8LGM (8-Legged Groovin' Machine, a name taken from an 80's pop group) who had scanned 22,000 datapak number entries and accessed 380 computers all over the country about two years earlier.[(2)] Otto describes them as "a group of top-notch hackers who released 'exploits' advisories between 1991 and 1994". (Exploits are ready-to-use scripts that were used to get higher privileges, usually root-access, on Unix systems.) A

consequence of 8LGM's scans was that all activity on Datapak was now logged and analyzed.

Otto didn't subscribe to Datapak in order to use it -- as a matter of fact, he only subscribed in order to access the technical documentation given to every subscriber, so he could find out how the system worked. That way he learned that you connected to Datapak by dialing 020-910037 and submit your network user identity (NUI). After this you could call as much as you pleased using Datapak, and be charged per sent/recieved information packet at the end of the month . In the Datapak network the NUI is used for customer identification, as opposed to the common phone network where you are identified by your own wall socket and phone number.

But the Datapak manual from Televerket also contained some other interesting things, e. g. this example from page 4:

To connect with a user number, call 020-910037 using a modem. When the modem has answered, you write three dots followed by carriage return: ...<CR> (CR = carriage return, enter). Then write: N123456XYZ123-024037131270<CR>. N tells the computer that user identity and password follow, 123456 is the user number you got when you signed up for the subscription, XYZ123 is your secret password, and the figures after the dash is the host computer adress. (i. e., the computer you want to connect to.)

Further on in the manual, it illustrates how user 123456 changes password from BERTIL to CAESAR. User identity (NUI) 123456 is clearly used as an example.

When Otto considered different ways of accessing Datapak, he came up with the idea of writing a so-called "scanner", which would test different combinations of usernames and passwords.

Scanning is a technique originally developed for the public phone network, and works by systematically calling every possible number in some order, e g 111111, 111112, 111113 and so forth until you get an answer. When a computer answers the call, you make a note of the number and move on to the next. Afterwards you can pick systems from this list of accessible computers and see if you can hack them. Of course you don't do scanning by hand. Just like in the movie War Games, you write a program to test all numbers one by one. Scanning in itself is not illegal -- part of the point of having a telephone is that you have the right to place as many calls as you like, to whomever you like.

Otto's scanner was a bit different. It was not supposed to call any numbers, just scan for user identities and passwords that granted access to the Datapak PAD. Usually a X.25-PAD will only allow you three tries to enter username and password before the line is disconnected, but Otto found out that by connecting to the Datapak password-database you could try three passwords at a time without having the line disconnected. Otto's scanner was a computer program that could test three passwords at a time, get thrown out of the database (without being disconnected from the PAD), reconnect to the database, test three more passwords and so forth. To disconnect / reconnect the phone line would take a lot of time and result in a slow scan, but with the scanner using the password database it was lightning-fast!

When Otto wrote his scanner he needed some number to test the program. By pure chance he entered the obviously stupid combination of user identity 123456 and password 654321, and it worked! (Does anybody besides me come to think of the movie "Spaceballs"? -- only an idiot would use that code on his suitcase.)

User identity 123456 was one of Televerkets own lines, a test line which purpose is yet unknown. It is perfectly possible that user 123456 was simply "left over" by mistake by Televerket.

Otto began using identity 123456 for regular calls to the conference system QSD, which functionally resembles the now very popular IRC, Internet Relay Chat. Apart from the conferences there are also mailboxes for the users. Among the most frequent participants were, for example, SCSI, who has hacked into every X.25 network in the entire world (no overstatement), Sentinel from ex-Yugoslavia, the female hacker Venix from Greece, Seven Up, the sysop at SECTEC (Sector Tectonics, another X.25-bulletin board), and Raol from Italy -- the master of VAX-hacking who was recently arrested for computer intrusion at the Bank of Italia.

This chatting kept going until he, on the night of the 7th of November, was called (on the chat system QSD) by another hacker from Sweden.

