



This document is a stripped version of my bachelor thesis. I hope you have fun reading it.
Spread it as much as you like. However, please leave this message in it.

Paris2k – Paris2K@awarenetwork.org

0. Abstract	2
1. Introduction	2
1.1 Main questions	3
1.2 Methodology	3
2. Media representation of hackers	4
2.1 Hacker representation in online news articles	4
2.2 Hacker representation in Hollywood films	5
3. How hackers see themselves	7
3.1 Hackers in the literature	7
3.2 Hackers questionnaire	13
3.2.1 The Questionnaire Explained	13
3.2.2 The Results	15
4. Subculture Theory & Hacker Subculture	17
4.1 Subculture Theory	17
4.2 Hacker Subculture	19
5. Conclusions	20
6. Bibliography	22

Appendix I: Analyzed News articles

Appendix II: Questionnaire

Appendix III: Questionnaire Data

Abstract

This paper examines the ways in which media represent the hacker subculture in both online news articles and Hollywood films. It examines how members of the hacker subculture see themselves and what differences exist between these two representations of the hacker subculture. It then builds upon existing theories about subcultures to explain the differences between the image portrayed by the media and the way that hackers see themselves..

1. Introduction

Somewhere roughly around 1994 I used my modem to dial in to the internet for the first time ever. Since then I have been extremely intrigued by computers, but even more so, by the internet and the hacker subculture. I have read many of the standard works that discuss hackers, the history of hacking and the history of the internet itself. Books like Steven Levy's "Hackers", William Gibson's "Neuromancer", Bruce Sterling's "The Hacker Crackdown: Law and Disorder on the Electronic Frontier", Paul Mungo's "Approaching Zero : The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals", Suelette Dreyfus' "Underground: Tales of hacking, madness and obsession on the electronic frontier", etcetera. I have found, throughout the years, that I agree with and subscribe to the ethics, views and ideology of the hacker subculture. However, when I open up a daily newspaper, or read the electronic news articles written by CNN or the BBC, or any other news source, I am greeted, every single day by such headlines as:

"Welsh hacker faces jail sentence",

"Russian computer hacker sentenced to three years in prison",

"Two arrested in Wales for credit card theft costing \$3 million",

"Analyst puts hacker damage at \$1.2 billion and rising".

The media try and explain to us who these hackers are and what it is that they do. They warn us, the general public of these cyber criminals. Who are these people that hack into computer systems and write viruses and cause such incredibly high amounts of damage? And what exactly is a hacker? Are they to blame for computer break-ins, for viruses, for trojans? Are they ordinary criminals, who, for some reason have chosen to use computers to commit their crimes? Or are they, as suggested in some articles, youngsters, teenagers? If so, then how is it possible that they cause millions of dollars in damages and get sentenced to years and years in prison? All of these questions come to mind when reading a daily newspaper or watching the evening news. Or even when going to a movie, where one can see hackers do all sorts of interesting and mysterious things.

The portrayal of the hacker subculture that the media present us with every single day, is not one that I recognise. Or, at best, it is one that I believe to be inaccurate. As Schwartau puts it:

"Forget what you've read in your local newspaper or seen on CNN. Some of it is right, but a lot of it is wrong."(Schwartau 2000)

This leads me to the following questions.

1.1 Main Questions

Main Questions

How are hackers being represented by the media and how do hackers see themselves?

What could be the reasons for any existing differences between these two views of hackers?

