The Hackers of New York City

By
Stig-Lennart Sørensen

Thesis submitted as part of Cand. Polit degree at the Department of Social Anthropology,
Faculty of Social Science, University of Tromsø.
May 2003

Contents

LIST OF ILLUSTRATIONS **3**
PREFACE **4**
INTRODUCTION **5**
MY INTENTIONS WITH THIS PAPER **8**
PROBLEM POSITIONING **8**
ENTERING THE FIELD **10**
ON THE FIELDWORK 10
ON INFORMANTS 12
FIELDWORK AND FILM ISSUES **13**
PRACTICAL CONCERNS: 13
ETHICAL CONCERNS: THIN AND THICK CONTEXTUALIZATION 14
ON NEW YORK CITY AND THE INTERNET **17**
NEW YORK CITY 17
INTERNET 19
PREVIOUS RESEARCH ON HACKER CULTURE **22**
COMPUTER SECURITY, CRIMINOLOGISTS AND JOURNALISTS: 22
SOCIAL SCIENCES: 23
THE MANIFESTATION OF HACKER CULTURE **28**
HACKING HISTORY 28
AN ETHNOGRAPHIC ACCOUNT OF HACKERS 40
ARENAS OF SOCIAL INTERACTION 41
DISTINCTION OF UNDERGROUND COMPUTER CULTURES 47
PRACTICE 50
ON THE PRESENCE OF POLITICS 52
DISCUSSION **57**
CULTURAL CAPITAL AND SUBCULTURAL CAPITAL 57
CONCLUSION **68**
LITERATURE LIST **73**
APPENDIX I: FIELDWORK CAMERA EQUIPMENT LIST **77**

List of Illustrations

Unless otherwise noted, illustrations or photos are by Stig-Lennart Sørensen.

Figure 1	[7]	The AT&T Long Lines Building, 33 Thomas Street.
Figure 2	[17]	Empire State Building, 350 5'Th Avenue.
Figure 3	[20]	Computing in 1971: the IBM 370 model 135. Courtesy IBM Germany GmbH.
Figure 4	[27]	CNBC headlines. Screen capture.
Figure 5	[29]	Ad : "Telimco Wireless Telegraph Outfit". Courtesy Scientific American, November 25, 1905.
Figure 6	[34]	The MITS 8800a. Unknown ownership.
Figure 7	[36]	The hero and his to-be girlfriend in "War Games", 1983.Courtesy Metro Goldwyn Mayer.
Figure 8	[39]	British Labour homepage defacing. Screen capture, unknown author.
Figure 9	[42]	Front page of "2600: The Hackers Quarterly", spring issue 2001. Courtesy 2600: The Hackers Quarterly.
Figure 10	[43]	Index of spring issue of "2600: The Hackers Quarterly". Courtesy 2600: The Hackers Quarterly.
Figure 11	[47]	The homepage of http://www.astalavista.com. Unknown ownership.
Figure 12	[51]	NetBus 1.60 Unknown ownership.
Figure 13	[54]	Protesting the MPAA.
Figure 14	[55]	H2K conference speeches and panels (excerpts). Courtersy H2K.
Figure 15	[64]	The hero "Neo". "Matrix", 1999. Courtesy Warner Bros.
Figure 16	[68]	Bentham's Panopticon. Courtesy Bozovic / Bentham and Verso.

Preface

Wow, I am there! Thanks first of all go to my Irene, who'd been such a lovely support and ass-kicker the last six months. Also to my parents, who've supported this venture all along, not really sure what I was writing about. And to all my friends, who despite my whining has been supportive and given me a lot of things to think about, and write about. Especially Erling, Nils, Per Harald, Myhre, and the rest of the bunch at the IfI cantina. Thanks to my supervisors Bror Olsen and Bjørn Bjerkli whom, without their advice and teaching, this work wouldn't be realized. Great thanks to Rosella Ragazzi, Lisbeth Holtedal, Marit Gjertsen, Brit Kramvig, Gøril Skotnes, Frode Lien and everyobody else at Visual Cultural Studies for being so cool people and great teachers during my time here. To all my fellow students, and especially the VA class of 99, thanks to you! Thanks to all my informants in New York City, Boston, Washington D.C and elsewhere "over there", especially Emmanuel, Izaac, Spudz, Shana, Kashpureff, Alan Kotok, Mike, Andy Miller, Cheshire Catalyst, Jon Johansen, Robin D. Gross. To the folks at #md2600, thanks for your participation and feedback! And thanks to all my Norwegian informants, you know who you are! Thanks to the "spooks" at Telenor FoU, Avd. Sikkerhet, who sponsored my trip to H2K in 2000. And thanks to all I meet after my film screenings with your valuable discourse.

You readers can email me at stigls@stud.sv.uit.no and let me know what you thought.

Going home to sleep, bye! EOF

Tromsø, 27/MAY/03

Introduction

The heat was almost unbearable and the air was very humid. As night fell on Manhattan, I was making my way to the Citicorp building. My cab crawled through the crowded traffic and its driver, a mild-mannered turban-clad Indian, told me that many New Yorkers fled the city at weekends escaping these almost tropical conditions. Outside the yellow cab, endless streams of people moved down on each side of the Lexington Avenue, ever moving and engaged.

Atop the Chrysler building the stone gargoyles stared down at the crowds rushing to or forth the subway station below the Citicorp building. The Citicorp building stands 279 meters high, a colossal structure with sleek glass and steel surfaces standing on four massive columns. The previous landowners, the church congregation of the St. Peter's Lutheran Church, sold their land on two necessary conditions; that a new church would be built in the same place and that the new Citicorp building would also accommodate the construction of a public plaza to continue the church's tradition of hospitality.

It is within this building, located at a sub-level within the Citicorp Building itself, that the "2600" of New York City, something as rare as a *public* hacker organisation, have their monthly meeting. With my arrival three days earlier I was now ready to commit to fieldwork and filming, and though jetlagged beyond belief there was still some sort of manic optimism mysteriously prevalent. Making my way out of the cab, I reaffirmed my grip on the camera bag and the cumbersome tripod hanging over my shoulder, and nervously approached the entrance to the public plaza, glancing about to spot any hackers. New Yorkers rushed about, most of them heading for the subway station, fast-talking to their company or cell-phones. The constant drone of the traffic, construction machines and the ambience of 12 million people permeated the atmosphere of the City. The heat and humidity were almost unbearable.

A young man in his thirties stands outside, dressed casually (but then again so does the stock traders down by Wall Street these days) and smokes a cigarette. He holds a document briefcase under his left arm, and as he stumps out his cigarette I approach him and ask him «is this the place where the 2600 have their meetings?" My Scandinavian accent makes me suddenly aware of that I am an anthropological student from Norway. He watches me for a second, then says, «yeah, this is the place. Come on, let's go in and meet the people». With a friendly wave, he beckons me inside and we enter the Citicorp building.

Hackers hold a special place in Western culture. Today they are viewed as dangerous subversives, likened to terrorists without an ideology, surfing the Internet with malice on their mind. But hackers have not always been viewed in a negative light. In the early seventies hacker was an honorary term among computer programmers. In the eighties, when the home computer became a household item, hackers were seen as pioneering technologists brandishing an anarchistic attitude (Levy, 1984). But during the nineties something changed, and they were viewed as criminals. The popular notion of hackers today is that of a teenage boy sitting alone in the middle of the night, hacking his way into corporate or governmental mainframes and wreaking havoc amidst the stored data (Chandler, 1996). Or someone who steals your credit card code and use it to steal your money. Or the ones who deface websites with obscenities that seem to have no motivation but destructive ones (Peneberg, 1999).

Contrary to these pathological depictions are the one of someone programming for hours, if not days, on end to finish a computer game (Levy, 1984). Or someone who hooks up phones around the world and speaks to himself, around the world (Rosenbaum, 1971). Or someone, in the absence of a wireless network, runs a 300 feet network cable from a high-rise building, set up a hub and let his friends surf the Internet on their laptops down by the beach (field notes, 2000). Hackers claim a hack is all about elegance, originality and geniality.

In my thesis I wish to describe how hacker culture is not random acts of greed or sabotage, but that the global hacker community encompasses a cultural content made up of a diverse configuration of political and computing history, pop culture and technical terminology, and that which ascribes to a set of ethical guidelines that puts a premium on the challenge and exploration of technology. Central to the hacker culture are the motivation for the hack, which determines the relationship to other underground computer user categories. Equally important is the dissemination and possession of hacker secret knowledge that is central in the hacker identity formation process.

Through their display of assumed information anarchy, the hacker culture could be challenging the institutionalized information access hierarchy of states, corporations and similar entities of power, inducing retaliation and prosecution that hackers perceive to be wrongful and exaggerated. For us, hackers may be forerunners of our own future relationship to technology, mirrored in their pioneering adoption and symbiotic intimacy of new technology,

After downing a couple of falafels in an East Village deli, we got into a couple of cabs and headed down to the mystery building located close by the Federal Plaza just off Broadway. This building was supposed to house the AT&T telephone switching central for the entire American east coast as well as carrying international calls. Theories abound as we got out of cabs as to which espionage governmental agencies where involved. The National Security Agency involvement where taken for granted.

Then, rounding a corner, we came upon the striking monolithic silhouette of AT&T's Long Lines building. The building, or skyscraper, filled an entire city block and was only lit at the street level. The rest of the building was visible as a gigantic structure reaching toward the Gotham night sky, it's details barely outlined by the streetlights below. It was at least 150 meters high, and its windowless surface yielded none of its secrets inside.

Later, over some hot cups of coffee, we discussed how we should proceed with the investigation of the building. Clearly the building had to house more than just switching stations!
(Field notes, February 2000)

Figure 1 The AT&T Long Lines Building, 33 Thomas Street

My Intentions With This Paper

After the introduction I will give an overview of my fieldwork experience, as well as discussing the strategies employed by me when I was faced with ethical and practical dilemmas in the field. This will be followed by a historic and contextual description and summary of each of the fields that I attended when conducting my fieldworks. I will then give an overview of some previous and relevant research on hacker culture before I start my analysis and description of hacker culture beginning with the historical origin and definition of the hackers. Hacker history is an important element involved in the formation of hacker culture and the construction of its boundaries. Later I will discuss how the hacker culture through the dissemination of hacker knowledge contributes to the process of hacker identity formation and boundary formation. I will then consider the relationship between practise and ideology as being the main strategy by which hackers separate themselves from non-hackers or computer subcultures, followed by a description of hacker practices. I will then discuss if there are a presence of politics within the hacker politics, which will lead into the discussion where I will attempt to relate the theories of Sarah Thornton – and in extension, Pierre Bourdieu - to the social dynamics and identity formation of hackers.

Problem Positioning

In this thesis I wish to describe the manifestations of the hacker culture as it were when I conducted my fieldwork in 1999-2000. I will focus my discussion on what I consider to be the apparent circumstances that I derive from my empirical material: the hacker subcultural capital, the hacker media relations and the relationship between gender and hacker subcultural membership. The hack forms a central pillar of hacker culture as this is the act of hacking as well as acknowledging the status of the hacker, but the definition of what a hack does may differ among the various underground computer user categories that use hacker practices. In order to clarify and constrain the definition and usage of the hack and by extension the boundaries of hacker group formation, I wish to discuss the hack in two separate perspectives: one, which see hack as a practice and the other as an ideology. If someone uses hacking methods, it doesn't necessarily mean he or she is a hacker. I see the motivation for the hack as the key to defining the user of hacker techniques as a hacker or as cracker, pirate, or any other category that name themselves hacker. A group of computer users that use hacking methods and who calls themselves hackers will not be accepted as hackers by the hackers that

claim hacking must be constrained by motivational ethics. Hacking motivation thus forms an integral and an important element of hacker identity.

One way to understand the hackers is as a subculture. The term subculture has been used for the last fifty years to describe a small group of individuals that adhere to similar behaviour, values and lifestyles that distinguishes themselves from other social groups (Thornton, 1997:1). The dissemination of hacker knowledge, of hacks, to other hackers, is important in the social dynamics and identity formation of hackers, perhaps even more important than the technical ability. Through his knowledge a hacker validates his status as well as acknowledging the hacker status of others.

The hacker subculture is elitist, meritocratic[1] and anarchistic in nature, and adheres to a power hierarchy of knowledge that effectively excludes outsiders (Taylor, 1999). Hacker knowledge is acquired through mentor-based confidential relationships, that puts a premium on non-curriculum knowledge, and through underground channels of dissemination whose content and ideology could spring back to the late sixties and early seventies counterculture (Clough & Mungo, 1992)(Segaller, 1999). The dominant culture defines the hacker culture as a "social menace" due to its potential threat both to normative education as well as property law (Ross, 1990). The hacker ideals of unlimited access to information threaten the cultural fields of power, such as institutions that adhere to an information hierarchy based on control and constraint (Boyle, 1997). The Internet appears to dispel state authority due to its uncontrollable infrastructure; it being an anarchistic network structure based on communications protocols that adhere to no central authoritative administrative entity (Guisnel, 1997).

Due to nature and limitations of my fieldwork my empirical material will mostly be derived from the USA east coast unless otherwise noted.

[1] "*A system in which the talented are chosen and moved ahead on the basis of their achievement"* or "*leadership selected on the basis of intellectual criteria",* Merriam-Webster Dictionary Online

Entering The Field

We entered the Citicorp building, passing chain stores with few customers inside this late business hour on a Friday afternoon, and as I stepped on the escalator bringing me down to the interior public place at the sub-level, I saw for the first time the participants of the 2600 meeting of New York City. Spread across six or seven round tables, about sixty people had gathered, mostly young men, but also a few older men. There were a few girls there, but no women. Most of the young men were moving about between the tables on which computer, telephone or other technological fragments of unknown origin were placed, together with magazines and manuals catering to all manners of technological issues and devices. Their language was English, yet I had difficulty tracking the meaning of their speech as it filled with technical terms beyond my understanding, and I felt as a complete outsider. Me, the computer wiz at the institute!

My guide, who had so generously brought me here, turned and asked what I did. "Oh, I am student researcher. I am here making a film about hackers," I answered. "Oh really. You are media", he said all of sudden icily. He gave me an equal cold glare before he turned, and joined a group at one of the other tables. Abandoned among the natives, I sat down at the table, going through the reasons for his quick departure in my head.

"So now what?" I thought, contemplating the academic hara-kiri that awaited me back home at the university upon return, data-less. The media-hating hacker had abandoned me alone in a sea of hackers, and none of them seemed to notice me. Disillusioned I contemplated doing some wide shots of the atrium and then head home to watch Star Trek Voyager on EPN[2]. But my self-pity didn't last long. "Hi there!" I heard, and a friendly face smiled at me and extended a hand to greet me. His name was Izaac and he became my gate opener.

On the Fieldwork

My chosen field was hackers, and the places I choose to conduct my fieldwork in were New York City, USA, and the Internet. The City became the economic, social and political framework of my field; a hub where important events, people and history central to the field of hackers appeared. Geographically the field even extended south and north to the nations capital where many of my Internet informants lived and up north to Boston where I visited the

[2] United Paramount Network – US TV network.

Massachusetts Institute of Technology where the hack was born. The City itself was a bottomless source of data: bewildering in all its manifestations and diversity.

I moved to New York City in the fall of 1999 and stayed there, with a brief interlude in Norway during Christmas, until spring 2000 and returned for two weeks in July 2000 for the H2K (Hope 2000) hacker conference arranged by the "2600 Magazine". During these months I lived in Manhattan, the last two weeks sleeping on a sofa at the abandoned, "2600 Magazine" office spaces. In New York City, as mentioned earlier, I attended the "2600" meetings, which is a loosely organized monthly occurrence attended by hackers and others interested in technology, that took place in the Citicorp building, and also observed the "Off The Hook" radio programs, sometimes joining the participants for dinner afterwards. On several occasions I "hung out" with people I meet on these occasions, which usually meant going to a bar, a club or visiting mysterious places. This proved to be the more gratifying experiences in terms of data collection, as people were more at ease and spoke more freely when it was just me and a few others present.

During my first visit it became quickly apparent that library computers and Internet cafes were an inefficient and expensive approach to Internet fieldwork. Meant to be more a minor addition to the "real" fieldwork in the physical world, it proved to be the other way around. Therefore during my second stay in spring 2000 I brought along my stationary PC, and through a 56K modem connection I maintained a rapport with my informants as well as gathering fieldwork data through Web pages and prowling through massive amounts of hacker knowledge in the form of articles, explanatory text files and computer software. The way I collected data from Internet informants, was by logging IRC (Internet Relay Chat - a form of Internet real time text based conversation) channel conversation[3] focusing on the #md2600 chat channel on the "2600" magazine IRC server. The participants on this channel I had met while visiting Washington D.C., where I participated in a small demonstration against the MPAA trial against "2600 Magazine" in the springtime of 2000. Afterwards I regularly logged on and participated as well as logging the conversations. This logging continued after I returned to Norway and even until I finished edited my exam film, "New York City Hackers" (2000)[4], in December 2000. These conversations were more of a casual nature than the interviews, and I will use the material from the log files less than the interviews in my thesis.

[3] A highly effective way of data collection but it can also prove to be overwhelming for the fieldworker in terms of the sheer amount of data collected; a six-hour chat with moderate participation can easily produce more than fifty pages.
[4] Website adress: http://www.atomsmurf.pasta.cs.uit.no

In addition the videotaped and transcribed interviews superseded the IRC logged material both in terms of analytical value, content and coherence.

On Informants

I met my informants both on the Internet and at the 2600 meetings. My informants ranged from professors at the Massachusetts Institute of Technology which according to hacker lore had partaken in the first hacks in the early sixties, to old time phone phreakers (a telephone systems network hacker; see history of the hack chapter) who had their glory days in the sixties and seventies, to adolescent hackers who had grown up with Internet. A majority of the interviews took place during March and April 2000 and at the Hope2000 conference of July 2000 in New York City.

During my work with the thesis and after public screenings of my exam film, I've also had the opportunity to talk and discuss hacker culture with people interested in my work. Most of these have been Norwegian computer professionals who have told me of their own experiences of hacking and hackers. The discourse has taken place verbally as well as by e-mail. I find the correspondence of such an interest that I have included some of it in my study.

Fieldwork and Film Issues

In this chapter I will discuss some of my experiences at the fieldwork in relation to practical, methodological and ethical concerns. How will governmental authorities or property managers react to me filming their buildings? What about ethics in relation to filming informants? Will the camera[5] impose itself on the informants, making them act or talk in a manner that aren't consistent with "reality"?