The "White Knight "

The hacker that called Otto named himself White Night. The duality of the name is a conscious misspelling of the kind that hackers love. The first conversation between Otto Sync and White Night went thus:[(3)]

White Night : Hi! Hej! [Hej is Swedish for Hi]
Otto Sync : Hi! Hej! Sorry I'm not Swedish I'm French. Calling from Flen, a #$&% city 120 km from Stockholm.
WN : I see. What are you doing there?
OS : Working as an automation engineer at a French company. And you?
WN : I'm working at Volvo.
OS : Where? I worked at their factory in Olofström some months ago.
WN : DA-verken in Göteborg. [Gothenburg]

Then they began talking tecnicalities, as all hackers do. Otto asks White Night how he manages to handle Swedish characters and they discuss the pros and cons of different terminal programs. White Night then turns the discussion to how he has managed to call QSD -- "Do you know how much it costs?". Otto suggests that they should swap "outdials" -- access codes to computers on public access networks such as Internet, with connected modems allowing you to dial out for free from that computer by accessing it's modem. He also tells the stranger that he often calls Synchron City, and that a lot of "H/P/A" (Hacking, Phreaking, Anarchy -- perfectly legal textfiles describing hacking techniques) can be found there. Strangely, White Night has never heard of Synchron City, and is immediately curious.

For some weeks Otto calls QSD on a regular basis. So on the night of November 29th, the white knight appears again, but he doesn't recognize Otto, as Otto is using another

alias this time. Otto has already forgotten about White Night and doesn't recognize him either when he is called. However he can see that White Night is also using identity 123456, and gets a bit suspicious, as he has revealed that identity only to a single other hacker, which we will call Phred. A bit hesitatingly, he starts chatting with the stranger:

WN : Hi.
OS : Phred?
WN : No, but I know him!
OS : I guess so... I know you?
WN : Fun, do I know U?
OS : Maybe, I'm usually Otto Sync here...
WN : Hi Otto, hm hm hm.
OS : Hey, could you tell me who you are... cool!
WN : U speak Swedish?
OS : Very badly. But can't you tell me who u are??? As for me, I'm the one who found the NUI you're using.
WN : Why do U think I use the NUI "you" found?
OS : You can ask Phred if you don't believe me.
WN : Why should I ask Phred?
OS : Because he was the first one to whom I gave the NUI. We talk voice sometimes.
WN : What NUI?
OS : The very obvious one with the very obvious password. And the second one that I see on QSD.
WN : Wow, I haven't spoken to Phred 4 a long time!

The misunderstandings between Otto Sync and White Night is of course due to the fact that White Night is not a hacker. As a matter of fact, he is using Televerket's test line, 123456, *from inside* Televerket. When Otto claims that he found it, White Night first gets a bit sulky, but then realizes he has to play the game:

OS : The previous [NUI I used] was 159800. Are you from Sweden by the way?
WN : Sweden what.
OS : Just wondering... If you don't want to chat, then why go on QSD?
WN : Of course I want 2 chat. I'm Swede! R U?
OS : Nope I'm French. But I like Televerket, except when they send me bills :)
WN : Do they? Why?
OS : I asked for a NUI some weeks ago to get the technical doc about the PAD... But I won't pay!

When Otto has made these statements, White Night disconnects the line and picks up the papers with the print-out of the conversation from the printer. These papers, most of which contents are cited above, are then used as part of the evidence in the trial against Otto Sync at the Katrineholm Court of Law.

What Otto didn't know when this conversation took place, was that Televerket was busy tracing him. From November 28th to December 1st, the day before the arrest, Televerket registered all telephone traffic from Ottos office at the French telecom company. In order to do this, they had taken some extraordinary measures.

Flen's telephone station was at that time not equipped with the new electronic switching system AXE (Automatic Cross-connection Equipment). Istead, an old electro-mechanical exchange was in use. (It has now been replaced.) *If* the telephone station had been equipped with AXE, the monitoring would have been a lot easier, since it would simply have been a matter of requesting information from Televerket's information system (IS), which can monitor a number automatically for unlimited time. Present-day Telia (a private corporation which has replaced Televerket after deregulation) even investigated the possibility of having computers examine all calls automatically in order to classify which subscribers that showed "fraudulent patterns" -- but these investigations didn't bear fruit .