Sub Questions

1. How is the hacker subculture portrayed in the media?

2. How do hackers see themselves?

3. What differences exist between the way that media portray hackers and the way the hacker subculture sees itself?

4. What explanations could exist for any possible differences?

5. How do media and subcultures generally relate to each other?

1.2 Methodology

In *chapter 2* I try to explain how hackers are represented by the media. In *paragraph 2.1* I will go into the way that hackers are represented in news articles from online sources like CNN.com (CNN's online news service), BBCi (The BBC's online news service), and Wired News. To be able to conclude how the hacker subculture is portrayed in these articles, I have analyzed over fifty articles from different sources, which can be found in Appendix I. In *paragraph 2.2* I describe how hackers are portrayed in several major Hollywood films like *Wargames* (1983), *Sneakers* (1992), *Hackers* (1995), *Swordfish* (2001) and *The Italian Job* (2003). In *chapter 3* I go into the way that the members of the hacker subculture see themselves. First, by discussing some relevant parts of the literature about the hacker subculture in *paragraph 3.1* and secondly by explaining the results of a questionnaire that I asked members of the hacker subculture to fill out, in *paragraph 3.2*. In *chapter 4* I give an overview of Hebdige's (1979) theory about subcultures and try to explain the reasons why the media represent the hacker subculture the way they do. A short explanation of subculture theories will be given in *paragraph 4.1* and in *paragraph 4.2* I will apply these theories to the hacker subculture in specific. In *chapter 5* I draw conclusions from my research. Finally the sources I used and quoted from are in *chapter 6* and relevant research data can be found in *Appendixes 1, 2 and 3*.

2. Media's representation of hackers

2.1 Hacker representation in online news articles

In order to fully understand how hackers are portrayed in the media, I have chosen to examine a large number of news articles published online by "respected" and "well known" news and journalistic sources. The sources are (amongst others) The BBC, CNN, and Wired. I chose to examine online news articles only, for two specific reasons; First because obviously the world wide web allowed me to easily gather and analyse these articles, and secondly because most of these news agencies have specific online departments which one would expect to have more knowledge of and feeling with the internet and its culture then regular news journalists.

I intentionally chose not to consider whether or not these news articles were factual or not, because my goal was to show exactly what image of hackers the media show us. Whether or not this image is correct or far from the truth is, at this time, irrelevant.

After analyzing these news articles I concluded that for the greater part the writers of the articles share a common view of who hackers are and what exactly it is they do. Of course there are some

differences between the various articles, but in general we can come to the conclusion that according to the media, hackers are:

Mostly, but not only, young teenage boys, who

Break into computers, use and write worms, trojans and viruses, perform denial of service attacks against vital computer networks and communication systems, steal and destroy all sorts of valuable information including credit card details, deface websites, blackmail and extort businesses, and basically cause billions of dollars in financial damages.

There were also some descriptions of hackers and their activities that were mentioned only in one or two articles. These descriptions ranged from:

"[...] an obsessive middle-class white male, between 12 and 28 years old, with few social skills and a possible history of physical and sexual abuse"(Glaves 1999)

to

"Hackers, [...] are nothing more than socially isolated nerds of substandard intelligence who spend 16 hours a day in front of their computers, growing increasingly out of touch with reality while manically putting "pre-written codes together" [...] Their criminal behaviour is explained by the fact that hackers are "more comfortable with machines than people."(Poulsen 2000)

One particular source of news articles, namely Wired.com seems to have its own idea about who hackers are and what it is that hackers do. The image of hackers they give their readers doesn't correspond with the image given by the other, earlier mentioned news sources. The hackers that Wired describes in its articles are mostly hardware and software engineers, programmers, that have used their knowledge to circumvent copyright protection devices, hack into digital devices such as the Tivo Digital television system, and cracking DVD anti-copying technology.

So if the question would be whether it is possible to conclude that all and every news source I used in my research, portray hackers in the same way, the answer would have to be no. However, the majority seems to agree on what it is that hackers do and who hackers are.

2.2 Hacker Representation in Hollywood Films

Ever since the 1983 movie Wargames, starring Matthew Broderick, hacker characters have occasionally played parts in big Hollywood productions. And as the general public got familiar with personal computers and the internet and the world around us digitalised, Hollywood did not stay behind. In this part of my paper I will discuss how hackers are portrayed in several films. These films being: Wargames (1983), Sneakers (1992), Hackers (1995) Swordfish (2001) and The Italian Job (2003).

Analysing hacker portrayal in any single one of these films in depth would probably result in enough material to write several interesting papers, but I have chosen to only analyze in short, what image is given in these films of hackers and their activities. My goal is not to analyze the portrayal of hackers in films as such, but as a part of the larger portrait that the media paint of hackers.