Practical Concerns:

For my governmental approval I sent an application for a research visa to the US embassy (only two weeks ahead of my scheduled flight), emphasizing my independent research and financial status. Since I was conducting research on a topic that governmental intelligence organizations probably considered a considerable security issue, I repeatedly underscored that I wished to get the voiced opinion from both sides. At that time I was considering many options for my exam film, one of which was pursuing a conventional documentary style that would include interviews with hackers as well as security personnel. In less than two weeks I received my research visa. In New York, when the Twin Towers where still standing, terrorist anxiety was understandably high (Oklahoma City bombing was only four years away, and the Columbine shootings were still reverberating in the evening news) and corporate interests were at stake as I experienced carrying out my shooting schedule. Repeatedly during my fieldwork, as I sat up my camera on a tripod to shoot a wide shot of an imposing skyscraper on the pavement, security quickly appeared and gently ordered me to stop filming. On one occasion after been given a stern warning, the security man then switched into a praise of the buildings beauty and said I should apply to the property manager to be granted filming access to the top floor. Once when I had set up the camera at the Federal Plaza, meaning to take some shots of the headquarters of the Federal administration in Manhattan (where the FBI have their offices), a *very* stern-looking – and armed - FBI agent came running and told I me I would be committing a federal crime if I continued filming, something I was not to eager to experience. Being a student filmmaker meant (not surprisingly) that nobody took you as serious as commercial or professional crews. As I was

[5] I used a Hi8 Sony Camcorder TR3100E, which is an analogue camera fully capable of acceptable image quality. Small and lightweight, it did not carry a heavy fieldwork signature and even with added external microphone it could be kept under a jacket. In addition I bought a video tripod during my fieldwork, which I used for my wide shots, interviews and TV recording.

eager to get interviews with the both sides, I tried to contact the FBI. After many weeks of calling and being rerouted throughout the building, I was suddenly talking to the press agent. He sounded very surprised that I actually had got through, and promised to call me back. He never did. A sympathetic clerk at the District Attorneys office later told me that FBI rarely agrees to being filmed unless they are portrayed as good guys and the film have a huge distribution range. In a sense understandable yet I found it frustrating. The National Security Agency proved even a tougher nut. The telephone directory (411) was unable to verify its existence.

Ethical Concerns: Thin and Thick Contextualization

The film is a powerful device of knowledge dissemination. But ethical questions in regards to the informant relationship tend to be of a more acute nature during filming and also when the film reaches public distribution. Jean Rouch's "Chronique d'un été" ("Chronicle of a Summer", 1961[6]), through its cinema verite style, offered a glimpse of the painful revelatory reaction of the characters themselves when subjected to a preview screening (Musser, 1997). But there are not many contemporary filmmakers that allow for this kind of discourse. Now and then I watch documentaries in the filmmaker, in my opinion, appears not to consider that some participants, who might not have a previous experience to filming, may act upon the camera without reflecting upon the directing or editing process that may change the meaning of that person's particular behaviour (Heider, 1976). Clifford Geertz contrast the observed with the meaning of the observed coining the two terms "thick" and "thin" description. Human action, Geertz claim, is observable on a concrete, physical level, but its meaning and motivation must be derived from analysing the greater context in which the action takes place (Geertz, 1973). I see a similar analytical use of Geertz terms, in analogical sense, on the aforementioned documentaries. A decontextualization of speech or behaviour due to editorial concerns, may water down the "thick" verbose verbal experience down to a "thin" sound bite. This is, as I see it, especially a problem in short-time commercial productions, where the "thin" meanings sustain the narrative and conclusive needs of the director or producer[7]. Not that my informants was unaware of this aspect of media exploitation. Indeed, one of my informants told me after a videotaped interview that "three sentences spoken un-interrupted"

[6] Jean Rouch and Egdar Morin shot the film in Paris in the summer of 1960, and is one of the first documentary films using portable cameras (Nowell-Smith, 1997).
[7] Heider (1976:7): "[…] in the use of editing to further distort and subjectively and aesthetically express the view of the maker."

would be shortest edit he would allow me to put in the film of himself. Such is my belief that the filmmaker has an ethic responsibility not to emphasize a nominal behaviour in order not to ridicule or humiliate the participant of the movie. Taking care not to reveal identities, of people of underground communities, is also of importance in the informant-anthropologist relationship during the process of making a film. Timothy Asch remarks that previously subjects of anthropological films had little or no influence on the filmmaking process, but things have changed now and exposure of people or situations may present real danger for those participating (1992). During one of the 2600 meetings the appearance of a Japanese TV-crew during prompted a flurry of questions and worried glances among the hackers towards the camera. Many of the hackers attending the 2600 meetings held normal jobs and were fearful of being sacked if their employer found out they were engaged in "illegal" activities. On one occasion when I was filming the 2600 meeting, a middle-age man came over to me and pleaded not to point the camera in his direction. "I have a job", he said, "and the boss don't know I attend these meetings". I agreed of course. But later, when I made a pan shot of the crowd, he cried out as he came into the frame: "Didn't I tell you to not film me?" I apologized profusely, as I by accident had captured him on film. He seemed so anxious that I showed him how I rewound the tape and erased the pan shot.

As I stepped on the escalator bringing me down into the 2600 meeting for the first time, I felt uncomfortable on how to shoot without compromising the identity of my informants in addition to the self-imposed feeling of the intruding myself upon strangers. After some time I settled on a strategy that seemed to solve both problems. Every time after I had unpacked my camera gear, and was ready to start shooting at the 2600 meetings, I went around to each table and asked if I could film them. I told them what I was going to use the material for and that I wished to give a positive portrayal of hackers. Although this was somewhat time consuming, I felt more at ease and almost everybody agreed to be filmed. Some even came to me after I had finished filming and inquired further about my project, to which I gave answers to my ability. Many times I gave them my e-mail and phone number in case they wanted to contact me. Some of the attendees of the 2600 meetings questioned my effort to ask permission, saying that people attending should expect being filmed; not only was the Citicorp Plaza public, but hackers also attracted heavy media attention.

During my filming, I started out with wide shots taken from afar, before I moved closer to the groups, taking close ups of people and their actions. This "zooming-in" approach to my subjects happened because of a practical and ethical dilemma. As I have mentioned earlier, being a student filmmaker means that huge corporations or governmental agencies,

very rarely responds to your inquiries to shoot at their locations. Usually it ends up with security chasing you away. This was the same problem with the Citicorp building. Headquarters of a gigantic international banking company, their property manager never answered my calls or voice messages. During that time I settled with longs shots of the building, and maybe some wide shots of the meetings. I didn't want to be banned from the building. But after having seen several commercial TV crews go about their filming among the participants of the 2600 meetings, I decided to don't bother with the bureaucracy and took up filming myself. My perceived ethical dilemma was a process of camera and anthropological naturalization both for the informants and me. In the end it was the informants who kept saying, "go on filming, don't worry too much, do your job!" This remark reminds of a documentary I watched some time ago about David Harvey who is a skilful National Geographic photographer (Piotrowska, 2001). In a segment, one of his students at a photo workshop inquired about how to conduct your work without the subjects indirectly being aware of your documenting them. Harvey pondered this for a few seconds, and then said, "you shouldn't think about doing it, otherwise they would be aware of it". In a sense that also illustrates a common situation of the fieldworker. The meaning of the informant behaviour changes when the anthropologist reflects upon his role as a researcher. This cognitive process is mirrored in the unconscious posture of the anthropologist as he aims his camera at the informants, making them suddenly aware of the eye of the researcher and consequently their own representation as seen through it. So in the end, if I interpret David Harvey correctly, the informants begets behaviour that mimics what they think gives a correct presentation of them selves. As Michael Rabiger writes "we judge character and motivation less by what people say than by what they do, and how they do it. Film is inherently behavioural so actions speaks louder than words" (1998: 189).

On New York City and the Internet

New York City

The Air France Jumbo jet landed heavily at John F. Kennedy airport late that evening, fully loaded with passengers and cargo, taking me to USA for the first time. An hour later, as I looked out of the cab window driving down Lexington Avenue, what struck me first was the smell. It smelled the same as in Cairo. Coupled with the voluptuous heat and darkness of a late New York summer night, I experienced the city as a something akin to an Oriental metropolis of splendour and chaos. Somewhat contextually confused I understood that my Eurocentric expectations of America were much different than the real thing. Everything was different; somehow it had been filtered out from the media experience that we Europeans assume to be American. One day Spanish was the only spoken tongue that I encountered. And I recall the anti Ku Klux Klan demonstration October 23'r, 1999. 16 de hooded Klan members. But more than 3,000 counter-demonstrators appeared, their shouts of anger reverberating across Foley Square that cold day. The sheer diversity and freedom of the cultures of this "Capital of the World" culture shocked me into revaluating my perspective on what constitutes Americanism. And which made me appreciate it to that degree that I now call the city my second home.

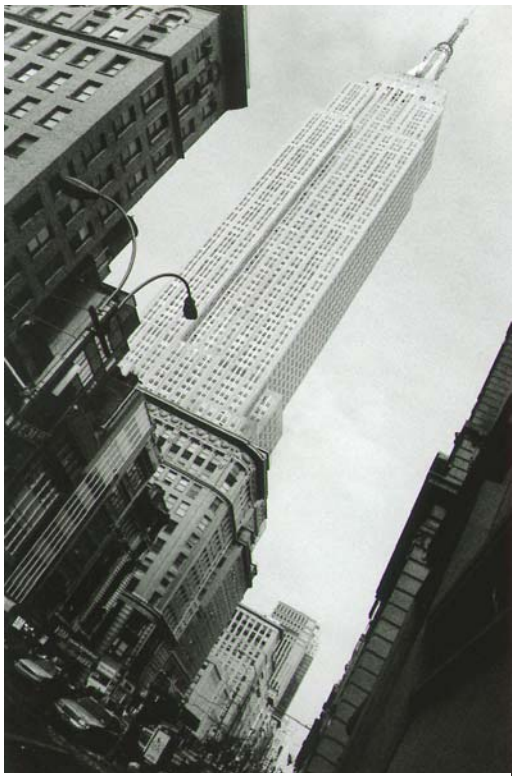

Figure 2 Empire State Building, 350 5'Th Avenue

New York City lies at the mouth of the River Hudson. The City is made up of five boroughs separated by various waterways. Brooklyn and Queens occupy the western portion of Long Island, while Staten Island and Manhattan have their own landmass. Bronx in the north is attached to the New York State mainland. New York City has an area of 780 square kilometres and is populated by more than 8 million people, while 21 million people populate the New York Metro area (Smallman, 1997).

History:

The area had been populated for more than 11,000 years before Giavanni da Verrazano, a Florentine, arrived at New York Bay in 1524. By 1625 Dutch settlers had established a fur trade with the local Indian population, and eventually their settlement was named New Netherland. Peter Minuit, the director of the Dutch West India Company, purchased the island from the local tribes for gods worth 60 guilders. By the 1670s the colony had became British and was renamed New York. Political resistance against the British colonial rule surfaced as early as the 1730s. By the end of the American Revolution in 1789, New York was a busy seaport of 33,000 people (ibid). During the Civil War, the city provided many volunteers for the Union army. But as the war wore on, protests against the war effort came about, especially after the mandatory conscription was introduced. In the Draft Riots of 1863, Irish immigrants protesting the provisions that allowed wealthy men to pay $300 to avoid fighting, after a few days turned their anger against black citizens, who they saw they as the real reason for the war, and eventually 11 men were lynched in the streets and a black orphans home was burned to the ground (Durham, 2002).

The rest of the 19'th century proved a boom time for the city's population due to European immigration and the lax oversight of industry and stock trade. The first skyscrapers were built to house corporate headquarters. In 1880 the population reached more than 1,1 million, which led to the inclusion of Queens, Staten Island, the Bronx and Brooklyn as 'boroughs' of New York City in 1898. Through Ellis Island, the immigration wave peaked for a second time, with the population exploding from 3 million in 1900 to 7 million in 1930. As the immigrant population gained political strength, demands for social change grew, and during the Depression, Fiorella La Guardia (a previous Ellis island interpreter) was elected mayor and he expanded the social service network and fought municipal corruption (ibid).

During World War II, New York became an important shipping port for supplies, weapons and troops to the allied forces in Europe and Africa. The city was refuge for many Europeans that fled Nazism and Fascism in their home countries, while Japanese nationals were interned at Ellis Island. After the war United Nations were formed, and the headquarters were built in New York City. The rising skyscrapers of corporate headquarters in Midtown Manhattan reflected America's new role as emerging international superpower (Durham, 2002). But social tension grew as more than one million white middle class Americans moved out the suburbs (nicknamed "The Great White Flight") and the influx of Afro-Americans and Puerto Ricans into the ghettoes of Harlem, Bedford Stuyvesant and South Bronx looking for better jobs and lives. During the sixties several race riots occurred across the city, and in the

seventies South Bronx were on perpetual fire. The recession culminated in 1975, when New York City had more than one billion US dollars in debt and bankruptcy was prevented by a massive state loan. In the early eighties the recession receded as international and national share values rose and the marked trends yielded positive results. New York City became the epitomized centre of Western Capitalism, the cultural birthplace of the Yuppie culture (ibid). During the late nineties the deflation of the .com industry signalled a possible new recession that the destruction of the World Trade Centre September 11, 2001, did nothing to abate. Post 11 September New York City saw a dramatic increase of lost jobs and increased unemployment rates[8], security paranoia and a national mindset of war against invisible enemies abroad and domestic (Eaton, 2003).

Internet

The Internet is a collection of smaller computer networks that are interconnected across the world through the global telecommunications network such as phone lines, Internet dedicated high-speed fibre optic cables and satellite connections. The Internet has no geographical boundaries and central government as such, but is limited by technology. Each computer on this network has a unique address and can communicate with each other through a common computer communications protocol known as TCP-IP[9] (Seagaller, 1999). TCP-IP is the current protocol of packet switching technology. This protocol forms the basis for computer communication on the Internet today. Files to be transmitted across the networks are disassembled into smaller electronic pieces (packets), and sent through the networks and reassembled at their destination. With this kind of technology, computers with different operating systems or type can communicate freely with each other, and even if parts of the network is disabled, the packets can automatically find a detour and reach its target destination. The Internet enables users to communicate through different media such as streamed video or sound, text or images (Hafner & Lyon, 1996). The most used dissemination of information on the Internet today is through Web pages, which constitute the bulk of

[8] More than 176,000 jobs lost since 2000 and unemployment rate has increased from 5.3 percent in spring 2001 to 8.4 percent in December 2002 (Eaton, 2003)

[9] TCP-IP consists of several layers, of which IP is responsible for moving packet of data from node to node, forwarding each packet based on a four-byte destination address (the IP number). The Internet authorities assign ranges of numbers to different organizations. IP operates on gateway machines that move data from department to organization to region and then around the world. TCP is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

Internet traffic. The exact number of Internet users is difficult to acquire but a recent census estimated the number of Internet users to be 605.60 million people[10] (as of September 2002). The numbers of Internet users still rises and unlike previous communication technology it does not need the construction of huge and costly infrastructure. Wireless and cellular networks enable third-world countries to set up their own networks relatively quickly and cheaply.

History:

At October 4th, 1957, a Russian rocket carrying the Sputnik satellite tore through the early morning mist and the U.S. foreign policy. Suddenly the Soviet Union now had the capacity to use atomic warheads on American soil beyond the reach of U.S. anti-air defence systems. In an effort to regain their technological lead, the U.S. government formed the Advanced Research Project Agency, abbreviated ARPA. One of their projects was the forerunner for the Internet and ARPANET gained funding in 1962 (ibid). ARPANET was an early academic research device to test the validity of packet switching technology (see above). The first "hackers" appeared at Massachusetts Institute of Technology as the first computer science researchers (Levy, 1984). In October 1969, the first network[11] demonstrating the packet switching technology was created, and in 1972 e-mail enabled network users to communicate with each other. In 1973 Arpanet became international when it connected the University College in London, England, and the Royal Radar Establishment in Oslo, Norway together (Hafner & Lyon, 1996). By this time the network is mostly an academic research tool In 1979 USENET is deployed[12], a form of public discussion forums with a wide variety of topics, today forming an important and massive communication channel with tens of millions users and hundreds of thousands topics. As the computers became cheaper, smaller and more effective during the late seventies and eighties, more and more companies started to use the Internet as a communication tool between themselves and their customers abroad and internationally, and the use of Internet grew exponentially. In 1983

Figure 3 Computing in 1971: the IBM 370 model 135.

[10] Survey statistics taken from http://www.nua.ie/surveys/how_many_online/ website
[11] The first hosts of the ARPANET connected the Stanford Research Institute, UCLA, University of California Santa Barbara, and the University of Utah together (Hafner & Lyon, 1996).
[12] Made by Tom Truscott and Jim Ellis, two grad students from the University of North Carolina (Hafner & Lyon, 1996).

the military network split from the ARPANET, becoming a separate network known as MILNET. During the period 1982 – 1987 TCP-IP is created, a computer network protocol, by a research team headed by Bob Kahn and Vint Cerf. The term Internet gradually takes over and replaces ARPANET. Personal computers appear in the eighties, spurring on a new generation of hackers (Walleij, 1998).

By 1989 commercial Internet providers begin to appear, such as CompuServe. In 1990 the Electronic Frontier Foundation is founded, its agenda to protect fundamental rights regardless of technology and "to educate the press, policymakers and the general public about civil liberties issues related to technology; and to act as a defender of those liberties"[13]. In 1991 the commercial limits on the use of the Internet were lifted and HTML is born at CERN in Switzerland. Hyper Text Mark-up Language is the communication language of Web browsing, which forms the main block of Internet use today. Mosaic, the first web browser is launched in 1991 (Seagaller, 1999). Internet traffic at this time grows at an amazing 341,634 percent rate each year (Zakon, 2003). From the early nineties onward, commercialisation and expenditure of web-based business accelerated dramatically, until the "dot-com" death in 2001 (Ellin, 2001). Simultaneously the image of hackers has gone from electronic pioneers to electronic criminals. As Sterling puts it in his final chapter, "Something is ending here, gone forever, and it takes a while to pinpoint it. It is the End of the Amateurs" (1991: 301).