When Televerket, under the command of Pege Gustafsson, had traced the "fraudulent" calls to the Datapak number 020-910037, they found that they came from a group number belonging to the company Otto worked for. A group number works by letting a company with an internal exchange connecting some number of telephones, say 500, share a suitably large number of outgoing lines (perhaps 10--20 of them) so that they can minimize the subscription charges. By tracing the group number, nothing was proven, as anyone at the company could have called using the group number. The calls could not be tied to a physical person, which is the kind of evidence required for this type of case.

To make further tracing possible, Telverket installed a reader on the exchange of the company Otto worked for[(4)] . With the reader, every outgoing call from any extension at the company was registered and printed. This list could then be compared by corresponding list for connections to the Datapak PAD at 020-910037. In this manner, Televerket's technicians found that Otto had called for 41 hours and 20 minutes through Datapak during the week the tracing was carried out, and during that time transmitted information packets for about 4000 Swedish crowns' worth [roughly $570]. (You can call this the total "postage fee" for the information packets.) The low cost thus depended upon the fact that you only pay for the data actually transmitted, not for online time, as in the case of common telephone calls.

All of this tracing was supervised by Pege Gustafsson.

A Night at the Hotel

Otto himself tells us what happened on the morning of December 2:

"They came to arrest me at work. Imagine the embarrassement. First I see these guys coming in my room and think 'oh shit, some more customers who want a demo on some product', but then they showed me their police ID and my heart stopped. They searched my office, took all notes and computer stuff. Then they took me out and had me open my apartment, and did a search there as well."

He was then brought to Katrineholm police station (the police authority closest to Flen) for interrogation. On his way there all sorts of thoughts ran through his head: "What to tell? I thought it was a BBS? I thought it was a free line? Reverse-charging?"

The interrogation begins without the representatives of Televerket as well as Otto's

counsel present, but as Otto doesn't understand all the Swedish words (though he knew some, as the company sent him to evening Swedish language classes), the interrogation is postponed until a French interpreter arrives.

When the interpreter arrives, Otto asks for a counsel but agrees to continue the interrogation without the defense present. Neither does he find it necessary to talk to the French embassy. He tells the interrogators that he is in non-combat military service duty at the company in Flen, and that he has considered working for them even after the service is finished. The police and Otto simply get to know each other.

At 14.25 Otto experiences the luckiest moment of his life so far. That is when his counsel arrives, and who by a remarkable coincidence happens to be an extremely professional lawyer with his own firm, who thought the hacker case looked interesting at first glance, and thus took upon himself to defend Otto. This lawyer primarily deals in industrial corporate disputes. Otto tells us about his lawyer that "he was a real pro (I know, as this was the third time I went to court), a very nice man, well educated, and interested in French wines".

The remainder of the interrogation session mostly consists of technical discussions between Pege and Otto Sync. The other people present soon have trouble understanding what is being said. Otto claims that he has been searching for a "reverse charge" number (the X.25 counterpart to a 800-number which are actually quite common) and that he thought NUI 123456 that he got from Televerket's manual to be a "test line" of some kind. He says he is very curious and that is his reason for exploring Televerket's systems. Pege Gustafsson produces his printouts from the chat sessions where he acts as White Night, and confronts Otto with parts of these printouts (the same that are partly reproduced above). Otto, who for the first time gets to know who White Night actually is, reminds the others that anyone can have used his alias on QSD. Pege asks if he has passed around the NUI 123456 to others. "No", he answers.

Today Otto tells us that "Pege tried to have me say that I knew what I was doing and that I hacked the NUI etc. All the way I denied it and said I thought it was public line to be used in reverse-charging mode, and kept that line all the way. Of course Pege could see it was bullshit, he knew pretty well what I was up to. And he was right."

When the interrogation ended at 6 p.m. he was brought to a cell, as it was too late to go to court that day. Otto was instantly impressed by the Swedish custody standard: "In France it's dirty, you get to sleep with drunkards, no food, rough treatment etc. In Katrineholm it was like being at a hotel, I had my own little bed in a neat room. In the morning I was given a breakfast as good as the ones you get on planes -- fantastic! Slept really well there."

The next day he was brought to Katrineholm court, which decided not to keep him in custody. Instead he was given a travel ban, which meant he had to leave his passport and had to report to the Flen police office before noon every day until the start of the trial.