Wargames

Simply said, WarGames is a movie about a young man who is looking for a particular computer game and ends up connecting to a military computer. What he thinks is a strategy game of warfare, actually is the real thing. He and the military computer "play" against each other in finding the best strategy to fight a nuclear war. The young man, David Lightman, played by Mathew Broderick, gets arrested for breaking into the computer and almost starting a real nuclear war. But after his arrest the computer continues the "game" and will soon find a winning strategy and thus start firing nuclear missiles. Lightman escapes and in the end saves the world by teaching the computer the simple game tic-tac-toe and showing him, that, as with nuclear war, there can never be a winner. Lightman is portrayed as a young man, who is computer-savvy and although he engages in some criminal behaviour, the audience tends to forgive him, because it is also his knowledge of computers, that saves the world.

Sneakers

Martin Bishop, played by Robert Redford, is the head of a group of experts who specialise in testing security systems. Bishop has a shady past when it comes to computers and hacking. When he is blackmailed by people who he assumes to be government agents, into stealing a top secret decryption box, the team find themselves stuck in a game of danger and intrigue. After they get a hold of the box, they discover that it has the capability to decode all existing encryption systems around the world, and that the agents who hired them didn't work for the Government after all.

Hackers

In this movie, hackers are young, rather hip teenagers that get blamed for a very destructive virus they didn't write. The virus was written by a security advisor to a big international company, whose sole purpose is to steal a large amount of money. To stop disaster from happening and exposing the real culprit, the group of hackers has to keep one step ahead of the police. The hackers basically perform harmless pranks and in the end are the ones that save the day, even though to do so, they have to perform some hacking activities that are officially against the law.

Swordfish

Hugh Jackman starres in Swordfish (2001) as an ex-computer hacker named Stanley Jobson, who is seduced into joining forces with renegade CIA agent Travolta. Although he has made some

wrong decisions in the past, Jackman's character Jobson is now on parole and is planning to clean up his act. However, John Travolta's evil character Gabriel Shear is rather convincing when using a gun, a beautiful woman and the knowledge that Jobson needs money in order to retrieve custody of his daughter.

The Italian Job

In the movie *The Italian Job* Seth Green plays the role of "Lyle", a hacker. The story is simple. A group of "good" thieves steal a large amount of gold bars from some other, less friendly thieves. They have a brilliant plan and everything seems to go well until one of the team turns on the others. This character, played by Edward Norton, kills the leader of the group and steals the gold. Of course the team will steal the gold back again and have their revenge. Lyle, the hacker uses his skills to help his friends find the gold and eventually take care of their evil enemy.

Although the above described films differ greatly from each other, they all have a few things in common. They all portray hackers in a rather similar way. In these films hackers are people who have great understanding of computer systems. They might have had some trouble with the law in the past, but they are in effect "good" people that the audience can identify with. In these films, hackers seem to have extraordinary abilities, and seem fairly able to do almost anything using computers. In most of these films hackers break the law, but it is obvious that they do this, not because they have financial gain in mind or because they have malicious intent, they do it because they are either forced to (*Swordfish*) or they do it by accident (*Wargames*) or, as in almost all of these films, they do it to take care of some greater evil and save the day. The image given of hackers by (these) Hollywood films is one of heroes. May it be somewhat nerdy heroes, but heroes none the less.

Thomas comes to a similar conclusion and describes this as follows:

"In films like sneakers (1992), The Net (1995), and The Matrix (1999), hackers serve as central figures who are able to outwit the forces of evil based on an extraordinary relationship to technology." [...] all presented hackers as technologically sophisticated protagonists able to perform acts of high-tech wizardry in the service of law enforcement or the state.(Thomas 2002)

Thomas goes on to explain that yes hackers are portrayed as criminals and outlaws, but that there sense of criminality is negotiated throughout the narratives themselves. In other words, in the storyline of the film it becomes obvious to the audience that there is a justification for the hacker to engage in these activities. Hackers are forced to use their knowledge of computers to fight a great evil, to save the world or to expose horrible secrets or injustices.(Thomas 2003)

The image portrayed by (these) Hollywood films is thus far more positive than the image portrayed by the earlier analyzed news articles. However, part of the difference between these two views could

probably be explained by the goals that these different media tend to have. News articles are expected to portray and reflect on reality, whereas in films, anything goes.