[13] Cited from Electronic Frontier Foundation homepage at http://www.eff.org

Previous Research on Hacker Culture

Computer Security, Criminologists and Journalists:

A majority of the research papers written about hackers appears to be written for the major opponents of the hackers: the computer security industry. This research seems to embrace a deviant behaviour perspective on the basis, formation and motivation of hackers and hacker culture with a pathological conclusive. The research rhetoric is judgemental and embraces hegemony notions of hackers being subsumed in the wider category of computer criminals. The primary audience of this research appears to be the academic, corporate and governmental milieus:

> "As the new millennium approaches, we are living in a society that is increasingly dependent upon information technology […]. Hackers represent a well-known threat in this respect and are responsible for a significant degree of disruption and damage to information systems. However, they are not the only criminal element that has to be taken into consideration. Evidence suggests that technology is increasingly seen as potential tool for terrorist organizations".
> *(Furnell & Warren, Computers and Security, 1999:28)*

> "As we can see from countless hacking scenarios, it is clear that hackers inflict various levels of criminal acts, which range from stealing money, defacing websites, and promoting political beliefs"
> *(Richard Thieme in Network Security, October 2002:1)*

There has been written many journalistic books on hackers, especially depicting tales of chasing down hackers from the chasers viewpoint. Titles such as "The Fugitive Game" (Jonathan Littman, 1997), "Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It" (Tsutomo Shimomura & John Markoff, 1996), "The Cyberthief and the Samurai" (Jeff Godell, 1996), "The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen" (Jonathan Littman & Roger Donald, 1997) and "Masters of Deception" (Michele Slata, 1996) are all examples of this genre befitting 21'st century crime books. This type of journalism appears to conceive and reinforce the media image of hackers as criminals (Chandler, 1996, Taylor, 1999).

Notable authors that divert from this criminal perspective on hackers are Bruce Sterling and Stephen Levy, the latter whose book "Hackers: Heroes of the Computer Revolution" has become a central cultural reference material for hackers and those aspiring to be hackers.

Bruce Sterling, in his book *The Hacker Crackdown*, claims that "hacking can describe the determination to make access to computers and information as free and open as possible [...] the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit" (1992:50-51). He muses over a historical parallel in which teenage males were kicked out of the telephone systems when they were abusing it; just two years after Alexander Graham bell had invented the telephone. Drawing on numbers from the US police crackdown on the computer underground he estimates that there are some 5,000 active hackers worldwide, with about one hundred "elite"-hackers that are capable of penetrating even the most sophisticated system (ibid). His book centres on the Secret Service hacker sting operation "Operation Sundevil" in 1991, the main characters, events and its fallout and documents the creation of the Electronic Frontier Foundation. This electronic civil rights organization was formed in the wake of the crackdown on hackers in the late eighties and early nineties (ibid).

Steven Levy, in his book *Hackers: Heroes of the Computer Revolution*, considers hacking to be "[...] the free-wheeling intellectual exploration of the highest and deepest potential of computer systems" (Levy, 1984, in Sterling, 1992:53). He explores the historical roots of hacking, establishing Massachusetts Institute of Technology as the birthplace of the first hackers and the term hack. He then narrates the home computer revolution, which formed around the Homebrew Computer Club in San Francisco, California, to the mid-eighties 's first software game programmers. Most of the characters in his book as described as "adventurous, visionaries, risk-takers, artists…" (Levy, 1984:7). A central feature of his book is the description of the hacker ethic that shapes and controls the actions of the 'real' hacker. This set of ethic guidelines Levy describes as evolving from the first computer research environments, and being adopted and politicised by computer users in the seventies in an attempt to "break computers out of the protected AI towers, up from the depths of the dungeons of corporate accounting departments, and let people discover themselves by the Hands-On Imperative" (ibid: 157). The ethics defined by Levy still are central in the identity formation of hackers, as we will see later, albeit it has evolved and multiplied into different version.

Social Sciences:

To my knowledge, and having exhausted the academic sources within my ability, there is not any anthropological research of importance on hacker culture. Much of the relevant research material has been located in sociological and criminological studies. I will base the

main part of the theoretical material on studies performed by sociologists, but still see the anthropological relevance as their findings have been based on participant observation techniques and interviews with members of the culture. In particular Jordan and Taylor's article "A Sociology of Hackers" (1998) and Paul Taylor's book "Hackers: Crime and the Digital Sublime" (1999) stands out as the most relevant works. I will present their findings with relevance to my work; with an emphasis on the group identity formation, hacker dichotomies, motivations and gender division. Amanda Chandler has written an interesting article on the media image of hackers (1996). I will refer to the relevant points of her article, as I am to later discuss Sarah Thornton's ideas on the relationship between subcultures and media.

A recurring problem with analysing underground communities is the difficulty in compiling adequate empirical data. Tim Jordan and Paul A. Taylor notes: "analysing any intentionally illicit community poses difficulties for the researcher. The global and anonymous nature of computer-mediated communication exacerbates such problems because generating a research population from the computer underground necessitates self-selection by subjects and it will be difficult to check the credentials of each subject" (1998:760). Beyond compiling ethnographic data, demographic data appears to be difficult as well to collect from the underground community.

Hackers has repeatedly been pathologically defined as isolated young men, but Jordan & Taylor repudiate this claim since they see hacker community as one of lively information exchange through computer-mediated communication, publication of papers and hacker conventions. They point out that psychological interpretations of individual hackers may reveal the reason behind hacking but that this kind of pathologic view[14] of hacking motives is related to the mainstream fearing computers controlling their lives (ibid).

Jordan and Taylor views the hacker community as one imagined in the sense of Anderson's concepts; "[…] the collective identity that members of a social group construct or, in a related way, as the 'collective imagination' of a social group" (ibid: 762-763). The computer underground can be understood as a "community that offers certain forms of identity through which memberships and social norms are negotiated" (ibid: 763). This makes it possible to understand a hacking community that use computer mediated communication to exist worldwide and in which individuals often never meet offline (ibid).

[14] The most recent pathologic explanatory model for hacker motivation is the speculation that hackers suffer from a mild form of autism, the Asperger Syndrome. The characterizations of this disorder are: poor social skills, persistent and repetitious fidgeting and collecting oddities that pertain to their technical interest (Zuckerman, 2001).

They claim this "imagined hacker community" can be outlined through six main elements. Hackers relate to technology in an all-consuming and comfortable manner. The publicity inherent in gaining information and recognition juxtapositions the illicit nature of hacks, which make hackers have an ambivalent relationship to secrecy. This relates to the anonymity of a hackers online identity that are different from the hack's secrecy. Hacking culture has "no formal ceremonies […] or ruling bodies to satisfy to become a hacker" (ibid:766), which make it similar to other informal networks in that its boundaries are highly permeable. Jordan and Taylor point out the male dominance of hacking culture, which accounts for its misogyny, and they claim that research fails to yield evidence of female hackers. These structures are internal to the hacking community in that their significance is largely for hackers and do not affect or include non-hackers. Jordan and Taylor consider that in order to categorize a hack as a hack, it must be related to its motivation and not to how you perform it. These motivations may be guided by a set of principles, based on Sherry Turkle's previous work: simplicity, mastery and unlawfulness (Turkle, 1984 in Jordan & Taylor, 1998). The simplicity principle implies austerity that is able to impress, mastery derives from sophisticated technological expertise and its unlawfulness becomes of its challenge of legal and institutional statute. Furthermore they discuss several discourses that may explain the motivations behind hacking: computer and computer network addiction or sheer curiosity exploring these, justifying illicit hacking by their boring offline life, being able to gain control over high-profile and status networks such as NASA and CIA, peer recognition from friends or other hackers, or the chance of obtaining a financially rewarding job position at a computer security firm (Jordan & Taylor, 1998). They see hacker community defining itself and its boundaries in relation to other groups, and especially the computer security industry (abbreviated CSI) of which the relationship is especially antagonistic and intimate. "There is no other social group whose existence is necessary to the existence of the hacking community" (ibid: 770), and these boundaries emphasise the ethical rendering of hacking because sometimes its difficult to acknowledge who is a hacker and who is a CSI member. Even if members of CSI community decry hacking activities, they themselves sometimes utilise hacking methods to catch hackers. In that respect they refer to Clifford Stoll's book "The Cuckoo's Egg: Tracking a Spy Through the Maze of Counter-espionage" where the author narrates his attempt to track down a hacker using hacking methods. By such means as borrowing colleague's computers without permission, monitoring other people's electronic communications and inventing his own surveillance equipment he chases the hacker across the Internet (Stoll, 1989).

Paul A. Taylor's book "Hackers: crime in the digital sublime" (1999) seeks to understand the social processes of hacking while attempting to steer away from the sensationalist crime journalism that marks contemporary hacker research (ibid). Based on interviews and e-mail correspondence Taylor discusses the issues from the perspectives of computer scientists, security analysts and hackers. He examines the hacking culture, their motivations and the state of the security industry. Hacking has become a term that is part of a complex social process in which certain computer users have become marginalized within a wider computing community. Due to the structure of Internet, it allows for co-operation spanning different levels of technical ability, but because of the absence of any central governing faction within the hacker culture, hackers have come to be affiliated with anarchism. Hacker culture exists outside the conventional, physical, society, in a non-traditional computer mediated / digital environment. Subsequently hacker motivations determine how the outside world views them. He finds it difficult to study hacking with a monetary or criminal motivation due to its underground nature, but finds that such hacking is performed on the margins of mainstream hacking, and then usually only in order to fund such activities. He also sees the academic theories of hacker motivation mainly pertaining to psychological models, focusing on obsession, addiction and compulsion. In his view hackers appears more as innovative and curious individuals who will not and cannot stop their inclination of exploration, with hacking emerging as an interesting application of subversion of resistance on the Internet. Taylor considers the apparent lack of female hackers due to societal factors such as the sexual stereotyping of young children through for instance gender divided toys, and the computer environment as masculine in which women feel threatened, uncomfortable or alienated (ibid).

Figure 4 CNBC headline in the aftermath of the Denial of Service attacks in February 2000.

Amanda Chandler has done a paper on the image of hackers in the popular discourse (1996), in which she sees the definition of hackers changing with each new generation of computers and computer users (ibid: 230). The first generation of hackers were members of the first computer research milieus, at US academic institutions, in the early sixties, and the second generation being the computer hobbyists in the seventies that saw the possibility of bringing computer power to the people. The ensuing personal computer revolution in the early eighties "may be seen as one of the many aspects of the Sixties counterculture, but it just as easily be described as illustrative of the success of capitalism" (ibid: 231). The third generation were the users that cracked, traded or sold the first pirated computer software of the personal computers. Cracking software piracy protection often became the incentive to learn computer skills. The fourth generation shares the same obsession of computers and has inherited the advances of the personal home computer, but has appropriated the term hacker and made it synonymous with computer crime. She makes an interesting note of how the American media, especially the press, has utilised symbol-laden language that pertains to American culture and history. The cowboy being the embodiment of Americanism extols values and ideas that many Americans appreciate and some even strongly advocate and defend. "The outlaw, the rebel, the rugged individual, the pioneer…the private citizen resisting interference in his pursuit of happiness – these are figures that all Americans recognise" (Sterling, 1992 in Chandler, 1996:233). With the cowboy and his world saturating American economic and cultural thought it is "not surprising that hackers […] adapt this positive heroic model for their own" (ibid: 234). Even so the depictions and representation of hackers are negative, especially in Britain where their exploits are explained as dangerous and subversive. The American image is more ambivalent, where the hacker can be related to the cultural backdrop of USA, sometimes even sympathises with hackers (ibid: 250)

The Manifestation of Hacker Culture

Hacking History

> *Hackers believe that essential lessons can be learned about the systems - about the world – from taking things apart, seeing how they work, and using this technology to create new and even more interesting things. They resent any person, physical barrier, or law that tries to keep them from doing this.*
> (Levy, 1984:40)

Hacker history is an important part of the process of cultural boundary formation. It defines the relationship to fields of power and as well as to other underground computer user groups within the cultural field. In this chapter I will introduce the reader to the chronological history of hackers, which I have divided into five parts. I start with what can be claimed as the basis for hacker culture, the early radio and electronic amateurs before I look at the first computer research environments in USA, which holds a central place in formation of hacker culture. The dissemination of telephone network hacking knowledge, or phone phreaking as it is called, emerges in the late sixties and early seventies as a tool that subversive political subcultures claim use of not only as rhetorical dissemination of protest but also as a form of subversive action. Following the introduction of the personal computer and its massive commercial success and proliferation thereof, it begets a whole new era where the spread of underground knowledge and hacker techniques spawns computer user groups that makes use of hacker techniques but don't acknowledge hacker ethics. The legal reactions of the state in regards to computer hacking change from viewing it as an unimportant nuisance in the mid-seventies to defining it as a severe threat to national security in the ranks of terrorism in the late eighties. The commercial adoption of the Internet in the mid-nineties – and the explosion of the number of its users – yields another generation of computer hackers as the hacking tools become readily available by just typing in a few keywords into a web search engine. We also see the up rise of hacktivism, consisting of hackers that claim a political incentive for their actions.

1900-1950: Radio and Electronics Amateurs

"*Electricity, especially Wireless, are positively the strongest home-magnets today. His workshop, his small Electric laboratory or his Wireless Den are the most powerful home attractions for the 20th Century Boy.*"

(Electro Importing Catalog 14, 2nd Edition, 1914:144)

Figure 5 Advertisement for the Electro Importing Company's new radio transmitting-and-receiving package, the "Telimco Wireless Telegraph Outfit". Scientific American, November 25, 1905.

The foundations for hacker culture, and its fascination of interpersonal communication and technology, can be traced back to the early 20'th century when the first radio and electronics enthusiasts made their own radio transmission and receiving equipment, and communicated by Morse code. The first technical instructions appeared in Amateur Work (*Hertzian Waves* of November, 1901), and Scientific American Supplement (*How to Construct An Efficient Wireless Telegraph Apparatus at Small Cost* of February 15, 1902).

The radio amateurs became the first virtual community, limited by technology yet existing beyond geography, where many of these early amateurs were adolescent males and gained their knowledge from radio amateur magazines (*Modern Electrics*, *The Electrical Experimenter* and *Radio Amateur News*) and other radio operators. Initially the press hailed the adolescents as boy-inventor heroes ingeniously mastering the ether, but as the number of radio enthusiasts grew steadily - especially in the more industrialized US northeast - their sheer numbers caused a lot of interference with commercial or US navy airwaves (Douglas, 1987). When the rescue operation of the Titanic on April 15, 1912 supposedly became disrupted due to radio interference, a national radio legislation was introduced that reduced the available wavelengths to 200 meters This regulation of amateur radio with its obligatory certification and courses meant that many previous amateurs were excluded for economical and practical reasons. Radio and electronic amateurs continued to thrive during the 20'Th century as the kits became more sophisticated, cheaper and more available (White, 2003)

1950 – 1970: From MIT to Yippies

MIT are one of the most prominent and advanced technical research universities in USA. Somewhat surprisingly maybe, the origin of the term "hack" can be traced back to pranks performed by unknown students at the MIT campus. These were practical jokes which were characterized by humor and finesse such as covering the MIT dome with reflective foil or – at the top of the same dome – place a police car replica complete with blinking lights, a policeman dummy and a box of doughnuts (Peterson, 2003).

The term eventually migrated to the first computer research environments where it became a synonym for intense, creative and innovative sessions of computer programming. One of the foremost recruitment places for this first generation of hackers was the Tech Model Railroad Club of MIT (Massachusetts Institute of Technology). This was the place were electrical engineering students and teachers met in their spare time in the fifties and sixties[15]. Their huge model train set was expanded upon with increasing technological finesse and one of its monumental achievements was the construction of a control system made out of telephone switches.

> […] This control system was an attraction to the sort of people who liked logic problems and switching circuits and the same kind of people who were attracted to computers when they first became available
>
> (Andy Miller, fieldwork interview spring 2000)

The control system consisted of sophisticated phone equipment that had been acquired by one of its members that also were in charge of the campus phone system. Using the control system enabled its users to simultaneously control several trains on different parts of the track. The hack at TMRC became synonymous with innovation, style and technical virtuosity and members who put the most time in the construction process were called "hackers" (Levy, 1984). When Digital Equipment Corporation (DEC), a leading computer manufacturer in the USA, donated one of its first digital computers[16] to the MIT, many of the TMRC members, who were students, started using the computer for their own student research projects. These projects were characterized by playfulness, technical virtuosity and intellectual challenges. The students – or hackers - would spend many days working non-stop on projects that weren't on any teaching curriculum such as programming a assembly program (an program that

[15] The TMRC is still 'operational', with a web page available at http://tmrc.mit.edu/

[16] The PDP-1. Before this computer appeared some of the TMRC members used the TX-0, which was a predecessor to the PDP-1 (field notes, 2000).

translates assembly language to machine language) for the PDP-1 during a weekend or making the first computer game called "Spacewar":

> [You'd] have a little rocket ship and a sun. One version of it had a real time diagram of the solar system were all the stars were and so fort. The sun had gravity; if you fired a projectile from your rocket it would curve inwards towards the sun because of the gravity and so fort. It had all these high-tech features and it was considered an intellectual challenge, I think, to add these.
> (McNamara, fieldwork interview spring 2000)

A hack was viewed as something benign, something that would help you and others gain knowledge as well as being aesthetically pleasing in terms of its technological sophistication. They were not meant to penetrate existing systems or do any harm:

> So I guess the point of all this is to say that computer hacks in those days were very innocent sort of pranks. That was not intended to - or in general design - break into anyone system or to do any harm or anything. The computers weren't networked and everything was fairly simple and transparent.
> (Alan Kotok, fieldwork interview spring 2000)

The first hackers also developed a working ethos – a hacker ethic- that two decades later was put into book[17] form by Steven Levy (1984). The working ethos can be seen as existing in the absence of administrative structures and not being constrained by any division of labor (Hannemyr, 1997). The hacker work ethos emphasized hands-on teaching, sharing of resources and free access to information. Progress and innovation often evolved or came about through non-curriculum experimentation or "hacking" as it was named. In "Hackers: Heroes of the Computer Underground", Levy distils the following points:

[17] "You bring up this question of hacker ethic. I had given of energy and time to Steven Levy [and] his book and I guess I would say he distilled that out of his interviews" (Alan Kotok, fieldwork interview spring 2000)

- Access to computers – and anything, which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On imperative
- All information should be free
- Mistrust Authority – Promote Decentralization
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer
- Computers can change your life for the better

(Levy, 1984:40-46)

As the academic and commercial research came under corporate-style management during the sixties, much of the hacker culture disappeared. "Scientific Management", an invention by the engineer Frederick Winslow Taylor, aimed at taking the control of the work activity away from the workers. This was done by increased standardization and work specialization. Taylor meant that this was the only way management could have the desired control over productivity and quality. For computer programmers, this meant that programming now had to go through standards, reviews, structured walkthroughs and "miscellaneous productivity metrics" (Hannemyr, 1997). Suddenly rigorous labor division made the free intellectual roaming of hackers impossible.