"Dangerous International Terrorist"

What initiated the chain of events that culminated in Televerket finding Otto Sync was the scanning of the Datapak PAD. When Pege found out that someone was scanning the Datapak PAD for user identities, he must have been shocked. This was exactly the thing that had happened two years earlier, and that time they had suspected that this was an act of international terrorism. In reality it proved to be the brothers Pad and Gandalf from 8LGM, two perfectly normal, curious hackers without any connection to international terrorists whatsoever.

As all other computer security officials in Sweden, Pege Gustafsson had read the book *The Cuckoo's Egg* by Clifford Stoll. In the book Stoll describes how he, using imagination and endless nights of unpaid work, managed to trace a hacker that had entered his system at Berkeley and started searching for military secrets throughout the American part of Internet. The hacker doing this was on mission from the KGB, receiving instructions through the circle around hackers like Pengo and Hagbard in West Berlin -- a bunch of freaked-out, coke-snorting, fuzzy leftist hackers who probably never caused any serious harm. Those last facts are never mentioned in the book, but it is closer to the truth than the image of international computer spies that Stoll conjures up.

So as Otto started scanning the Swedish Datapak network, Pege hit the sirens. The incident was probably associated with other, similar incidents, and was therefore interpreted not as the sum total of some small hacking adventures using simple scanners, but as a systematic pattern of intrusion attempts by some foreign power. Simply pure paranoia.

After closing a ring round Otto in Flen and after conducting a series of tracings, there was also "confirmation" of the suspicions: Otto made several calls to Thailand -- which were interpreted as communications with his mission providers, which could be anyone ranging from the KGB to the IRA. Actually, these calls were made to a long-time friend, and he had the company's permission in calling Thailand every now and then. Every hacker gets to know lots of people around the planet, as the "global village" is their home district.

So what the police and Televerket expected to find, as they turned up at Otto's office on the 2nd of December 1992, was a dangerous international terrorist. They found a 25-year-old socially maladjusted, and bored engineer, who had been amusing himself by exploring the Swedish Datapak network for the lack of anything better to do. Otto describes the situation as \"Pege thought he was the good guy trying to catch the bad guy. He told me himself that he was a fan of Clifford Stoll and that he met him at some security conference some years ago." During the interrogation with Otto, Pege drew maps showing which countries Otto's X.25-connections had accessed -- maps that according to Otto himself looked like "maps from your average international terrorist handbook".

Even though this was clearly stated in the following investigation -- which didn't even mention the suspicion of espionage -- these suspicions about Otto stuck to him long after he left Sweden. When the computer programs that were to control starting lists, time measures and result lists during the Olympic Games in Lillehammer 1994 were stolen from a military storage in the autumn of 1993, the Norweigan police (for some reason) believed that Otto was involved. Expressen (a major Swedish evening paper)

called him "the hacker leader", and took the opportunity to draw suspicions to Otto as well as to the company he had worked for in Flen. In between the lines, they hinted that this was a way in which the French military sent spies to Sweden[5] . Personally, he tells us that "I was in Thailand, and at that time didn't have job nor a computer." Thailand is quite far away from Lillehammer.

He is also backed up by SÄPO (Swedish counter-espionage) who through director Jörgen Almblad said that the French volunteer workers in Sweden in general, and Otto Sync in particular, did not pose a security risk. "If they are Frenchmen or Russians doesn't matter, as far as being security risks" he told Expressen. SÄPO are ultimately responsible for the national security and should be well-informed. If they publicly deny any suspicions, you can be certain that they are telling the truth. If they had even the slightest suspicions, they would rather not comment. So much for that terrorist.

Even Pege himself realized that Otto was not what he first thought him to be. In private he told Otto, that if he had known what a small-timer he actually was, he wouldn't have carried the case this far. He even "said he'd like to have a beer with me when all this was over." Today, Otto is doubtful about Pege's competence as a security officer: "I remember he told me he was involved in concerts security as well (rock concerts). Although he was the security officer there, he didn't know too much about Unix security or hacking techniques. In fact he seemed to be ignorant of some basic things about Datapak such as reverse-charging".