3. How Hackers see themselves.

3.1 Hackers in the literature

To be able to understand who exactly hackers are and what hackers do, we have to take a look at a little bit of hacker history.

A Very Short History of the Hacker Subculture: The Old & The New Generations

Contrary to popular believe, hacking and the hacker subculture are not phenomena that came to life in the 1990's or even later. Hacking and hackers go back quite a long way.

The Old Generation of Hackers

The term "hacking", as used to refer to the activities of members of the hacker subculture, was born in the 1950's at MIT. As Steven Levy explains in his book "Hackers", a hack, was the name given to

"a project undertaken or a product build, not solely to fulfil some constructive goal but with some wild pleasure taken in mere involvement"(Levy 1984), by the members of MIT's Tech Model Railroad Club.

"[...] to qualify as a hack, the feat must be imbued with innovation, style and technical virtuosity"(Levy 1984)

These students working with all sorts of machines had a desire to explore technology and didn't merely want to use things, they wanted to figure out how they worked. Douglas Thomas explains that these *"old-school hackers were usually graduate students at large universities"*.(Thomas, 2002) They lived within the institutional culture of the big Universities, where they had access to the large mainframes. They pushed computers and computer programs to the limit and solved all kinds of problems. What they were doing is hacking (amongst other things) computers. These "hackers" also shared a particular set of ethics. It is important to have a look at these ethics to be able to understand who hackers are and which rules the subculture lives by.

Hacker Ethics

The early generations of hackers subscribed to a particular set of values, of ideas. They shared an ideology and a set of ethics. In his book "Hackers", Steven Levy (Levy 1984) explains what this set of ethics is all about.

1. 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!
2. All information should be free.
3. Mistrust authority--promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

The anonymity that the internet provides to users and to hackers in particular, makes it possible for people to be judged by their actions, rather than by the colour of their skin or the fact that they are a man or a woman, a teenager or a businessman. The internet thus makes equality possible and rids us of prejudices. In the hacker subculture this particular attitude seems deeply rooted, as can be seen in the following lines that were taken from "*The Hacker Manifesto*", which is arguably the most famous text in the computer underground.

"We exist without skin colour, without nationality, without religious bias... (...) My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like." (Mentor 1986)

5. You can create art and beauty on a computer.
6. Computers can change (your) life for the better.

Richard Stallman, a famous member of the hacker subculture explains it as follows:

"In 1971 when I joined the staff of the MIT Artificial Intelligence lab, all of us who helped develop the operating system software, we called ourselves hackers. We were not breaking any laws, at least not in doing the hacking we were paid to do. We were developing software and we were having fun. Hacking refers to the spirit of fun in which we were developing software. The hacker ethic refers to the feelings of right and wrong, to the ethical ideas this community of people had -- that knowledge should be shared with other people who can benefit from it, and that important resources should be utilized rather than wasted."(Stallman)

As computers spread around the rest of America, hacking flourished in computer labs of several big Universities, such as Harvard, Carnegie Mellon University, Stanford and others during the 1960's and 1970's. It was the institutional environment that allowed hackers to use computers and hack, because Universities were the only place where one could work with these early computers.

However, in the San Francisco Bay Area, a number of people formed the "Homebrew Computer Club". The goal of these hobbyists was to build and use their own computers. They helped each other and shared code and software and information on how to build and use computers that they could use in their homes. People like Microsoft founder Bill Gates and the founders of Apple, Steve Jobs and Steve Wozniak were part of this wave of computer enthusiasts, this wave of hackers. These hackers played a very large role in the birth of the personal computer.

It is these hackers, the hackers of the 1960's and 1970's that are considered the "Old-school hackers". It is these hackers that created the personal computer and developed the internet, with military funding. It was possible for this generation of hackers to use and fiddle with computers and subscribe to their set of ethics and to reject secrecy and promote freedom, because the institutional environment that they lived in (MIT and other Universities) allowed them to do so.