In the late sixties another kind of hacking came into being, the hacking of telephone networks, or *phone phreaking* as it was called. This was a name for a number of techniques that basically enabled you to use the telephone for free. Phone phreaking utilized technical information that was readily available in libraries or technical magazines. But most, if not all, of the information on telephone systems security, was so technical and obscure that most people wouldn't know how to use it.

> Well I think there was a view that telephone systems security was mostly security by obscurity, that's the assumption that people wouldn't know well enough about it to exploit [it]. So you get a bunch of MIT students who for whom understanding how things work is a major goal in life […] so how this system works will be learned and [it's] weaknesses will be exploited!
>
> (Alan Kotok, fieldwork interview spring 2000)

Captain Crunch gained worldwide notoriety after an Esquire article highlighted his elite phone phreaker skills[18] (Rosenbaum, 1971). He gained his nickname when utilizing a children's whistle found in the "Cap'n Crunch" breakfast cereal box. Given to him by blind friends – that constituted a substantial percentage of the phone phreaking community – he used the whistle to access AT&T long distance switching equipment. The whistle emitted a tone with the frequency of exactly 2600 Hz. This was exactly the same note that AT&T and other long-distance companies used to indicate available long-distance lines. Thus, used in conjunction with a Blue Box[19], Captain Crunch could make long distance calls to his girlfriend from Los Angeles to New York. He also connected two telephones in the same room to each other, across the globe, hearing his own voice with a 20 second delay (ibid).

During the early seventies, dissemination of subversive technological techniques such as phone phreaking starts appearing in an underground leaflet called *Youth International Party Line*. Founded by Abbie Hoffman – author of "Steal This Book!" - YIPL brandished a neo-anarchist, anti-establishment and anti-war agenda, publishing detailed instructions on how to exploit telephone networks systems as well as other governmental and corporate infrastructures. YIPL was the technological manifest of *Yippies*, hippies with a revolutionary agenda, that during sixties and seventies "carried out a loud and lively policy of surrealistic subversion and outrageous political mischief" (Sterling, 1994:43), including tossing hundreds of dollars to the trading floor of the New York Stock Exchange - causing general mayhem as the brokers scrambled for the money - and gathering hundreds of meditating demonstrators attempting to levitate the Pentagon[20].

The subversive activities of YIPL and the Yippies diminished as the Vietnam War wound down to an end, and in 1973 a new phone phreaking leaflet appeared. TAP, or Technological American Party[21], published more sophisticated telephone systems exploiting articles as well as formula for explosives, pirate radios and how to illegally alter gas or electric meters but playing down the political agenda (Taylor, 2001). An important turning point was TAP's decision not to publish the plans for the Hydrogen bomb as this would destroy the phone system which its readers so enthusiastically exploited/explored (Ross, 1990).

---

[18] Captain Crunch is still a household name among phreakers and hackers. His website at http://www.webcrunchers.com/crunch/ retells some of his old tales of phreaking as well as his current work as a computer security developer (http://shopip.com/index.html)

[19] A Blue Box is a tone-generating device that enables its user to communicate with the switches of the telephone company that utilizes the multi-frequency (MF) system.

[20] "They sought to pull Uncle Sam's pants down in public, to show that revolution could be conducted in a spirit of festive non-violence", http://www.cleartest.com/testinfo/anitahoffman.htm

[21] In 1979 it changed its name to "Technological Assistance Program".

The "newsletter for the exchange of anti-Big Brother technical information" ceased its publication in 1984, but in the same year "2600[22]:The Hackers Quarterly" took over, its editor taking on the pseudonym of Emmanuel Goldstein the name of the protagonist that battles the totalitarian regime of Big Brother's Oceania in George Orwell's *1984* (Sterling, 1992). "2600" catered both to the phreaking and emerging hacker culture of the eighties.

1970-1980: Computers To The People

In 1968, two engineers, Robert Noyce and Gordon Moore, left their jobs at Fairchild Electronics, and started their own electronics company that they called Intel. They started producing semiconductor computer memory, but revolutionized the computer business when they produced the first microprocessor in 1969. This was basically a multipurpose logic device that received its instructions from a semiconductor memory. In 1971 Intel began producing the Intel 4004, a 4-bit microprocessor[23], and in 1972 Intel released the 8008, an 8-bit microprocessor, which sold for US $360. For the first time, computer power was now available not only for corporations and research institutions, but for everyone (Levy, 1984).

The MITS (Model Instrumentation Telemetry Systems) Altair 8800[24] was the first computer kit available as a mail order. The Altair used the new Intel 8080 microprocessor. It was introduced on the market through an article in Popular Electronics in January 1975 and MITS[25], who was on the brink of bankruptcy, went in three weeks from a negative bank account to plus US$250.000 when the sales of the Altair went through the roof. One of the first programs sold with the Altair was BASIC (Beginner's All-purpose Symbolic Instruction Code) authored by Paul Allen and Bill Gates from their own experience and other public available versions of BASIC. The Altair prompted the appearance of several computer user groups around the USA. Most of its members were electronics hobbyists as well as professional engineers and technicians that shared the same fascination for computers as the members of TMRC. The Homebrew Computer Club of San Francisco and the Altair

Figure 6 The MITS 8800a

[22] The "2600" refers to AT&T's long distance MF-system and Captain Crunch's hack.
[23] A 4-bit architecture in a microprocessor means that it works with 4 bits of data. 4-bit is very limited in terms of usage, as you cannot express characters or letters. An 8-bit architecture means that the computer is able to handle computer instructions, upper and lower case characters, numbers and symbols.
[24] The MITS Altair 8800 was based on the 2 MHz Intel 8080 processor with 256 bytes standard RAM. It was programmed through front panel switches in machine code language that consisted of binary digits.
[25] The demand for the Altair was beyond the production ability of MITS, and Pertec, a large electronics company, eventually bought up the company.

8800 spawned several small business enterprises that eventually would become multi-billion international corporations (ibid).

Even though the Altair wasn't either user friendly or a long-lived commercial success, an example had been set, and numerous other personal computers appeared quickly in its wake. Computers now also appealed to non-experts in computing and electronics, as it did not need complicated assembly work. One of the first commercial success was Apple][(2) made by the Apple company released in 1977. The founders Steve Jobs and Steve Wozniak had both been inspired by the Altair presentation in a meeting at the Homebrew Computer Club and had shortly thereafter constructed the Apple I in Wozniak's garage. The Apple][was a unique machine in that it had the ability to being hooked up to a TV and gives the user sound, colour and graphics. Together with VisiCalc, the first spreadsheet program, the sales reached 300,000 units by 1981 (ibid).

The commercial conception and viability of personal computers post-dated the notion of political and intellectual empowerment by taking computer power away from the corporations and governments and giving the people access to computer in their homes. This ideology grew out of the Community Memory organization in Berkeley (Levy, 1984) and the Whole Earth Catalogue (Sterling, 1992). Letting people having access to computers and communicate with each other became "a testament to the way computer technology could be used as guerrilla warfare for people against bureaucracies" (Levy, 1984:156). A few years later this was ultimately commercially epitomized by the 1984 Super Bowl commercial[i] for the Apple Macintosh were an utilitarian bureaucratic entity was toppled when a sledgehammer hurled by a young, athletic woman destroyed its Big Brother TV screen spouting propaganda to its mindless drones. As the light of freedom liberated the drones a voice over announced: "On January 24th, Apple Computer will introduce the Macintosh. And you'll see why 1984 won't be like "1984."" (Friedman, 1997)

Following upon the success of the Apple][[26], several other personal computers appeared on the marked. The Commodore Vic 20 (1980), IBM PC (1981) and Commodore C64 (1983) were each hugely popular[27] and formed the basis for the next generation of hackers. By 1983, there were 10 million personal computers in USA alone, and by 1989 the number had raised to 54 millions (Knight, 2001). Computers and computer power were no

[26] Apple][ceased production in 1993 (http://www.lowendpc.com/history/index.shtml)
[27] The Commodore C64 alone selling between 17 and 22 million units worldwide (http://www.ballyhootown.com/bite/compsci/timeline6.html)

longer confined to corporate or governmental institutions and a new generation of hackers grew out of the new technology now available to most teenagers (Chandler, 1996).

1980-1990: The Golden Age Of Hackers

My personal experience with computer started about 1984. Many of my friends received a computer as a Christmas or birthday present from their parents. We would gather at their house and type program listings found in computer magazines into the computer as well playing games. Most if not all of the games were pirated, that is their copyright protection had been broken, and the software was distributed on cassette tapes or disks, depending on what equipment your computer had. The network that we exchanged tips, programs and utilities through was of a peer-to-peer type. You knew someone who had friends with access to software, or someone who knew someone closer to a software source, and during time this network also grew to encompass people with different computers, skills and accesses. Payment of pirated software was unheard off; not only was it illegal but it was frowned upon as the general consensus was to swap software. Cracking computer software copyright protection often became the incentive to acquire computer skills:

> It was on these meetings that a guy […] started to bring along games that his father had brought home. This was the incentive to learn assembly [in order to] remove copyright protection. The games that we then managed to hack/crack/whatever was distributed very quickly among the local network of people, and later among the channels we had to other groups in Norway and other countries (but only within Western-Europe, not that it was conscious choice). New people that came into the local network got what they wanted of what we had. After some time it was expected that one should give something back or contribute with coding or something else. I never experienced that someone expected to be paid for something.
>
> . (Norwegian informant, email correspondence 2003)

A film released in 1983 captured the societal fascination with the new computing technology prevalent in many homes at that time as well as immediately becoming a major cultural reference point for hackers. “War Games” (1983) essentially caught the zeitgeist of hackers in the early eighties. It portrayed a young hacker who without any malice evident explored computer and telephone networks.

Figure 7 The hero and his to-be girlfriend in ”War Games”, 1983.

The extent of his misconduct was when he changed his school grades, and it was by pure chance that he came across a phone number that connected him to a computer that controlled the American missile defence command, NORAD (IMDB website[28]).

The main protagonist of "War Games" used a war dialer to find phone numbers to computers. A war dialer is a computer program that identifies phone numbers that connects to computer modem. It dials a defined range of phone numbers, and logs the successful phone numbers. In the early eighties, most computers could only be accessed by individual phone lines[29], and discovering a phone number that connected you to a computer became a secret knowledge. This type of secret knowledge could be distributed on a Bulletin Board System[30]. A BBS is a computer, or a program, that is dedicated to the sharing and exchange of messages and files. A BBS may cater to a specific subject or be more general (Walleij, 1998).

The dissemination secret knowledge previously featured in YIPL and TAP, were now available as text files at secret BBS's. In order to get the phone number to the BBS, as well as the password, you had to prove your ability to the hacker underground, which operated on the mentor principle; unless you could find someone who inducted you into the inner circle of a hacker group, you were left outside. By 1985 it was assumed to be 5,000 BBS's in the USA, and by 1990 that number had grown to 30,000. Most systems enabled its users to use "handles", or nicknames, to ensure their anonymity (Sterling, 1992).

At this time the first hacker groups started to appear. Many of the first groups were formed by phone phreakers who migrated to network computers as the telephone corporations not only replaced their analogue switching technology with computerized telephone switches but utilised automated blue boxes scanning devices to deter further telephone fraud. Following the release of "War Games", the media quickly focused on this new generation of hackers, berating their assumed criminal activities but at the same time portraying the hacker as a groundbreaking pioneer on the new computing frontier. The media rhetoric assumed a Wild West analogy that to a large degree pertained to American values and ideals concerning the sovereign rights of the individual and the ingenuity of economic entrepreneurs (Ross, 1990)(Chandler, 1996). The Milwaukee group 414, Kevin Mitnick and Master of Destruction all became household names in the public arena as well as becoming part of the hacker culture (Walleij, 1998).

---

[28] The Internet Movie Data Base, available at http://us.imdb.com

[29] Until the commercial ban on the use of Internet was lifted in 1991, only scientists at research institutions and universities (that had been funded by the American Defence Department) could use the ARPANET (Hannemyr, 1997).

[30] The name derives directly from the bulletin boards at small convenience or grocery stores where people can put up simple messages.

Simultaneously other computer users that utilized hacking methods for non-hacking purposes began to appear. The destructive and criminal activities of crackers, pirates and virus creators led to a hardened governmental stance on "hacker" activities, prompting federal and state investigations, arrests and harsher sentencing (Sterling, 1992). Hacking had become synonymous with computer criminality and electronic terrorism (Chandler, 1996). Operation Sundevil in 1990, a huge Secret Service raid on several BBS's suspected of harbouring information on credit card and phone number frauds, signified a change of attitude towards hacking and hackers. The Electronic Frontier Foundation was formed at this time to protect the online civil liberties as well as to give juridical assistance to individuals it deemed wrongly accused or convicted of electronic crime (Sterling, 1992).

1990-2002 From Mosaic to Hacktivism

1993 introduced the Mosaic. Basically this was a graphical interface to the Internet. With this program, users with just a basic understanding of computer operation could easily download text files, images and sound. Mosaic, and other web browsers, introduced computer networks to people that had no such previous experience. This simplification of Internet access, as well as the introduction of readily available commercial Internet service providers, meant that BBS's no longer were the main disseminators of secret knowledge. This knowledge was now available at thousands of web sites available for a much larger audience than previously before (Walleij, 1998).

Another venue of knowledge dissemination that took over from the BBS's was the IRC networks, chat channels where the users communicated real time through text interfaces. Newcomers to the hacker scene could just listen to the conversation, or lurking as it is called, then join in and ask questions. Mentors could take newcomers in under their wing and learn them hacking skills online. Hacker IRC channels often became discursive areas pertaining to technology, recent hacking experiences and of course social banter (ibid).

The oft-publicized web defacement of corporate and governmental web sites in the mid-nineties caused much public consternation and official condemnation. Defacement usually meant replacing the home page with a message, ranging from random obscenities to political agendas. Semiotic attacks changed the meaning of the homepage, often ridiculing the original website. For example the CIA homepage was changed from Central Intelligence Agency to Central Stupidity Agency and the slogan at the British Labour party website was changed from "Road to the Manifesto" to "Road to Nowhere" (Jordan, 2001)

Figure 8 British Labour homepage defaced on December 6'Th 1996.

The nineties also saw the emergence of hacktivism as a form of online civil disobedience both on an individual and organized level. The proclamation of the Electronic Disturbance manifesto (by the Critical Arts Ensemble) in 1994 and the attacks on Mexican government network servers in support of the Zapatista movement in 1998 was hacking with a political motivation (ibid). It has also been suggested that the rise of hacktivism came about as the first generation of web hackers became politicalized in their mid-twenties and political groups became more computerized[31].

Hacktivism uses a variety of measures to attain their political goals but in general use the Internet for two different uses: Mass Virtual Direct Action (MVDA) and Individual Virtual Direct Action (IVDA) (ibid). MVDA involved the simultaneous use of Internet by many people to create civil disobedience. This could include trying to overflow the World

[31] John Vranesevich of Antionline.com in "The Golden Age of Hacktivism, Wired Magazine, September 22, 1998. No author indicated

Trade Organization homepage servers or jam the secret US-controlled surveillance Echelon[32] network. IDVA are the use of classic hacker techniques for a political reason. This could be the use of semiotic attacks, network attacks and exploiting network flaws. One such exploit was the BackOrifice by the Cult of the Dead Cow group. CDC claimed the purpose of BO was to publicly uncover the security issues related to individual privacy and safety before other exploiters with a less benign motivation could exploit it (ibid). Other hacktivism activities have taken the form of giving poor economically marginalized people Internet access as a form of digital empowerment (field notes 2000). One of my informants reflected on the impact of hacktivism when I interviewed him at the H2K conference:

> I think some of the things they are planning […] are great, such as providing Internet access for the Chinese. What the hacktivists are planning to do is punch some holes in their defences if you will, where they are keeping the Chinese inside and letting them out on that they can see […] the whole global internet. […] I think its time that the Chinese got their eyes open beyond what's given to them by their government so that they can see what's really going on out here, and let the citizens of that country decide for themselves whether or not they shall be granted that access and a revolution will occur.
> (Spudz, fieldwork interview, July 2000)

An Ethnographic Account of Hackers

> "This is our world now… the world of the electron, and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore … and you call us criminals. We seek after knowledge … and you call us criminals […] I am a hacker, and this is my manifesto. You may stop this individual, but you cant stop us all … after all, we're all alike".
> (Hackers Manifesto, by Mentor)

One of the questions I often was met by my informants during my fieldwork was if the hackers actually could be defined, in anthropological terms, as a social group? One of my informants snorted ironically when I happened to mention to another 2600 attendee, that I was interested in the hacking community. "What community?" he added to his snort, obviously disagreeing with me. It could be my older informant was making a disillusioned observation of the lack of any 'communal' feeling at that particular meeting, perhaps even suggesting that

[32] The actual existence of ECHELON remain disputed, but its potential super-surveillance capabilities had the European Parliament worried enough that they enquired a committee to investigate the alleged US-led electronic intelligence agency. ECHELON is supposedly an automated global interception and relay system that is capable of intercepting 3 billion communications daily, including phone calls, e-mails, Internet downloads and satellite communications. After collecting the data, it is filtered through the DICTIONARY, which are computer search algorithms that pick out, or 'flag', any communication that contains keywords, addresses or voices that the ECHELON supervisors are looking for. For more information go to: http://www.echelonwatch.org/

the new generation of hackers present was not hackers as he saw it. As Chandler suggests, each new generation of computers spawn a new generation of users, an electro-ecological evolution that excludes as well as includes (1996). As each new computer generation gained foothold and became more accessible, old knowledge are shelved or at best kept running for sentimental reasons. But that makes it the more interesting is to relate his statement to the rest of the material I have gathered. What defines a subculture, what differs it from a community or any other social group? Semantically the word 'community' in the Anglo-Saxon context suggest a permanent population, while 'subcultures' are in a "state of transience" (Thornton, 1997:2). Subcultures also carry connotations of insecurity, of 'appropriating the neighbourhood' for an underground, often illicit, subculture. Subcultures are also portrayed as being in opposition to the mainstream, the hegemony or just 'the mass'. As Thornton points out, up till recent subcultural research has labelled uncritically the majority in favour of the minority, accepting the subcultural definition as de facto (ibid, 1995). But even if the 'majority' actually consist of more subtle and diverse categories, as Thornton sees it, hackers still see a mainstream out there, which makes it important from an anthropological viewpoint to define it.