Good versus Evil

It appears as though Pege was carried away by the idea of defending Sweden from imaginary terrorists. Just as American counter-espionage was completely disinterested in the practically harmless hacker hunted by Clifford Stoll, SÄPO was as disinterested in the equally harmless hacker hunted by Pege. Otto wasn't even looking for military secrets -- he was considered a threat just because he was so curious.

So, on the 18th of December the, "white knight" from Televerket drags the French dragon to a Swedish court with the help of district prosecutor Christer Pettersson. The trial itself is a farce -- soon it turns out that of all the people present, only Pege and Otto have the technical knowledge required to understand the summons from Televerket. Then the first thing Otto's counsel does as the trial begins, is to throw Pege out of the court room, as no reasons have been given for his presence. The only time that Pege is allowed in the room, is when he is cross-examined by the court. Suddenly Otto himself is the only one that understands what the prosecution is actually about. None of the members of the court have any kind of practical technical knowledge.

"The trial was real fun because no one really knew the subject. Some of the documents I produced during the trial were a bit dodgy, like this e-mail from some guy telling me how to use reverse-charge on Televerket. I also produced a valid list of all Swedish BBS:es, telling the judge that they were 'free access computer systems'. Of course no one had a clue about the difference between a BBS running on a 386SX in a 17-year-old teenager's room and a nationwide X.25 data network."

Otto doesn't think he is guilty of any crime, and is wise enough to use simple descriptions which the court can understand. He doesn't deny using Datapak exactly as much as Televerket claims, and is prepared to pay for it. But he think it's unreasonable that he shall pay the costs of tracing and investigation by Televerket.

Pege is called in only to describe how the tracing of Otto was performed. In all other questions they must refer to the preliminary investigation protocol, a horrible pile of papers containing almost exclusively technical desciptions and different lists of tracings carried out by Pege. Among the "evidence" is Ottos own notes, some of them completely harmless, with detailed technical information about phone numbers etc. to different computer systems all over the world. Without further explanation of what kind of information this is, these cryptic notes are called "hacker notes". There are also a bunch of print-outs of files found on Ottos hard disk.

This material has apparently only been included in the protcol in order to make Otto look "obscure". The print-outs could just as well have been xerox copies of "unsuitable books" from his bookshelf. The only purpose of including this material must have been to throw suspicions on Otto for belonging to a certain subculture.

At some point the court must have grown bored with the fact that Televerket had not been able to present an understandable prosecution. Regardless of whom had lied or told the truth, Ottos claim that he had believed that the calls were for free seemed probable to the court. As the prosecutor could not prove the opposite, the court found for the defendant. Televerket's claim for damages, and the claim that Otto should be forced to leave the country, was also dismissed. Televerket had to pay their own costs for the trial. In short, Televerket lost, and Otto Sync won. This decision was made December 18th 1992, but wasn't made public until January 8th.

Lookin back he says that "although I was guilty like hell and went to court, Televerket lost the case."

All's well that..

Televerket, now named Telia, appealed the sentence in the court of appeals on January 15. As Otto would only be present in Sweden until April 1st, they asked the court of appeals to review the case before then, which was of course a hopeless request.

In September, Otto was back in France, still hacking. Then, one night "White Night" turns up at QSD again. "I started chatting with Pege, who was expecting me show up at appeals court in October", Otto says. The court of appeals probably couldn't have him extradited to Sweden, and in any case he had already booked a ticket to Bangkok for October 4.

The court of appeals considered the case at a hearing October 25th. As Televerket hadn't added something new to their application of summons, and as Otto wasn't available, the court of appeals decided to dismiss the case. Televerket and Pege lost again.

Note: Otto Sync recently left his job as an engineer at a huge, multi-national

enterprise in Bangkok. He is currently busy setting up his own Internet-service company. Pege Gustafsson still handles security issues at Telia.

---

1. All quotes are lifted from e-mail communication with Otto Sync.

2. **Ledell, Göran** (ed) *Dataolyckor -- Har det verkligen hänt någon gång?* INFOSEC, Lund 1992

3. Quotes from the conversation are drawn from the court documents.

4. To be technically precise: a DNR -- Dialled Number Recorder.

5. *Expressen* , Friday February 4th 1994, page 11.