As Levy explains it:

"To a hacker, a closed door is an insult, and a locked door is an outrage. Just as information should be clearly and elegantly transported within a computer, and just as software should be freely disseminated, hackers believed people should be allowed access to files or tools which might promote the hacker quest to find out and improve the way the world works. When a hacker needed something to help him create, explore, or fix, he did not bother with such ridiculous concepts as property rights."(Levy 1984)

Levy also mentions another example in his book. He explains that in the perfect hacker world one should be allowed to open up a traffic light and improve the way it works, whenever one would feel like doing so.(Levy 1984) That perfect hacker world seemed to exist within the compressed space of the institutional world, where with access to technology and military funding, it was possible to live by the rules of hacker ethic.

The New Generation of Hackers

The latest generations of hackers have always had computers around. They have grown up with computers.

"The introduction of the personal computer into the home, in the 1980's and 1990's, transformed a predominantly male, university culture into a suburban, youth culture and set these two histories, in part, against each other," as Thomas puts it.(Thomas 2002)

No longer was hacking something that was only possible to do within the environment of universities and science labs. Everyone who so desired could now buy a personal computer and start hacking. However, the newer generation of hackers lives in a world where society comes to depend more and more on computers and a digital infrastructure. There isn't much room left to tinker with computers and networks, other than in the safety of a computer user's home. The new generation sees the older generation as examples, people to look up at. But some people of the

older generation are less loved. They have started their own companies, they have become part of mainstream society and the new generation of hackers feel that some members of the old generation have disregarded the original hacker ethic. The younger generation is comprised of mainly teenage boys, who find computers to be a way to gain independence, to defy authority and to deal with the struggle of growing up. Never before have teenagers experienced such a large amount of power, as they do now, through the use of personal computers and the rise of digitalization.

Semantics

A very important issue concerning the different views that media and the hacker subculture itself have of hackers and hacking seems to be a problem of semantics. As explained earlier the term hacker was used in the past to refer to the people who worked with early computers and who had a desire to tinker with things and to understand how things worked.

So let us have a look at how a few well known members of the hacker subculture describe the meaning of the word "hacker".

In "*Hacker Being; on the meaning of being a hacker*"

Valerio Capello, in the subculture known as "*Elf Qrin*", writes the following:

"Another idiot has been locked up because of committing a senseless act with little or no thought to the consequences. Law enforcement needs to look good, the news becomes public domain and the press is unleashed, using attention grabbing headlines like: "Computer terrorist busted", or better, a "hacker". Not only is the term misused, but it is usually only understood to be a mere synonym for "computer pirate", which is not only limitid, but completely wrong. Few people, even those who would define themselves as such, really know what "being a hacker" means."(Capello 2000)

Capello then goes on to compare several meanings of the word hacker and finally ends up quoting from the "*Jargon File*" which is "*a comprehensive compendium of hacker slang illuminating many aspects of hackish tradition, folklore, and humor*". (Raymond 2003)

The on-line hacker Jargon File, version 2.9.10, 01 JUL 1992 (part of the Project Gutenberg), at the "hacker" entry says:

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.
3. A person capable of appreciating {hack value}.

4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it; as in 'a UNIX hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.)
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
[deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence 'password hacker', 'network hacker'. See {cracker}.(Capello 2002)

Both Capello and Raymond explain that hackers are not people with malicious intent. They are merely people who love computers and programming. Both Capello and Raymond also distinguish between hackers and people who commit crimes using computers. (computer pirate/cracker)

Members of the computer underground

The literature shows that hackers distinguish between different members of the computer underground. Whereas the media tend to refer to any person who is a member of the computer underground as "hacker", the hacker subculture itself feels there is a clear difference between the following people:

Hacker

Although the definition of the word hacker is very controversial, most people in the computer underground seem to agree that a hacker is someone with a thirst for knowledge. Someone who has a profound understanding of how computers work, or at least the desire to know. A hacker is a person who likes to tinker with computers and try and understand them and push them to the limit.

Cracker

Cracker is a word comprised of two different words: *criminal* and *hacker*. Hence, a cracker is a criminal hacker. Crackers are regarded as people who are hackers but whose motivation lies not (solely) in gaining knowledge but also in profiting from their hacking skills. Generally a cracker is seen as someone who does not abide by the hacker ethic.

The word cracker is also used to refer to people who "crack" software, or break limitations of use on copyrighted games or software.