I would now attempt to show the different manifestations of hacker culture both on the Internet and in the physical world. What became clear during the analysis of the empirical material was that the motivation of the hack is a central part of the process that defines the social boundaries of hackers. Hackers also meet in different arenas, which all are layered in a hierarchy of confidentiality.

Arenas of Social Interaction

> We would communicate by cell phone, email, personal presence, you know. Gathering at the 2600 meetings every month. IRC, ICQ, you know, any place where I just happen to bump into them, you know, that's the place to communicate.
>
> (Spudz, fieldwork interview July 2000)

Hacker culture is one of several levels and arenas of participation and information bartering ranging from large international annual conferences[33], monthly meetings and a frantic banter going on around the clock on the IRC networks countering the media image of the social loner (Chandler, 1996)(Jordan & Taylor, 1998). Hacker culture also manifests itself

[33] Such as the biannual HOPE conference in New York and the annual DEFCON conference in Las Vegas and Chaos Communication Camp in Berlin.

through many independent magazines, radio and TV shows of which many are underground web casts (field notes, 1999-2000).

“2600: The Hackers Quarterly” and the “2600” meetings

> " Your best bet on meeting people is to show up at a 2600 meeting. Information on these is available at www.2600.com/meetings
> (PorkChop, e-mail reply)

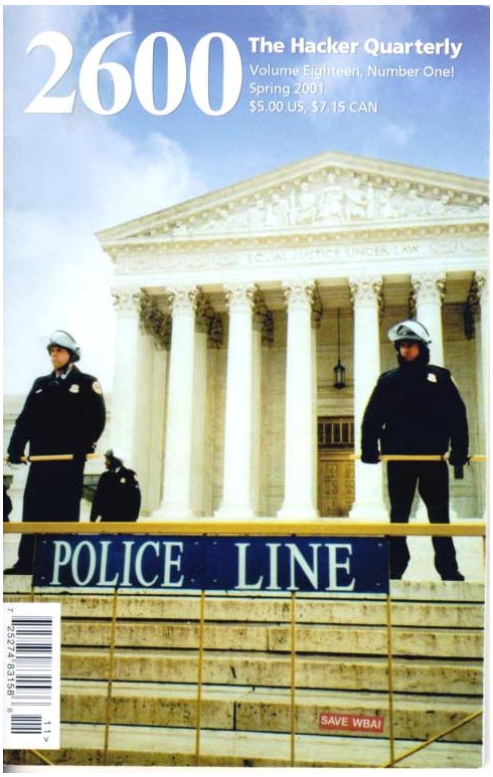

Figure 9 Front page of "2600: The Hackers Quarterly", spring issue 2001

When I first began posting Usenet messages looking for hacker informants, I received a couple of emails that indicated that the best way to get in contact with the hacker underground was to attend the “2600” meetings. The “2600” meetings springs out of the “2600: The Hackers Quarterly”, the quarterly hacker magazine, that publishes articles on hacking issues and tech related articles much in the same manner as TAP and YIPL did. The political aspect is downplayed, most of the articles relate exploit explanations of technological systems, including computers, security equipment and computer software.

But if articles seem to be devoid of a structuralized critical political stance, the editorials tend to be carrying a political annotation by for example reflecting on the current criminal liability of hacking, criticizing the societal attitude towards hackers and attacking state and corporate entities for their lack of concern for the individual. The editorials tend to repeatedly postulate the hacker ethic as a guideline for its readership in terms of hacker behaviour, and later in the “Letters” section, chastises readers that ask for “cracking” tips and tricks with reference to the hacker ethic that emphasizes the benign exploration of networks and decry the manipulation and destruction of information:

> *"Perhaps you should keep your brain open to an intelligent thought or two. One of them might be the realization that the kind of stunts you're involved in are just plain and simple fraud and have nothing at all to do with hacking. We're not interested in your little crime ring".*
>
> *"2600:The Hacker Quarterly, Volume 15, Number 3. Fall 1998.*

"2600: The Hackers Quarterly" also organizes meetings each first Friday of the month. These meetings, according to the information at their website, "exist as a forum for all interested in technology to meet and talk about events in technology-land, learn, and teach. Meetings are open to anyone of any age or level of expertise." The foremost reason to having a "2600" meeting in a public place is to counter the popular image of the hackers as having secret exclusive meetings. By meeting in large numbers in transparent places hackers want to show that they don't have anything to hide and that everybody can attend. Another reason why the hackers have their meeting in the Citicorp Plaza was explained to me being the readily access to public payphones, a highly symbolic place for hackers as it reflects upon their phone phreaking roots as well as being an practical opportunity to do hacks and show off your status as a hacker.

Signs of Hope
Police Searches of Computers
The Future of PKI
PHP/CGI Vulnerabilities and Abuses
Breaking the Windows Script Encoder
Liberating Advants Terminals
A Romp Through System Security
Hacking QuickAid Internet Stations
The Billboard Liberation Front
Computing With The Fabric of Reality
Secrets of Electronic Shelf Labels
Anomaly Detection Systems, Part II
The Anna Kournikova Virus
Declawing Your: CueCat
Scum
"Takedown" Taken Down

Figure 10 Index of spring issue of "2600: The Hackers Quarterly"

When I arrived in New York in September 1999, my first thought was to secure a meeting as soon as possible and start my fieldwork from there. The meetings would serve to be the main arena of my physical fieldwork.

The meetings followed a loosely ordered sequence of happenings whereas the first was the meeting itself. The meeting started at 5 pm down in the enclosed public space inside the Citicorp building, located next to the payphones, surrounded by brand chain stores. Participants would come and go, and in general the number of attendees were around fifty but this could vary considerably, especially when the media granted the "hacker" culture attention. This was exemplified when MTV screened a "documentary" on hackers October 13'Th 1999, and on the following meeting the 5'Th of November, the number of attendees rose to more than seventy (field notes 1999).

The Citicorp building security was obviously aware of the meetings, and the management told me that they did increase the number of security every time the "2600"

organized their meetings in their building. For the most part the security guards didn't interfere with the meeting as long as the hackers didn't get rowdy or started to disturb the other guests. One or two times the guards told the attendees not to be more than five persons at each table. Most of the time the guards just hovered just outside of the meeting boundaries, and the majority of them seemed intrigued rather than appalled by, for instance, the spectacle of young hackers showing off ("it fell out of a truck") a gutted but still complete public payphone (field notes, 2000).

Most meeting attendees were young, between 15-22 years, but the youngest hacker I meet was thirteen. Many hackers drop out from the hacker scene when they end their college education, which is 22 years (Sterling, 1992). There was a second group of attendees that appeared to be in the thirties. There were not many girls attending, a few appeared to be the girlfriend of the male hacker and had just come along (field notes 1999-2000).

The attendees would as the meeting progressed talk with others, and discuss technical issues and on occasions demonstrate their skills on equipment that they had brought with them. Others would bring books or magazines and start a discussion from a problem or a solution they had experienced (field notes, 1999-2000).

The status of the hacker was in a sense being determined by the demonstration of his expertise in technology and mastering of the terminology. A hacker would show his skills to a group of other hackers, all different in their own levels of expertise, but when he pulled off a "hack", a hacker who had equal or higher expertise would verify the validity of his "hack" by verbal approval. On one occasion a newcomer to the meetings was given the cellular phone of hacker group member then progressed to open it up, modify it, and then hand it back to the hacker. He then switched it on, looked at it for a few seconds, and then exclaimed "wow, you're our phone guy now!" The newcomer grinned, obviously proud, and received several congratulatory pats on his back by the other hacker group members (field notes, 2000).

The ways in which technological exploits are told is important, and carry the similar denotations as the performance of a hack. The story must carry structure, precision and creativity. The structure acts as a step-by-step set of instructions, the precision refers to using the correct terminology and the creativity marks the hack as unique. The cultural dynamics of the relationships between hackers derive from the consistency of the storytelling of the hack. The dissemination, whether verbal or textual, determines the status both for the recipient and the hacker. The recipient will either approve or disapprove of the story's validity, his reaction thereof will grant the hacker insight into his own status as a hacker. Did the recipient understand it and did he approve of it?

Around 8 pm the meeting at the Citicorp building would start to wind down, but some of the attendees would gather their gear and head downtown to Empire Szechuan Balcony, a Chinese restaurant, for the traditional post-meeting dinner[34].

The dinners were held in the second floor of the restaurant, in a very informal manner. What I found intriguing was the scramble for the best table seating. There was one large round table in the inner corner of the room, which seated about 5-10 people, and about five or six rectangular tables at the rest of the floor. Each time the hacker dinner guest were arriving, there were a considerable shuffling going about as people tried to get seats by the round table. Most of the old time regulars had their seats there, but at times foreign guests or pretty girls would be seated there. Me, the student anthropologist, had to observe the merriment from one of the rectangular tables at every dinner I attended.

Not that the rectangular tables were any less rich in anthropological data. The conversation focused on hacks or exploits, hacker lore and popular culture items such as Monty Python, Matrix or Star Wars movies. There was some political discourse, which could be perceived to be utterly leftist, had it not been for the fact that most hackers seemed to loathe the status of domestic politics, with typical "we're not in a democracy, its just a two-party system", "whoever wins, it will be no change of politics" and "the American public is to stupid to choose any different". The latest statement surprised me, but this appeared to be part of the elitist thinking prevalent of the hacker culture as suggested by Jordan and Taylor (1998).

When the dinner ended about ten pm, most people would head home, but a few attendees would gather together outside the restaurant and organize a visit to a pub, club or a private party. On my first meeting we headed to what was refereed to as the Club House, which turned out to be the desolated offices of "2600". It had for some time functioned as a meeting place for the New York hackers, but was at that time abandoned and it now only housed the http://www.2600.com web servers, huge quantities of computer hardware stocked away in every available corner, dusty office furniture and a hacker book library. Surrounded by skyscrapers plunging upwards the damp New York September night I found the scene hauntingly similar to Sebastian's apartment in "Blade Runner"(1982). Only the blimps floating overhead, buzzing adverts on their projector screens, were missing.

[34] Any explanation for having the dinner at a Chinese restaurant was not given but I have come across a historical reference emanating from the Stanford University in the early seventies. Apparently the Stanford hackers appreciated the late opening hours of the Chinese restaurant matching their own unorthodox working hours, the mysterious logical complexity of the Chinese menus which was similar to that of a computer instruction set, and that the food was both tasteful and spicy ("You're eating spicy food, and you cant help but talk loudly. As a result, ideas were passed on, and that explains the [Silicon] Valley") (Markoff, 1999)

The party had been progressing for some time at the time we had been arriving, and after being introduced around by Izaac, I mingled about trying to get an anthropological handle on the situation but the effects of jet lag kept muddling it. Finally I caved in to the overpowering sleepiness, crawled out and snuck into a cab heading back to the YMCA hostel.

The meetings seemed to progress on a scale of confidentiality, and it was obvious from my first attendance that the New York scene was one of increasing secrecy and exclusiveness and in fact represented a hierarchy based on subcultural knowledge. As the hackers meet at the meetings and later at the dinners, demonstrating technical knowledge mandated the hacker status, but as the social arenas became smaller and more exclusive, social capital in the form of social networks ensured confidential relationships to emerge. These confidential relationships I assume forms the basis hacker group formation in the New York scene.

Websites and Internet Relay Chat

Subcultural hacking knowledge was historically disseminated through underground leaflets such as the YIPL or TAP, before migrating to BBS's in the eighties and nineties (Walleij, 1998). Today the knowledge is distributed through underground ftp sites, web sites or through IRC channels. The ftp sites are online file listings that use an Internet communications text-only application for downloading or uploading files.

The web sites contain huge numbers of text and software files related to hacking and hacking techniques. The user accessibility of web sites is much higher than ftp sites or BBS's. The files are indexed for different usages as well as different skill levels and may also be found by typing in key words in one of the onsite search engines. One such web site is the http://www.altalavista.com web site (figure nr. 11). These types of web sites also includes discussion forum for a whole range of subjects.

These web sites often claim their content is IT security-based but at the same time may link searches for popular games or applications programs directly to serial numbers suppliers web sites. These latter illegal web sites enable users to use the supplied serial number on the pirated software and bypass the obligatory payment registration.

The IRC (acronym for Internet Relay Chat) are text-based only chat channels that serves as the main interaction area for dissemination of secret knowledge. Actual downloads or uploads of significant size or numbers do not happen there. The IRC networks are a meeting-place mostly (Norwegian informant interview, March 2003).

Figure 11 The homepage of http://www.astalavista.com

Distinction of Underground Computer Cultures

> Distinctions are never just assertions of equal difference; they usually entail some claim to authority and presume the inferiority of *others*.
>
> (Thornton, 1997:201)

The definition of what constitutes hacker culture differs between hackers, central institutions of power, the popular opinion and other underground computer user groups. The fields of power and the popular opinion define hackers as a deviant and criminal subculture while hackers consider themselves disseminators of secret knowledge and extollers of unlimited information access (Chandler, 1996). In addition, other underground computer users that use hacking methods also claim to be hackers. But these groups are denied a hacker status by hackers and are called crackers, pirates, script-kiddies and virus-writers, terms that has strong negative connotations among the hackers (Taylor, 1999). The question then arises, what is the causing effect or situation by which these groups are denied hacker status? During the analysis of my material I found it revealing to consider what hackers claim constitute their ethical guidelines, which in term determines the motivation of the hack. What determines if

you are categorised a hacker or not, is your motivation for hacking. For analytical purposes one has then to divorce the practice from the ideology, to differentiate the hack from the users motivation.

The hacking tools and descriptions constitute a diverse collection of technological knowledge that in it itself is not malignant towards computer security. It is the motivational use that determines its potential malignity[35]. Since motivation, from the hacker point of view, constitutes the difference between hackers and non-hackers, it forms the core element of hacker identity formation. Central in the formation of motivational guidelines are the hacker ethic.

Steven Levy distilled the Hacker Ethic out of the interviews he did during his research for his book "Hackers: Heroes of the Computer Underground" in 1984. The book version have since migrated into several other manifestations, but the central themes underscores the importance of sharing unlimited access to information, mistrust authority in any form and believing that computers could have a positive effect on your life. The hacker ethic evolved from US computer research environments in the early sixties:

> "Well the so-called hacker ethic is just something that's has been evolving […] taking bits and pieces from the M.I.T., from CALTECH and Carnegie Mellon […] and hang a tag on it calling it "computer ethics". Basically its "don't screw up!" […] if you can fix it, you try and fix it, otherwise just let the guy [in charge] know".
> (Cheshire Catalyst, fieldwork interview July 2000)

Many of my hacker informants refereed to the hacker ethic when they described the incentive for their own actions in contrast to those of other underground computer user groups that, from their viewpoint, utilized hacking tools for malignant purposes (field notes, 1999-2000).

Crackers

Crackers are an underground computer user groups that "cracks" into, using hacker methods and tools, computer system security or computer software for malicious purposes. Hackers referred to "crack" as a negative version of the "hack".

[35] There is though tools constructed that leaves little option but malignant action, such as credit card and computer software serial number generators, that literary only leaves the "push enter button" as the sole available option. But these are tools that are primary been constructed for cracking or computer software piracy purposes and I find it debatable whether they fall into the description hacker tools.

> To me cracking is more the realm of the acts of vandalism; most often acts of vandalism using tools that are created by others. There is no new technology, there is no new thought presented when cracking happens
>
> (Kashpureff, fieldwork interview spring 2000)

Computer Software Pirates

Pirates distribute cracked commercial computer software. "Warez" is what computer underground brands it. Pirates also use "cracking" methods to bypass the copyright protection software of the application and then distribute it either by swapping it with other pirates or selling it. This illicit trading network seems to have appeared in the early eighties with the commercial success and widespread dissemination of the home computers and computer software (Wallij, 1998). A Norwegian informant told me that in order to download the latest cracked computer games from American BBS's, they used stolen credit card to pay for the cross-continental phone bills[36]:

> This became a way of showing how you were ahead of the pack, and it meant that your status as a software pirate increased as you could show off the latest computer games.
>
> (Norwegian informant, discussion 2001)

During the nineties, the BBS's disappeared in favour of the Internet as the main distribution channel for pirated computer software (ibid).

Black hat, white hat and grey hat

These are generalizing terms used for computer user groups that ascribe to different motivation and ethical guidelines. It is normally used to stratify the level of legality and visibility among these groups with white hat being at the top. The black and white hat analogy derives from sixties television westerns where the bad guys usually had black cowboy hats, whereas the good guys had white ones (Raymond, 1998).

> Well, it's pretty much the difference between a malicious hacker and a real hacker. The white hat hacker is generally someone [who] is considered as a security expert and works for companies securing systems. […] Black hat hackers [are] generally someone who goes around breaking security. There are a lot of people who call themselves grey hat hackers, the L8pt being a case in points. They do a lot of consulting but at the same time they play around

[36] The pirates that used long-distance phone lines to connect to BBS's and download or upload pirated computer games were called "couriers" and they utilized phone phreaking techniques in order to do that (http://www.defacto2.net/monolog.cfm)

> in the grey areas that can't really be classified as white hat or black hat, it's just not that clear cut.
>
> (Mike Hudack, fieldwork interview, April 2000)

Black hat are malicious computer users, grey hat are the ones who use cracking and hacking tools but work for the "good" side i.e. computer security businesses. White hat works only in legal context and don't use hacker or cracker tools and usually are consulting security experts.

Script-kiddies

A "script kiddie" is a hacker derogatory term usually ascribed to adolescent boys that has gotten Internet access and that subsequently downloads hacking tools. Since the hacking tools have become successively user-friendly during the nineties, a "script-kiddie" may just have to "aim" it a target and "push the enter button". They call themselves hackers, but because they supposedly don't understand how hacking tools work in detail coupled with their defrayal of hacker ethics, they are denied hacker status. The "script-" refers to pre-programmed actions authored by someone else than the user. "Script-kiddies" are generally blamed for destructive and immature acts such as defacing websites:

> The script-kiddies are just children who like to be naughty […] you have a situation where the playground bully has come indoors and learned how to type. And, you know, all he wants to do is to go out and scratch discs, and dump cores and just … wreak havoc. Those guys are real pain. And there isn't a whole lot you can do to stop it.