Whitehat

A whitehat is seen as a "good" hacker. Hacker and whitehat are words which are often used as synonyms. In some cases people refer to a person as a whitehat when he or she works as a computer security professional. Whitehats are considered to be hackers, who might have been active in several sorts of hacking activities at one time, but who are now purely "legit".

Blackhat

A blackhat is seen as person who is "evil" as apposed to good. Blackhat is a word sometimes used as a synonym for cracker. Blackhats engage in hacking activities and have less regard for the law then hackers, if any.

Greyhat

A greyhat is a hacker who is somewhere in between white and black (hence the grey). He or she is a hacker but might, at times, engage in illegal activities simply because all things are not black and white.

Scriptkiddie

A scriptkiddie is seen as the lowest of lowest. This person has no particular skill. He or she is often a young person lured by the myths of hacking and uses readily available tools and code. A scriptkiddie is not able to create code. He has no profound understanding of computer systems. A scriptkiddie engages in malicious behaviour and generally is seen as someone who spoils the hacker name and is definitely not worthy of the title of hacker.

Viruswriter

A viruswriter is a programmer who enjoys writing viruses. Although they can be regarded as skilled people, because of the knowledge it takes to write good code, they are often frowned upon because of the destructive intent of most viruses.

3.2 Hackers Questionnaire

3.2.1 The Questionnaire Explained

In the former paragraph I have tried to discuss the way that the hacker subculture sees itself, as based on different literature about the hacker subculture. In this paragraph I will discuss the results of a questionnaire I had members of the hacker subculture fill out. My goal was to see whether or not actual members of the subculture agree with what has been written in the literature

about hackers. After combining the literature about hackers and the views of hackers themselves, I feel I can give an accurate image of how members of the hacker subculture see themselves. Furthermore, this allows me to compare the way hackers are described in the media with the way hackers see themselves.

First I will explain the questions that I asked people to answer and why I asked these specific questions. The actual filled out questionnaires can be found in Appendix II. The data and statistics as calculated with SPSS 11.5 can be found in Appendix III.

Questionnaire:

1. About Yourself

1. *Are you male or female?*
2. *How old are you?*
3. *Are you currently in a relationship?*
4. *Do you consider yourself to have little friends / a normal amount of friends / a lot of friends?*

The goal of the first section of questions was simply to see whether the image portrayed by the media, of hackers being mainly teenage boys, with few social skills corresponds with how hackers see themselves.

2. About Hackers

5. *Could you describe, in a few sentences, what a hacker is, by your definition?*
6. *Could you describe in a few sentences, what a script kiddie is?*
7. *Could you describe in a few sentences what the difference is between a white hat and a black hat?*
8. *Is there a difference between hackers and crackers? If so, could you explain the difference?*

This second section of questions serves to examine whether members of the hacker subculture actually have a different definition of the word hacker, than the media does. And, to examine whether, unlike the media, they distinguish between different members of the computer underground, as the literature suggests.

3. About Hacking

9. *Have you ever done anything, in terms of hacking, that might have been against the law? If so, did you feel that what you did was a bad thing?*
10. *Do you live by a hacker code or a set of hacker ethics? If so, could you explain the main "rules" of this ethic?*
11. *Do hackers write Trojans?*

12. Do hackers write viruses?
13. Do hackers perform (distributed) denial of service attacks?
14. Do hackers steal credit cards numbers?
15. Do hackers deface websites?

This third section is meant to examine whether members of the hacker subculture actually engage in the negative and sometimes illegal activities that the media would have us believe.

4. Hackers in the Media

16. Could you describe how hackers are portrayed in the general media?
17. Do you feel the general media show a correct image of what hackers are?

This fourth and last section serves as a way to examine how the hacker subculture feels it is being portrayed in the media.

3.2.2. The results

About Yourself

Questions 1 – 4

The results show that of the 14 participants in the questionnaire, 92.2% are males and 7.1% is females and the average age is 17. This supports the medias view that hackers are mostly teenage boys. 42.9% of the participants is currently in a relationship and the other 57.1% is not, while 0% claims to have few friends, 64.3% feels they have a normal amount of friends and 35.7% answered that they have a lot of friends. This clearly contradicts the medias view that members of the hacker subculture could be considered as people with few social skills or a lack of a social life.

About Hackers

The questions in this section couldn't really be calculated in SPSS and so I will try and explain the average answer given by the participants.

Questions 5 – 8

Almost all of the participants agreed that a hacker is someone who has a great interest in and love for computers and who is on a quest for knowledge. Someone who wants to know how computers work and who wants to explore them. Many participants also clearly stated the fact that hackers have no malicious intent. This answer corresponds to the definition of hackers as described in the literature and clearly shows that the hacker subcultures definition of a hacker is different from the medias definition of a hacker.

The idea that hackers hack for intellectual challenge and to understand computers is also what Lieberman found in his extensive studies of hackers. Lieberman interviewed over 42 hackers and came to the conclusion that hackers are motivated to hack for several reasons:

"(..) they hack for the intellectual challenge, to get knowledge, to learn about computers and computing, to get to know how things work, to get feelings of achievement and to satisfy their curiosity".(Lieberman)

A scriptkiddie is regarded by the participants in my questionnaire as someone with little knowledge of computers and who generally uses other people's code and programs to perform malicious acts.

From the results it is clear that the majority of the participants distinguish between different members of the computer underground. Hackers are generally seen as computer enthusiasts who have a desire to learn and who have no malicious intentions. Crackers are seen as criminal hackers whose pure purpose is to profit by their hacking. Whitehat hackers and blackhat hackers seem to be used as synonyms for hacker and cracker.

About Hacking

Questions 9 – 15

The majority of the participants admit that at one time or another they have engaged in activities that might be considered against the law and all of them claim they don't feel that what they did was wrong. Most of the participants do not specifically seem to live by any hacker ethic.

The results show that 50% of the participants agree that hackers write Trojans. 28.6% disagrees with this statement and 21.4% agrees but mentions the fact that although hackers may write them they won't use them for malicious activities, rather to learn.

14.3% of the participants say that hackers write viruses. When 64.3% says that hackers do not and 21.4% state that yes hackers write viruses but they do this to learn and without causing harm.

21.1% of participants state that hackers do perform (distributed) denial of service attacks. While 71.4% answers that hackers do not and 7.1% answers that hackers might but without doing any harm, stating the desire to learn as a reason.

When asked whether hackers steal credit card data, 7.1% answers yes, 78.6% answers no and 14.3% answers that they might do so but again, with the attention to learn things and without the intention to do any harm.

When asked if hackers deface websites, 42.9% answers yes and 57.1% answers no.

Hackers in The Media

Questions 16 and 17

Almost every single participant feels that the Media give the wrong image of hackers. Some simply answer that the media do not correctly portray hackers, but most explain that when the media describe hackers they are actually referring to black hat hackers, criminal hackers (crackers) or scriptkiddies. The majority feels that the media give hackers a bad name.

In conclusion we can say that the results regarding average age and sexe correspond with the views of the media. Contrary to the image that the media portray of them, hackers themselves feel they have healthy social lives. Furthermore, hackers distinguish between different members of the computer underground (hackers, crackers, whitehats, blackhats, scriptkiddies) whereas the media uses the term hacker to describe all of the above. The majority of participants feel that hackers do not engage in the malicious activities mentioned by the media and of the part that answered that they do, a large part explained that when they do, it is with the intention to learn, not to do harm. Finally, all of the participants feel that the media incorrectly portray hackers.

4. Subculture Theory & Hacker Subculture

4.1 Subculture Theory

The unnatural break: subcultures and parent culture

In his article *Betrayal and Fear: Press Coverage of Canadian Skinheads*, Murray Foreman explains that subcultures intentionally oppose the status quo. There exists a divide between on the one hand a (youth) subculture and on the other hand the parent culture. The subcultures are said to produce new codes and means of signification through which they create a self-imposed exile. In this way, subcultures try to distant and differ themselves from their parent culture and from other subcultures. (Forman 1992) The meaning of style is, according to Thomas, generated by the subculture that takes symbols of mainstream culture and gives these symbols, these parts of mainstream culture, a different and often oppositional meaning. (Thomas 2002) This new style, which is created by a subculture, signals refusal of the mainstream discourse and creates the subcultures own discourse. Style is used as a way to rebel and defy against the parent culture.