(Cheshire Catalyst, fieldwork interview July 2000)

Practice

The practices the hackers, and the aforementioned underground computer group's categories use, may be divided into social practices and technological practices.

Social Practices: Social Engineering

To let people solicit information by posing as an authoritative person or to-be-trusted person. This practice stems from telemarketing where telemarketer focuses on the customer's weakness and build trust while still remaining concise and effective. Phone phreakers picked up on it, and it is now a common hacker practice performed over the telephone.

> My favourite technique has been calling up and saying 'Hi, how are you doing? We just had a bit of an intrusion [and] we need to change our passwords. We would prefer it [if] you would

change your password through us, we're at the facility right now. If you change your password through your computer it's a chance that it'll be intercepted by the people who still may be in the network. Give me your current password and the password you wish to use in the future, that'll be great.' Nine times out of ten they'll give you the password and they'll give you the new password. You'll change the password to their new password and there you go, you have access. Incidentally this is not me, I've never done this!

(Mike Hudack, fieldwork interview)

Social Practices: Dumpster Diving

This is a practice to retrieve un-shredded garbage from corporate refuse dumps. It is still a fairly common occurrence, since many don't shred their garbage (Walleij, 1998).

Dumpster diving is looking through paper-garbage; not real garbage but you know papers, discarded papers, for any kind of information. Dumpster diving is the main way people get into systems and hackers get into systems. You'll find a discarded piece of paper with a username and a password on it, and that'll get you in

(Mike Hudack, fieldwork interview)

Technological Practices: An Overview

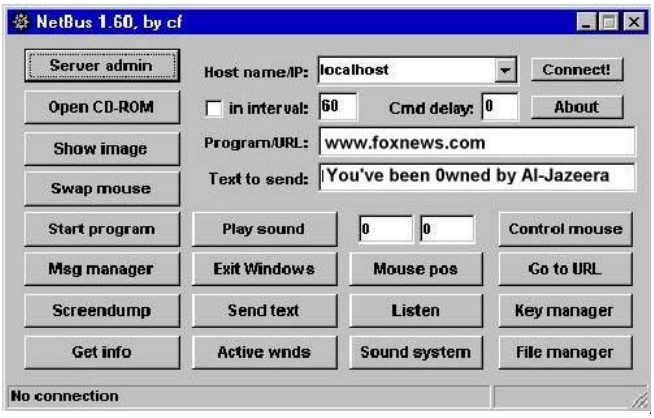

Figure 12 NetBus 1.60 one of the most popular Trojan programs. Note the number and range of actions the user can remotely control on the victims computer

Hacker use a wide variety of tools to access computer networks. The sheer number of programs and "how-to" text files makes it impossible to give a detailed overview within the context of this study. I will instead give a short description of some of the basic techniques and tools that hackers and other underground computer users employ[37]. The first step usually involves network sniffers or port scanners that enable the hacker to determine the type of operating system and running applications on the remote computer. All operating systems and applications contain bugs, or programming errors, ranging from hardly noticeable eccentricities to more severe errors that may pertain to

[37] My own level of technical expertise is intermediary to say the least, which made it necessary to confer with my Norwegian informants in order to be given an introduction of the most commonly used hacker tools.

serious security issues. After running sniffer and scanner programs he can easily look up the security bugs of that particular operating system or application. Using an exploit that attacks that particular vulnerability he then may for instance install a Trojan[38], such as the Netbus program, install it at the remote computer, and later access the and control it (see figure 11). Other programs are snoopers, applications that capture password or other data as it pass through the network or the computer and root kits[39] which is a program, or collections of program, that conceals the fact that the computer has been taken over.

On The Presence of Politics

When I began my fieldwork one of my key suppositions was whether there was presence of politics within the hacker culture. A majority of the hackers that I meet did not appear to brandish any political agenda, apart from a detached political interest that seemed to stem from the elitist thinking prevalent among my hacker informants. Yet I found political dissent to appear on two levels, first on individual level and secondly, at an organized level. On an individual level it became apparent that several social entrepreneurs within the New York scene were actively embracing and pursuing a politicalization of hacker culture. These individuals were older hackers that had experience and relations with the phreaking and hacking culture of the seventies. Their social networks appeared to extend beyond hackers, often mobilising dissent in other computer user groups, such as when the New York Linux user group appeared at the anti-MPAA rally (see later) outside the courthouse in July 2000. On the organized level it appeared where the hackers could meet and they assumed to be in control over the media (be it their own websites or press conferences), and in such circumstances there was a diverse range of techno-political dissent, ranging from handing out flyers, Internet radio shows to huge hacker conferences.

Eric Corley, a freelance reporter that goes by the pseudonym Emmanuel Goldstein, began publishing ”2600:The Hackers Quarterly” in 1984 following the collapse of “TAP” magazine. His pseudonym derives from the diffuse public enemy in George Orwell’s book “1984” that the dictatorship Oceania defines it perpetual war against. Today Eric still runs the “2600” as well as hosting “Off The Hook”, a weekly radio show in New York City. His considerably social capital, the extent of his social networks, enables him to organize large

[38] “A Trojan […] is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage”, taken from the searchnetworking.techtarget.com website.
[39] For looking up some of the terminologies I used the Wikipedia Free Encyclopedia, which is online, and is free! Available at: http://www.wikipedia.org

hacker conferences as well running a hacker magazine. In addition he appears regularly in the national media and is a known figure within the New York political liberalist milieu, "being best described and understood as a dissident" (Sterling, 1992: 61). When he attended Long Island's State University of New York in the 1970s he became involved with the local college radio station. After gaining an interest in electronics he came into contact with the publishers of TAP and became a "self-described techno-rat" (ibid: 61). Both in his magazine and radio show the Yippie tradition is continued, expressed in sarcastic, ironic or paradoxical terms. The articles and radio shows still retains the ideals of technical power and knowledge belonging to the individual that acquires it and that measures that hides or denies access should be removed (ibid).

During the beginning of my fieldwork I came in contact with Emmanuel through Izaac, and had frequent "sit-ins" at the studio where his radio show is broadcast from each Tuesday. WBAI is a non-profit community radio station in New York City that has been operating[40] since 1960, with "Off the Hook" broadcasting since October 6'th 1988. Located at Wall Street, a mere quarter's throw away from the New York Stock Exchange, WBAI carry a programming schedule that within the American political context probably would be considered leftist-liberal. Emmanuel's presence was much more evident in the radio show than at the monthly meetings in the Citicorp building, but this most likely came as a consequence of his long experience as a journalist. After the highly publicized Denial of Service[41] attacks in early 2000, which forced several high-profile commercial web-sites offline, hackers were generally blamed for the attacks, and in the following radio show, Emmanuel complained:

> But how do you know hackers did it? I mean somebody going out there and turning on a … you know a OC-12 and aiming it at somebody […] bringing them down to their knees and taking them off the net entirely, that turns them into a hacker just because they do that? […] You know anybody with the access could have done this and not everyone with access is hacker!
>
> ("Off the Hook" transcript February 8'Th, 2000)

[40] WBAI broadcasts at 99.5 FM and is available as an live audio stream at http://www.2600.com/wbai/

[41] "On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users." Definition from searchnetworking.techtarget.com website.

Figure 13 Protesting the MPAA lawsuit outside the Federal Court, July 17'Th 2000,New York City.

Two months before the DoS attacks, Emmanuel was sued by the Motion Picture Association of America (MPAA) for making the DeCSS code available on his website. DVD's are encrypted with CSS (Contest Scrambling System), which makes copying impossible. In late 1999, a group of European hackers reversed-engineered[42] a commercial software DVD player and extracted the CSS code. With this they made DeCSS, which is a free DVD decoder that enables people to make their own DVD software players as well as copying the content of a DVD. Jon Johansen, a Norwegian teenager, began distributing the DeCSS code on his web page and it quickly spread throughout the Internet. MPAA followed suit by getting court orders that shut down web sites or in Emmanuel's case, brought him to court. In the months before the trial in August 2000, "2600" mobilized their networks across the globe to demonstrate against the lawsuit and MPAA's crusade against DeCSS distribution. Eventually "2600" lost to MPAA in August 2000, and had to remove all their links to web sites that published the DeCSS code. They though still retained the right to type the web site addresses, i.e. removing the actual hyperlink connection, in effect still linking to the aforementioned web sites. The "2600" versus MPAA trial were the focus of many of the speeches and panels at the largest hacker gathering in New York, the H2K[43] conference. It took place 14-16 July 2000 at the Pennsylvania Hotel in New York City, and had more than 2300 attendees from around the world. Hope2000[44] was the third in a series of conferences that had been arranged and sponsored by "2600:The Hackers Quarterly" and has generally been viewed as one of the most important hacker conferences in the world. The other large hacker conference in the USA is the annual DEFCON conference in Las Vegas, which is considered more of a recruitment and job opportunity place than the HOPE conferences (field notes).

---

[42] "Reverse engineering is taking apart an object to see how it works in order to duplicate or enhance the object. It's a practice taken from older industries that is now frequently used on computer hardware and software. Software reverse engineering involves reversing a program's machine code (the string of 0s and 1s that are sent to the logic processor) back into the source code that it was written in, using program language statements." Definition cited from whatis.techtarget.com website.

[43] H2K, or HOPE2000 is an abbreviation for Hackers On Planet Earth 2000

[44] The conference started with Hope in 1994, celebrating "2600"'s ten year anniversary, continued with Beyond Hope in 1997 followed by H2K in 2000 and H2K2 in 2002.

Secrets of the DNC/RNC
Friday, 11 am
Paris Suite
For the first time, a HOPE conference is taking place just prior to the two major national political conventions. As you can guess, the kinds of security precautions and methods of utilizing technology are subjects that are of great interest to hackers. Learn a thing or two about how the Secret Service plans to control things in Philadelphia and Los Angeles - and how they use and misuse technology. Yes, we've got the frequencies.

The Hacker's Code
Saturday, 1 pm
Paris Suite
This session will ask audience members to work together on a "Hacker's Code." Is it possible to have a shared code of ethics? Is it desirable? Will this help distinguish hackers from script kiddies from criminals? We will look at some possible examples, including the Hacker's Manifesto, Hippocratic Oath, The Three Laws of Robotics, and others.

Speaker: Greg Newby

Cyber Civil Disobedience
Friday, 4 pm
Paris Suite
Discusses the roots of civil disobedience from the Boston Tea Party to Martin Luther King and how hackers are follow in these footsteps. Beginning with the ideal of hacking as a public service to improve security on the early Internet to more contemporary examples, hackers around the world have used their skills to promote social good. In Bosnia, East Timor, and even the United States hackers have put the best traditions of free speech to work online: to draw attention to human rights abuses, criticize oppressive laws, and fight injustice. This presentation documents the history of hacking to encourage social change and examines the question: "If hacking has proven a non-violent and effective form of civil disobedience, is it protected by the First Amendment?"

Hosted by Dan Orr.

Figure 14 H2K conference speeches and panels (excerpts)

H2K covered a number of themes related to hacker issues and many of them appeared to be of a political nature, as well featuring mock trials, numerous discussion panels and speeches in advance of the MPAA lawsuit. I counted a total of 52 planned speeches or panels during the conference, of which I graded forty-two percent, or 22, that brought up political issues (see figure 11).

One informant told me the reason for New York conference being perceived as more political active than other hacker conferences was due to it being held in New York which was an activist centre as well as being host to the headquarters of the major national and international news organizations:

> Because it's a communication capital, we get all these political activists, and they happen to come to the technology convention of ours. They get up and they bring their politics into our technical sessions.
> (Cheshire Catalyst, fieldwork interview July 2000)

The lawsuit, the trial and final verdict demonstrates the ongoing struggle to define the property laws in light of the advent of the Internet and its ability to disseminate proprietary knowledge beyond juridical boundaries in endless copies. This is appears to be part of a

struggle to define access to knowledge that is contested by the fields of power and the hackers. This is something I will return to later in my study.

Discussion

Cultural Capital and Subcultural Capital

> I don't know how it became so popular to call oneself a hacker, but I can tell you there are a lot of people who call themselves hackers who really aren't.
> (Mike Hudack, fieldwork interview spring 2000)

Sarah Thornton[45] did a study on club cultures in nineties England, basing her analysis of their values and social and cultural hierarchies on the concepts of Pierre Bourdieu's[46], with special regards to the links between taste and social structure (Thornton, 1995). Bourdieu explored cultural and economic capital as the prime causes in determining the social status of a person, being acquired through upbringing (for example your accent) and education (for example your university degree). It connects social hierarchies with cultural ones, with people's taste being the foremost indicator of class (Thornton, 1997). Cultural capital carries a wide meaning in Bourdieus work including material things as well as more abstract notions such as status and authority, and cultural capital (cultural taste and what people buy for instance). Cultural capital are the social relations within an exchange system, including goods, material and symbolic, that are presented as rare and desired items within the given social formation (Harker et al 1990). Cultural capital differs from economic capital, and usually a high level of cultural capital correlates with a high level of economic capital. Mocking comments on the 'new rich' - be it American oil billionaires or Russian mobsters - illustrate the conflict inherent when this is not the case. Such a conflict is revealed by Bourdieu's multi-dimensional matrix of social structure which Thornton find more relevant than the traditional vertical models of social structure. Bourdieu also includes a third category, social capital, which is not related to what you own or know, but who you know and vice versa. Particular social relations bestow status, which sometimes takes precedence over cultural or economic capital, for example the social networks of boarding school or private semi-secret clubs.

---

[45] Thornton's position derives from the subcultural studies at The Birmingham Centre for Contemporary Cultural Studies, which includes Dick Hebdide's heavily influential work "Subculture, the Meaning of Style". His subjects were London working-class subcultures, and his work emphasized the importance of subcultural style, the subcultural oppression and economic disenfranchisement by the hegemony and the acknowledgement of subcultural ethnicity (Thornton, 1997).

[46] Bourdieu's writing may appear to be 'vociferous indignation' (Wacquants, 1993 in Webb et al, 1990:2) conducted in convoluted French, but his great strength is in crossing and utilizing crossdisciplinary boundaries employing research from a variety of disciplines such as cultural anthropology, philosophy and art studies. His theories have shown to be viable in many different cultural contexts beyond the French and Algerian settings, with symbolic capital, cultural capital and cultural fields being redistributed differently consequently (Bourdieu, 1998).

Antonio Gramsci defined hegemony as a situation where domination by one class over another is achieved by political and ideological means. The dominance is achieved not through force, but through the consent of the other groups, who associates themselves with the moral and intellectual leadership (Abercrombie et al, 1994). Today the term has no single definition of hegemony, but prevalent among all the differing variants the notion of domination is present. One may instead consider hegemony as a discourse on the dominant and the dominated, and how dominating and dominated groups operates and affect the entire social field: "Instead it [hegemony] sees the relations of domination and subordination, in their forms as practical consciousness, as in effect a saturation of the whole process of living – not only of political and economic activity, nor only of manifest social activity, but of the whole substance of lived identities and relationships, to such a depth that the pressures and limits of what can ultimately be seen as a specific economic, political, and cultural system seem to most of us the pressures and limits of simple experience and common sense" (Williams, 1977:110). I assume that in order to understand hacker culture as a subcultural group which is embedded within a hegemony means considering subtle and overt power relations at play both within and outside the social group. As I have tried to show in the preceding empirical material the struggle between an overarching, dominant culture and a subversive, counter- /subculture is manifested as an attempt to redefine knowledge distribution that power hierarchies of both cultures adhere to. In Bourdiean terms, power is described as how individuals and institutions of dominant fields (governmental or economic for instance) relate to one another and the entire social field. Fields of power[47] are the configuration of capital that 'makes things happen', resources such as social networks, and personal or institutional status for instance. Bourdieu says that the power comes from the relationship to other dominant fields and its position within this field of power (Webb et al, 1990). These power relations are also central in the hacker identity formation process, defining the social groups outside the hacker community as well as the hierarchies within it. The hacker dichotomies and categories arise from conflict-laden relations with other underground computer users as well as governmental and corporate entities.

[47] Inhabiting these fields of power are the fields that dominate other fields: government, banks, media, universities, the military and so on. A bank for instance is located within the economic field and is the primary institution within that field as it regulates the economy through a number of resources and activities (interest and currency rates and the cash flow of the bank for instance), and it is able to 'make things happen' because it has the sort of capital that allow it to do so. But the bank cannot 'make things happen' alone. It must relate to the other dominant fields as well; such as the government will allows it to be a bank, or to the media that reports on its decisions (Webb et al, 1990).

As mentioned earlier in my text, Sarah Thornton do not want to overemphasize the role of the dominant ideology in relation to the subculture itself, but seek to investigate the "subtle relations of power at play within it" (Thornton, 1995:15). She wishes to explore how subcultural ideologies let youth imagine their own and other social groups as well as how the members of the subculture define themselves in relation to the mainstream (ibid, 1997). The subcultural ideologies make meaning in the service of power, "however modest these powers be" (201). She base her analysis of British club cultures on cultural capital, and sees club cultures as 'taste cultures', subcultures where members gather on their shared taste in music, media and "preference for people with similar taste to themselves" (Thornton 1997: 200). She coins the term subcultural capital as being central in the creation and maintenance of the social boundaries and internal hierarchies of sub cultures. "Just as books and painting display cultural capital in the family, so subcultural capital is objectified in the forms of fashionable haircuts and carefully assembled records collections" (ibid: 202), or embodied as 'being in the know', using the correct slang and performing on the dance-floor as if you haven't done anything but clubbing in your life. Subcultural capital confers status on its owner in the eyes of the relevant beholder. Thornton use an example in the form of a subcultural gaze upon stereotypes of mainstream the poor girls Sharon and Tracy, who happen to be "weekend-clubbers", and who are described rather derogatively as 'dancing around their handbags'. They represent the unhip and unsophisticated in the eyes of the clubbers, the mainstream, that attends clubs for dating and not listening to music. Their handbags are symbols "of the social and financial shackles of the housewife" (Thornton, 1995:101), associated with mature womanhood or someone pretending to be.

The question then arises if the term subcultural capital is viable in an analytical perspective on the hacker subculture with particular regards to internal hierarchies and group boundaries. In Thornton's work the clubbers expressed their subcultural capital mainly embodied and objectified. The objectified subcultural capital was expressed in cool haircuts and clever record collections. In its embodied state it was talking, walking and dancing the proper club semantics, but at the same time not overdoing it, being "in the know". In regards to my empirical material some parallels to Thornton's work appears, but in relation to objectified subcultural capital it seems at first to negate the denotation of Thornton theory. Hackers don't dress to be cool, they dresses are supposed to be useful. Indeed if one is looking for an aesthetical dress code for hackers, what would be striking is its absence. In regards to clothes at least, hackers prefer functionality to aesthetics. Clothes are meant to be functional, comfortable and demand little or no maintenance. Among the young hackers I

meet, a few dressed streetwise, but this was nothing particular different from the general trend among their age group. Most hackers dressed in jeans and sweaters, nothing flashy or trendy. Haircuts, as clothes, were quite functional, with little or no emphasis on signalling symbolic capital. It was a distinct lack of style. Yet adhering to a functionalistic dress code is a sort of style, and even if most hackers vehemently claim dress functionality is a non-style, it's still an important part of hacker identity[48]. And more importantly, it is recognized as an aspect of hacker identity by the outside culture. After the Columbine shootings in 1999, www.Slashdot.org (a website catering to 'nerd' news) asked its readers of accounts at their high school following the tragedy. The media exasperated a negative image of hackers with personal websites, role-playing games and "anti-social" behaviour becoming part of a nationwide profile of potential mass murderers. Anti-style beaconed danger, as the Slashdot readers experienced, with parents suggesting their offspring to become more mainstream, attend sports and "get a girlfriend" (Katz, 1999).

Beyond the lack of any stylistic common denominator in terms of dress sense, there was an interesting tendency to carry technical tools on person, from Swiss army knifes to advanced telephone engineering devices. These tools appeared to attribute to the display of technical knowledge and hacker status. In addition to being used when technical problem situations arose, they functioned as a cultural signal device since the usage demanded a skilled and attentive user especially in regards to more advanced tools, The media image of hackers includes particulars that I did not observe during my fieldwork; such as mirrored sunglasses, roller blades or skateboards. One hacker exclaimed horrified on the notion of roller blading hackers in the film "Hackers" (1995); "have you ever seen a hacker sweat?"

The tendency to favour functionality may even extend to hacker semantics, as the frequent use of words such as "mumble", "groan" and "sigh" in a hacker conversation may represent a tendency to migrate the grammatical meaning of text-based communication in electronic media to the real world (Raymond, 1998).

I consider the embodied state of hacker subcultural capital as being information. A central tenet of hacker culture is the free access and distribution of information. Hacker culture both through the cultural dynamics of identity formation and its historical tradition

[48] The spectacular nature of style as it is noted by Hebdige, and by extension Thornton, is one of the main aspects of subcultural communication of group identity. With respect to the hacker non-style one might consider a transformation of the spectacular subcultural style as such. Paul Willis notes that the early subcultures of the 1950's and 1960's foresaw the contemporary situation by defining themselves early on and gain their own spectacle from finding style and identity outside or against work and working ethos. The idea of a "spectacular subculture [now] is strictly impossible because all style and taste cultures, to some degree or another, express something of a general trend to find and make identity outside the realm of work" (Willis, 1990:16).

puts a premium on secret knowledge, the kind of information that is locked away and not easily available and beyond a mainstream curriculum. This information was previously published in underground leaflets such as the YIPL or TAP, and was transformed into informational currency by the diffusion of BBS's in the eighties and nineties. This knowledge, which now is available at hacker web sites as well as being traded on Internet chat channels, could be considered the objectified form of subcultural capital. With this kind of knowledge your status as hacker is defined within the hacker community. The authenticity of being a hacker must be confirmed beyond his technical ability. Technical semantics acts as subcultural gate keeping, entrance is granted through the display of technical terms and exploits. By hacking the cellular phone of a hacker group member, the newbie hacker is granted status and acceptance into a hacker group; "wow, you're our phone guy!" Beyond the display of technical prowess, embodied subcultural capital emphasises the knowledge of confidential social networks, the ones that define a hacker merely beyond a technically able person. With this knowledge, this form of 'being in the know', hackers may form groups and operate together ensuring mutual anonymity as well as acknowledging each other's abilities. Yet the hacker emphasis on the free access information

All this does in effect paradoxically illustrate the contradiction by emphasising free and unlimited access to information, while simultaneously embracing and enforcing its stratified layers of secrecy and hierarchies of secret subcultural knowledge.

Media Relations:

A critical difference between Sarah Thornton's subcultural capital and Bourdieus cultural capital is the role of the media. Thornton sees in Bourdieu's works an absence of the role of the media, except with film and newspapers being symbolic goods or marker of distinction in relation to cultural capital. She sees media as a "primary factor in the circulation" of subcultural capital (Thornton, 1997:203), and finds it impossible to understand the distinction of youth subculture without investigating media consumption. The media serves to define and distribute cultural knowledge. The difference between hot and not, the highs and lows of subcultural capital, correlates with media coverage, creation and exposure (ibid). Negative media coverage is, even if its looked upon with disdain, anticipated and aspired to, while "positive tabloid coverage, on the other hand, is the subcultural kiss of death" (Thornton, 1995:135) The "kiss of death" subsumes their taste culture down into the cesspool of mainstream, apparently letting all the Sharon and Tracy's of the world into the

echelons of the cool and distinct. Yet Thornton points out that even though social cultural studies has tended to depict the youth cultures as victims of this media stigmatisation, its actually being pursued by subculture industries. "Moral panics" are the carefully wrought cloth of *hype*, targeting the youth market. The image of the drugged sex-crazed rocker[49] ensures considerably media attention while at the same time preventing the notion of being a "sell-out" (ibid).

As we have seen earlier, the popular image of the hacker is the result of a mediated relationship between the hackers and the media (Chandler, 1996). The early eighties portrayed hackers as the heroes of the new digital underground (Levy, 1984), using rhetoric that hailed the apparent groundbreaking economical entrepreneurialism of computer "wiz-kids" and welcomed the rugged individualism and digital freedom of "hackers" it being reminiscent of American cultural values (Chandler, 1996). But in the latter part of the eighties and early nineties hacking became synonymous with criminal activities (Peneberg, 1999). This change of media attitude came about as an increased public attention to computer crime in general and due to the widespread adoption of personal computers in people's homes. Today hackers are associated with criminals and anti-social behaviour, with an emphasis on subversive, dangerous and damaging activities. Terrorists are no longer confined to foreign countries, but he may live upstairs in the attic under the guise of a teenager (Kovacich, 1999).

The difference between Thornton's clubbers and my hackers as I see it are that the repercussions of being caught and prosecuted are much more severe than the clubbers face if arrested for, for instance, substance abuse. A computer hacker may serve years in prison for what the courts decide is a grave electronic crime, but its decision probably stems from both a fear of - and inability to understand – technology. As such, the hackers have every interest in maintaining a positive media image, as they see themselves being targeted for a societal misunderstanding and criminal branding of hackers. Kevin Mitnick was prosecuted and sentenced to more than five years on charges of wire fraud and illegal possession of computer files. The book "Takedown" by computer security consultant Tsutomu Shimomura was co-authored with the New York Times journalist John Markoff who, in advance, had written numerous scathing newspaper articles that warranted Mitnick's role as a super-villain (Wright, 1996). Shortly after his prison release, Mitnick angrily accused Markoff of remodelling the facts to fit the story:

[49] In my opinion, Marilyn Manson is an example of such; with such sales figures (his latest album, "The Golden Age Of Grotesque" debuted first place on the US Billboard charts, see http://www.billboard.com and album charts for May 31'st 2003) he can hardly be labeled an underground artist, yet he loudly advocates such an image.

> John Markoff was successful in creating a character that he could, you know, write a book about […] what he was trying to do was create a western […] me being the bad guy and Shimomura being the good guy […] basically he ruined my life, anyone who has the power to write a fictional story that is accepted as truth by the world and the front page of the New York Times has an enormous amount of power to destroy someone's life.
> (Kevin Mitnick, guest appearance on "OffTheHook", February 8'Th 2000)

Douglas Thomas wonders if Kevin Mitnick and Kevin Poulsen were circumscribed by the term "hacker" and thus prosecuted and sentenced not for what they did, but what the court feared they could do[50] (2002). Gerald Kovacich puts it bluntly; " Mitnick may have been a pain in the ass, but he was no Capone, although he was treated as if he was that dangerous" (1999: 574).

Thornton's clubbers viewed the mainstream media as being a part of what constituted the hegemony and the acceptance, or positive media coverage, of club culture constituted a subcultural "kiss of death" (Thornton, 1995). Hackers see most large news organizations as pursuing a sensationalist policy directly related to commercial interests, and showing little interest in portraying hacker viewpoints. On several occasions the hacking community have been trying to reiterate their seemingly tarnished image by aiding media organizations in the forms of exclusive interviews and access. The most infamous, and heavily quoted, example among hackers I meet was MTV's attempt to describe hacker culture. The MTV "documentary" showed a world of troubled teens, most of whom had problems both with the law and drugs, with the tag-line running: "never before have people so young had so much potential power to disrupt the systems we all rely on", inciting the following furious reply on a notable hacker website:

> So the lessons to be learned here are several. The most important being: DON'T TRUST THE MEDIA! Especially the slick and trendy media. They're not interested in the story but rather in being cool and accepted in the industry. If you don't know how to deal with them, they will screw you over and as a result screw over those people you're supposedly speaking on behalf of.
> (Emmanuel Goldstein, http://www.2600.com/news/view/article/350)

[50] The post 9/11 Anti-Terrorism Act (ATA) could make violations of the Computer Fraud and Abuse Act as "federal terrorism offences", meaning that offenders could face life in prison. 2600 news story from: http://www.2600.com/news/view/article/726

MTV's inability to render a realistic documentary portrayal of hackers stems more from its wholehearted commercial embracement of *style*, but the show nevertheless showed both the frustrations of hackers trying to get "the right image" out to the people and the hackers symbiotic existence with the media. At this point, Thornton's subcultural media relation seems not to diverge from my material. Hacker identity formation is to a certain extent shaped by its relation to both news and fictitious media. The news media constantly updates the "bad boy" image of hackers in the media ensuring a steady stream of youths that flock to be part of the underground, and for sure, the MTV documentary caused the number of "2600" meetings attendees to rise from forty to more than seventy three weeks later on (field notes, 1999). Also at that particular meeting a couple of TV crews, brought on by the surge of interest, repeated the media exposure process. When I started shooting my interviews, it was impossible to have my informant's recount their own exploits since that meant potential juridical repercussions. Hackers, who told about hacking, told about other hackers. When questioned directly about their hacking activities, my informants wouldn't answer. One in particular kept saying "I can't speak to that issue" whenever I asked him. I gather the camera savvy ness epitomized by most of my informants, stems from a prolonged relationship with the media. Many of them had pages long curriculum vitae of TV, radio and newspaper interviews on their homepages. My informants eventually succumbed to my editorials needs, and recounted, in their opinion, good hacking stories. But these were stories that others had done and in addition my informants didn't reveal any names except for their handles.

Figure 15 The hero "Neo". "Matrix", 1999

In fictive narratives of hackers both in film and TV, they are generally portrayed as naïve, socially handicapped but good-hearted computer nerds or, at the opposite end of the spectrum, as dangerous anonymous anarchistic cyber burglars. In "Matrix", the hero was a hacker who at the end of the film made the ultimate hack: changing reality itself by destroying the alien bureaucratic entity that controlled it. In "Sneakers" (1992), the hackers were a group of tech-savvy dissident liberals that saved the world from an Orwellian dictatorship. The fictitious - and news media - material constitute a substantial part of hacker identity. The many references to the "Matrix" (1999) or "War Games" (1983) movies and the adoption of names, terminologies and cosmology taken from these films and many others undoubtedly came about as an admiration and appreciation of the fictitious hacker depictions.

Notable the widespread use of the handle "Neo", Keanu Reeves character in the "Matrix" (field notes, 1999-2000).

The media production of hackers themselves merits a closer look. Hacker fanzines and web pages are physically separate from the hegemony culture and its production and dissemination are not limited by economical or practical concerns. The huge number and range of hacker websites confesses to their ability to understand the importance of media to the degree that they create and maintain their own media. Which can disseminate hacker knowledge and culture without the meddling and mediation of a hegemonic media and culture. Hebdige's Punks produced photocopied fanzines which had a limited distribution, often marred by errors and typographic anomalism. While they probably could become more sophisticated and accessible, they didn't, as their possibilities to do so were limited. Hacker websites and fanzines don't have to worry about printing or distribution costs, which are negligible to say the least.

Gender Differences:

Why are there no girl hackers? Thornton points to the fact that the most delineated aspect of subcultural capital is gender. One of the reasons for this marked difference in subcultural membership could be that girls invest more of their time and identity in doing well at school, while boys pursue leisure activities (Thornton, 1995). In such a sense, the hacker subcultural capital would define itself as extra-curricular knowledge, one that is not acquired at school. Thus, boys might be more likely to be drawn to the hacker culture due to its non-curricular structure of dissemination and learning. In my experience, there are very few girl hackers, but those who do adhere to the same subcultural economy, adopting the embodied non-style by not using any makeup or brandishing any particular hairdos. Some girls that are not hackers but still attend the meetings and conventions seem to be drawn to the hacker culture due to its underground affiliations, and a hacker informant told me that they were called - very derogatively - "scene sluts" which I find as an example of the prevalent misogyny among hackers pointed out by Jordan and Taylor (1998). Notable portions of these girls were "gothic girls" (field notes, 1999-2000). Goth is a subculture – originally starting as an element of punk rock - that emphasises black clothing, body piercing and bondage gear. Goth's claim they are drawn to subjects such as death, Victorian and medieval history, and being attracted to a particular musical style that is a quite dark kind of rock music[51]. They may

[51] "Historically, Gothic rock started with Siouxsie and the Banshees, The Cure, Joy Division, & Bauhaus. These bands were contemporaries of such early punk bands as The Sex Pistols, The Clash, The Buzzcocks and Generation X in the UK in 1977 – 1979 […] Goth rock is at its most basic level a combination of punk rock &

be drawn to the hacker culture since hacker has such a strong underground and counter-culture connotations in the popular culture.

A note on dominant versus subversive culture

The CCCS school views subcultures as a result of class stratification. Subculture members saw themselves and their culture as response to the dominant culture and its inherent contradictions. For the dominant culture, subculture meant working-class. But most hackers are middle-class and above, with high costs of pursuing the technology that maintains the lead of subcultural knowledge gathering.

> About, I guess, four or five years ago I got my first computer. It was a used 486sx 33. Didn't even come with a cd-rom drive, I had a little 13 inch monitor. I paid about $800 for it.
> (Mike Hudack, fieldwork interview spring 2000)

The very first generations of hackers was even more so an upper-class phenomenon with members attending the most prestige universities in the US such as MIT or Carnegie Mellon. Even though the hackers might suffer the scrutiny of high-school principals and being tormented by the sport jocks, their experience of marginalization is slim, as they tend to earn very high salaries early in their workplace experience.

> I own IBM PC's, Apple's, Commodore's; the Vic, the C-64, the Commodore 128. I owned VAX's; I owned Next computers, [I've] owned all kinds of computers, vintage computers, different kind of operating systems, everything under the sun.
> (Spudz, fieldwork interview, July 2000)

Criticism has been levelled against defining the hackers as a political and social counterculture. Hayes notes that hackers appear to be white, upper middle-class adolescents, whose computer has been bought, subsidized or tolerated by parents (1989). They don't have any political motivation beyond voicing disdain against the authorities and bureaucracies that stand in their way when they are digitally exploring. They appear as an "alienated shopping culture deprived of purchasing opportunities" (Ross, 1990: 26)

---

new wave. Between 1979-1985 it was variously known as post-punk , alternative, & new wave". Taken from the www.wikipedia.org online encyclopedia.

On the other hand Andrew Ross notes that previous studies of youth cultures have shown that the political meaning of cultural resistance is difficult to interpret. Such meanings are either highly coded or expressed through the language of media or private peers or even customized consumer styles, unorthodox leisure patterns and categories of subcultural knowledge and behaviour that appears to have no fixed or inherent political content. Indeed, if hackers appear to be without a "cause", they are not the first youth culture do so (ibid).

Conclusion

The term "Big Brother" originates from George Orwell's "1984" (1950), an account of Oceania, a future information dictatorship where everything is monitored and everybody is subject to incessant propaganda. It has become a general term for our societal fear of a possible dystopian future, in which there is no chance to escape the clutches of the State. But as 1984 came and went in real life, one wonders if Orwell was bound up by the context of his world with its Italian fascism, Soviet Stalinism and the Spanish Civil War and did not contemplate a future where consumerism have foregone totalitarianism[52]. Orwell was probably aware of authoritarian tendencies in our own, western capitalistic societies, but what he probably didn't foresee, was the application of totalitarian surveillance in democratic societies (Lyon, 1984). The conception - and widespread usage - of the Internet brought upon the exercisers of general surveillance of the citizenry a technological upheaval as they saw their entire policing machinery, developed throughout the Cold War; perform inadequately in relation to the new reality facing them on the Internet. Recently state instigated panoptical technological devices begin to appear, in order to reclaim control and authority, signalling a tendency toward the more subtle applications of discipline and surveillance.

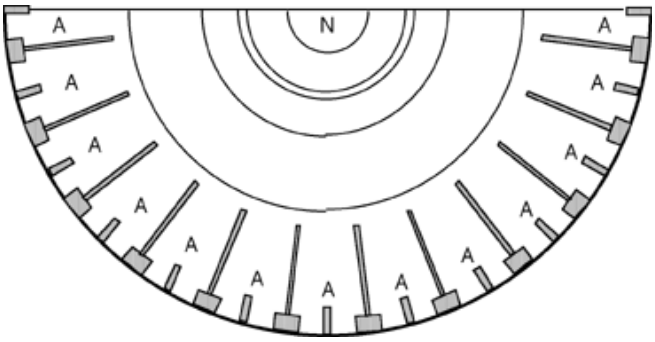

Figure 16 Bentham's Panopticon. N = the guardian, A = the individual prison cells (Bentham, 1995).

In its original shape, the Panoptican was a ring-shaped building, with a tower standing in the centre that had windows that faced the inner side of the ring. Inside the ring were cells, each having two windows with one facing out of the ring, and the other facing inwards, with carefully constructed blinds to ensure the prisoner could not see out, towards the tower. The tower housed the guard, who

[52] Lyons considers the modern social order to consist of two classes; the consumers and the underclass. The consumers experience the panoptic power as pleasurable, assisting them in their desires for consuming goods, while the unskilled underclass is isolated and encircled by it. Denied credit card, checks and even employment due to lack of information, they are unable to partake in the consumer class behavior. But even the consumer class may be manipulated by panoptic power in the form of marketing: in which carefully constructed adverts attempts to change the behavior of consumers (Lyons, 1984). Modern marketing stems from the behaviorism of John. B. Watson, who abandoned psychology and joined the Walter Thompson advertising company in 1921. He saw people as machines, and believed their buying behavior could be predicted and controlled, with ad messages conveying desirable messages, so that the consumer would feel dissatisfied with the products they owned (Schultz & Schultz, 1992).

could observe each cell without being seen. Conceived by Jeremy Bentham[53] in 1791, it was originally an architectural – as well as an reformism - device to centralise surveillance of prisoners and ensuring discipline through a prisoner's[54] uncertainty of knowing if he was being watched or not (Bentham, 1995). Foucault saw in the Panopticon (a greek-based neologism that meant "all-seeing-place") how surveillance was brought to bear on the individual himself, and in which older and more violent, as well as costly, ways of surveillance were replaced by a "subtle, calculated technology of subjection" (1977:221). In the Panopticon Foucault saw our modern society, with panoptic power being embedded in every relation, and in which every action is visible for the invisible inspector. Compliance emerges from uncertainty of being observed or not (ibid).

Internet propagators has emphasized the apparent difficulty of a state authority to enforce its juridical might and will upon Internet users, but this definition of state authority derives from John Austian who saw "law [as] a command backed up by threats, issued by a sovereign who acknowledges no superior, directed to a geographically defined population which renders that sovereign habitual obedience" (Boyle, 1997[55]). Foucault challenged exactly this kind of model as an explanation of state coercion, and emphasized the private, informal, and material forms of coercion organized around the concepts of "discipline" and "surveillance". Which returns us to the concepts of electronic panoptic applications, such as the log files that Internet Service Providers[56] use to track the movement of its customers across the Internet, or the encryption software and hardware standards that governments attempt to enforce embedded into public and private electronic devices[57] (Boyle, 1997). And lately, the Total Information Awareness (TIA) program, that will attempt to collect and analyse data from all US intelligence agencies as well as utilising public and commercial databanks such as the financial histories and medical records of individuals as well as their library and video rentals. In this gigantic database, sophisticated database search algorithms will flag any suspicious activity (Hentof, 2002). TIA also aims to develop biometric technologies for identifying and tracking individuals, such as gait and facial recognition

[53] Bentham's title goes as: "Panopticon; or the inspection-house: containing the idea of a new principle of construction applicable to any sort of establishment, in which persons of any description are to be kept under inspection" (Bentham, 1995: 29)
[54] Bentham imagined not only Panopticon prisons, but also factories, poor-houses, hospitals, asylums and schools (Bentham, 1995)
[55] No side number available as this is an Internet published article. Please refer to the literature list for citation details.
[56] ISP is an abbreviated denominator for suppliers of Internet access, i.e. the ones your modem phones up every time you log on.
[57] Such as the Clipper chip, which was meant to be a cryptographic device to protect privacy, but was equipped with "backdoors" for governmental agencies to listen in (Guisnel, 1997).

amongst large groups of people (Dowd, 2003). These are all devices or strategies designed to ensure discipline through its perceived omnipotent surveillance.

> Many people feel that the Internet is a free information communication medium, when in fact is not. The Internet as we know it today is controlled by the United States Government. And I am opposed to this.
> (Kashpureff, fieldwork interview spring 2000)

Hackers have, through their high understanding and application of technical knowledge occasionally protested the deployment of panoptic regimes, and has in a few cases, together with activist groups, been able initiate public discourses. The international "Jam the Echelon" is one example of this (Taylor, 2001). Hackers can be seen as an esoteric subculture, even more so than punks or Goths, as hacker membership is granted only through very high levels of technical competence and assets of secret knowledge. But a central and very important difference between, for example, the Goths and the hackers, may be that hackers has direct access to knowledge that the fields of power contest as their own, because by their activities bypass the institutionalised hierarchies of power. The hackers define the hegemony, which they see themselves up against, as a range of institutions that include governmental, military and corporate entities. In a debate about the political counter cultural validity of the hacking community we must bear in mind that hackers primarily imagine themselves hacking police, military and intelligence agencies and the they rationalise their reason for doing so in terms of their defence of civil liberties against the increasing activities of centralized military and intelligence agencies. Can hacker technical knowledge be defined as the cultural capital within the cultural field that hackers and fields of power inhabit? Normally the fields of power contain and control the dissemination of knowledge through its own institutions and agendas. The level of cultural and economic capital determines an individual's access to information; and educational institutions control the dispersion of information through a hierarchal curriculum-based learning. Hackers on the other hand, get their knowledge through non-curriculum channels of learning; from other hackers, from websites or just by borrowing books at the library. As one of my informants said: technical knowledge about sophisticated communications networks weren't necessary locked away in a safe somewhere because it was assumed that the technical obscurity would ensure its security (fieldwork interview, 2000). As Jordan and Taylor notes, "the key to understanding computer intrusion in a world increasing reliant on computer-mediated communication lies in understanding a community whose aim

is the hack [...] It is this community that stands forever intentionally poised both at the forefront of computer communications and on the wrong side of what hackers see as dominant social and cultural norms" (1998: 760). Ross (1990) finds the increasing negative definition of hackers occurring because they are perceived as a potential threat to normative educational ethics and national security. The definition of hackers as a "social menace" occurs because property law is rewritten in the light of the new information technology, causing the way power is exercised and maintained to change (ibid). The situation when seven of the major movie production companies in the US (the MPAA) sued the hacker website http://www.2600.com illustrates the ongoing conflict to define what is proprietary information in the advent of digital distribution[58]. This information is no longer contained within the producers own distribution network as popular file-sharing clients such as Kazaa (which has been downloaded more than 230 million times[59] to date) enables its users to swap music and movies across international and juridical borders.

> I think the MPAA is just running scared; they've started something, they don't understand what they were starting, because they don't understand the bits and bytes of the technology. And I think its going back to bite them!
> (Cheshire Catalyst, fieldwork interview July 2000)

Ross claim that deviant groups / hackers are defined as "public enemies" in order to rationalize the general law-and-order clampdown on free and open information exchange (1990). The free dissemination and access to knowledge stands as a central tenet in hacker culture, but what I derive from my anthropological fieldwork is that hackers themselves construct social hierarchies based on secret knowledge and confidential relationships. Therefore, paradoxically, hierarchies of secrecy constitute a central social dynamic that defines who has access to the hacker subculture while at the same time declaring free and unlimited access to information. The secret knowledge define power and status inside hacker culture, with a reciprocal exchange of hacker knowledge that appears exactly the same as that of any gift-based cultures only that the currency is different. Just as the Trobriand Islanders exchanged yams, hackers instead swap information, be it in the form of text files, web-site

[58] "[…] The technological factor involves those aspects of the electronic 'information revolution' which have digitalized information generation, storage, transfer, and reception while drastically reducing the size, cost and operational complexity of equipment used to control and manage data […] Stealing information in the digital age can be accomplished merely by intercepting formatted data at some points, either were it is stored, or as it is transmitted" (Warner, 1994: 143-160).
[59] Reuters news story at: http://zdnet.com.com/2100-1104-1009418.html

addresses or applications, signalling hacker status and establishing social connections. What I see as a central result of my study is not to define and categorise hackers as a subculture, but to investigate the social dynamics and mechanism in the relationship that defines the "outside" and "inside".

> I believe in social responsible hacking […] The hackers are largely the peoples voice that can be raised up to have an effect on the development of those rules, those laws which govern the deployment of the technology for the people, not for the commercial interest.
> (Kashpureff, fieldwork interview spring 2000)

Hackers appear to play out the same game as their opponents in the quest for knowledge and power. The hierarchy-based accesses to knowledge distinguish hackers as well as the hegemony they define themselves up against. What gives power is the access and appropriation of secret knowledge, its this power that define them as a social group, as well as granting them resources in their opposition to the hegemony, The paradox of their ideology of unlimited information access versus the practice of hierarchies of secrecy are not as disconcerting as it appears at first. Since power controls knowledge, opposing that power implies partaking in this game of knowledge and secrecy.

Literature List

Abercrombie, Nicholas, Hill, Stephen and Turner, Bryan S. (1994): *The Penguin dictionary of sociology*, London, Penguin

Asch, Timothy (1992): "The ethics of ethnographic film-making", in Crawford, Peter Ian and Turton, David (editors): *Film as Ethnography*, Manchester: Manchester University Press

Bentham, Jeremy (1995): *The Panopticon writings*, Miran Bozovic (editor), London, Verso

Bourdieu, Pierre (2000): *Pascalian Meditations*, Stanford, Stanford University Press.

Boyle, James (1997): *Focault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors*, Internet published article at: http://www.law.duke.edu/boylesite/foucault.htm

Chandler, Amanda (1996): "The Changing Definition and Image of Hackers in Popular Discourse" in *International Journal of the Sociology of Law*, Volume 2, Number 24.

Douglas, Susan J. (1987): *Inventing American Broadcasting 1899-1922*. Baltimore, Johns Hopkins University Press.

Dowd, Maureen (2003): "Walk This Way", *New York Times*, May 21'st.

Durham, Michael S. (2000): *En Guide fra National Geographic: New York*, Bagsværd: Forlaget Carlsen.

Eaton, Leslie (2003): "ECONOMIC PULSE: New York City; Economy Is Tough All Over, But in New York, It's Horrid", *New York Times*, February 19'Th

Ellin, Abby (2001): "PRELUDES; Dot-Coms' Loss Is Peace Corps' Gain", *New York Times*, April 15'Th.

Foucault, Michel (1977): *Discipline and punish: the birth of the prison*, London, Allen Lane.

Friedman, Ted (1997): "Apple's 1984:The Introduction of the Macintosh in the Cultural History of Personal Computers", paper presented at *the Society for the History of Technology Convention, Pasadena*, California, USA

Furnell, S.M. and Warren, M.J. (1999): "Computer hacking and cyber terrorism: the real threats in the new millennium?" in *Computers & Security*, Volume 18, Issue 1

Geertz, Clifford (1973): *The Interpretation of Cultures*, New York, Basic Books.

Godell, Jeff (1996): *The Cyberthief and the Samurai: The True Story of Kevin Mitnick – And the Man Who Hunted Him Down,* New York, Dell Publishing.

Guisnel, Jean (1997): *Cyberwars: Espionage on the Internet,* New York, Plenum Trade.

Hafner, Katie and Lyon, Matthew (1996): *Where Wizards stay up late: the origins of the internet*, New York, Simon & Schuster

Hannemyr, Gisle (1997): "Technology and Pleasure: HACKING CONSIDERED CONSTRUCTIVE" invited paper for *Pleasure And Technology,* Sausalite, CA

Hayes, Dennis (1989): *Behind the Silicon Curtain: The Seductions of Work in a Lonely Era*, London : Free Association Books

Heider, Karl G. (1976): *Ethnographic Film*, Austin, University of Texas Press

Hentoff, Nat (2002): "We'll All Be Under Surveillance", *The Village Voice*, December 6'th.

Jordan, Tim & Taylor, Paul (1998): "A Sociology of Hackers" in *Sociological Review,* Volume 4, number 46

Jordan, Tim (2001): "Mapping Hacktivism: Mass Virtual Direct Action (MVDA), Individual Virtual Direct Action (IVDA) And Cyberwars", in *Computer Fraud & Security*, Issue 4

Katz, Joe (1999): "Voices from the Hellmouth", series of internet published articles at http://slashdot.org/article.pl?sid=00/10/23/1521250&mode=nested

Knight, Dan (2001): *Personal Computer History*, Internet published article at http://www.lowendpc.com/history/index.shtml

Kovacich, Gerald L. (1999): "Hackers: Freedom Fighters of the 21'st Century" in *Computers & Security*, no 18

Levy, Steven (1984): *Hackers: Heroes of the Computer Revolution*, Harmondsworth, Penguin.

Littman, Jonathan (1997): *The Fugitive Game*, New York, Little Brown & Co

Littman, Jonathan and Donald, Roger (1997): *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen*, Boston: Little, Brown and Co.

Lyon, David (1994): "The Electronic Eye: The Rise of Surveillance Society*"*, Minneapolis: University of Minnesota Press Minneapolis.

Markoff, John (1999): "Palo Alto Journal; Hackers Enjoy One Last Meal From the Master of .com Cuisine", *New York Times*, New York, 11 September 1999.

Michele Slata (1996): "Masters of Deception", New York, HarperPerennial

Musser, Charles (1997[1996]): "Cinema Verite and the New Documentary" in Nowell-Smith, Geoffrey (editor): *The Oxford History of World Cinema: The definitive history of cinema worldwide*, Oxford: Oxford University Press

Orwell, George (1950 [1999]): "Nineteen eighty-four." Norwegian edition, translated by Tryggve Width, Oslo, Gyldendal

Peneberg, Adam L. (2000): "The Demonizing of a Hacker", Forbes, April 19'Th

Peterson, T.F. (2003): *Nightwork: A History of Hacks and Pranks at MIT*, Boston, MIT Press

Piotrowska, Agnieszka (2001): *True Originals: David Alan Harvey* (director), New York, National Geographic Television Networks

Rabiger, Michael (1998): Directing the Documentary, Boston, Focal Press

Raymond, Eric (2000): *The New Hacker's Dictionary*, Internet published dictionary at http://www.eps.mcgill.ca/jargon/jargon.html

Rosenbaum, Ron (1971): "Secrets of the Little Blue Box", *Esquire Magazine*.

Ross, Andrew (1990): *Hacking Away at the Counterculture*, Princeton, Princeton University.

S. M. Furnell and **M. J. Warren (1999):** "Computer hacking and cyber terrorism: the real threats in the new millennium?" in *Computers & Security*, Volume 18, Issue 1

Schultz, Duane P. and Schultz, Sydney Ellen (1969 [1992]): *A History of Modern Psychology*, San Diego, Harcourt Brace Jovanovich

Segaller, Stephen (1999): *Nerds 2.0.1: A Brief History of the Internet*, New York: TV Books

Shimomura, Tsutomo and Markoff , John (1996): *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It*, New York, Hyperion Books.

Smallman, Tom (1997): *New York, New Jersey & Pennsylvania: a Lonely Planet travel survival kit*, Hawthorne, Lonely Planet Publication.

Sterling, Bruce (1992): *The Hacker Crackdown*, London, Bantam.

Stoll, Clifford (1989): *The Cuckoo's Egg: Tracking a Spy Through the Maze of Counter-espionage*, New York, Simon & Schuster.

Taylor, Paul A. (1998): "Hackers. Cyberpunks or microserfs?" in *Information, Communication & Society* 1:4

Taylor, Paul A. (1999): *Hackers: Crime in the Digital Sublime*, New York, Routlegde

Taylor, Paul A. (2001): "Editorial: Hacktivism," *The Semiotic Review of Books* 12.1

Thieme, Richard (2002): "The Hacker Preacher" in *Network Security*, Issue 10

Thornton, Sarah (1995): *Club cultures: music, media and subcultural capital*, Cambrigde, Polity Press

Thornton, Sarah (1997[1995]): "The Social Logic Of Subcultural Capital" in Gelder, Ken and Thornton, Sarah (editors): *The Subcultures reader*, London, Routlegde

Walleij, Linus (1998): *Copyright Does Not Exist*, translated by Daniel Arnrup, Internet published article at: http://svenskefaen.no/cdne

Warner, William T. (1994): "International Technology Transfer and Economic Espionage" in *International Journal of Intelligence and Counter-Intelligence*, volume 7, number 2

Webb, Jebb and Schirato, Tony and Danaher, Geoff (2002): *Understanding Bourdieu*, London: SAGE Publications

White, Thomas H (2003): *United States Early Radio History*, Internet web project at http://earlyradiohistory.us/

Williams, Raymond (1977): *Marxism and Literature*, Oxford, Oxford University Press.

Willis, Paul (1990): *Common Cultures: Symbolic work at play in the everyday cultures of the young*, Buckingham, Open University Press

Wright, Robert: "Brave New World Department: Hackwork", *The New Yorker*, January 29Th

Zakon, Robert H. (2003): *Hobbe's Internet Time Line v.6.0*, Internet published article http://www.zakon.org/robert/internet/timeline/

Zuckerman, Michael J. (2001): "What fuels the mind of the hacker", *USA Today*, February 6'Th.

Appendix I: Fieldwork Camera Equipment List

Camera Sony Hi8 TR3100E. Sony Wide-angle Converter 0.7 VCL-R0752. Remote Control RMT-717. Sony Power Adaptor AC-V315 w/power cable. Batteries NP-F530 and NP-F750. Body Monopod Hama BS 51. Microphone Sure Prologue 16L w/wind protection. Microphone Sony mosquito w/power supply ECM-144, clip and wind protection. Cable XLR 0.5 meters. Cable XLR 12 meters. Cable minijack 4 meters. Adaptor minijack/male XLR/female. Adaptor EuroSCART/3xphono/female. Cable 3xphono/male. Microphone grip extender. Microphone grip. Minolta 505si still camera, with 100-400 telephoto lens and fisheye lens.

Total recorded material: 5 Sony Hi8 tapes (PAL length) plus additional 20 tapes (NTSC length), two audiocassettes (60 minutes each), and more than 300 stills.

---

[i] The commercial was directed by Ridley Scott at a budget of US $900.000 and aired during the Super Bowl XVIII on January 22, 1984. The voice of the Big Brother spouted, "My friends, each of you is a single cell in the great body of the State. And today, that great body has purged itself of parasites. We have triumphed over the unprincipled dissemination of facts. The thugs and wreckers have been cast out. And the poisonous weeds of disinformation have been consigned to the dustbin of history. Let each and every cell rejoice! For today we celebrate the first, glorious anniversary of the Information Purification Directive! We have created, for the first time in all history, a garden of pure ideology, where each worker may bloom secure from the pests of contradictory and confusing truths. Our Unification of Thought is a more powerful weapon than any fleet or army on Earth! We are one people. With one will. One resolve. One cause. Our enemies shall talk themselves to death. And we will bury them with their own confusion! We shall prevail!" Apple denied any comparison of the entity Big Brother in the commercial with its main competitor, IBM.