Hebdige states that:

"(...) violations of the authorized codes through which the social world is organized and experienced have considerable power to provoke and disturb".(Hebdige 1979)

A specific example of hacker style could be the so called "l337 sp34k". (Elite speak) Code, normal language, is taken from the parent culture and is altered. In a digital society where everything exists of ones and zeros, certain members of the hacker subculture have chosen to write words in a different way, replacing the "a" by a 4 and the "e" by a 3 for example. Another example would be

the use of "ph" where one would normally use an "f". As in "phreak" in stead of freak, to show the fact that a "phreak" is a person who hacks phones.

This is what Hebdige calls the unnatural break; taking a part of mainstream society, of parent culture and changing it, creating ones own style, opposing parent culture by creating ones own style. This phenomenon is disruptive to mainstream society, to the parent culture of which the subculture is a part and thus asks for a reaction from the parent culture.

Ways of Incorporation

Hebdige's *Subculture; The Meaning of Style* (Hebdige 1979) is considered a classic work in several disciplines. It describes several different subcultures in the post war United Kingdom from rockers to skinheads and punks. In his book Hebdige explains the different ways in which mainstream society can deal with the unnatural break that is created by subcultures. The unnatural break causes a wave of hysteria in the media. Media seem either amused, fascinated, shocked or outraged by the emergence of a new subculture and it is the subcultures specific style that plays an important role in this process. It is, as Hebdige explains, firstly its style and secondly a subcultures anti-social or criminal behaviour that creates a certain moral panic within the parent culture. Hebdige distinguishes between two ways in which mainstream society "*defuses*" or "*freezes*" the threat posed by subcultures. They are the commodity form and the ideological form.

The Commodity Form

The commodity form is when style of subcultures is recognised by companies and businesses (mainstream society) and then packaged and sold. Specific style elements of a subculture are hyped and are made generally available to anyone who wants to buy it, use it or wear it. Thus, that which first was a subcultures way of defying and opposing parent culture and other subcultures, now becomes common good. Thereby "*freezing*" or "*defusing*" the threat that the subculture posed to mainstream society. An example which is rather unlikely to happen, would be when shaving ones head would become common good. This example of skinhead subcultural style, of shaving their heads, would loose the power that differentiates them from mainstream culture.

The Ideological Form

The ideological form of incorporation basically normalizes the subculture or transforms it into *meaningless exotica* (Hebdige 1979). Any existing differences between parent culture and subculture will be reduced to something not worth of much attention. The impact of subculture gets trivialised or members of subcultures will be seen as social misfits, outcasts, but definitely not as people who could form a threat to parent culture.

As we have seen above, Hebdige explains that there are several ways in which mainstream society or parent culture, can deal with the unnatural break caused by subcultures. A very important role

in this decision to handle subcultures in a particular manner, is played by mainstream media. As Foreman explains it:

"As a prominent cultural institution, the media are strongly associated with the privileges of social dominance and are actively involved in the process of 'consensus building.' They are situated in a central social position enabling them to inscribe certain preferred ideological values and attitudes over those alternative, oppositional or resistant propositions emanating from the social periphery."(Foreman 1992)

Foreman goes on to explain that the media act as social monitors that focus on subcultures newness, on subcultures being different from mainstream society and on a possible danger that subcultures could pose to the existing parent culture. However he also comes to the conclusion that, leaving aside some alternative media, media coverage mostly remains supportive of the present social structure. (Foreman 1992)

4.2 Hacker Subculture

The question now is, whether Hebdige's theory about subcultures applies to hackers and especially hackers in the year 2004. Hebdige's theories about subculture are based on research he did into post war subcultures in the 1970's in the United Kingdom. The subcultures he examined and discusses are teddyboys, mods, skinheads, punks, rockers and others. Of course these subcultures are completely different from the hacker subculture in the year 2004. However, many of the theory that Hebdige formed, seems to also be applicable to hacker subculture, its style and the way media deal with the hacker subculture.

We've seen, throughout this paper and research, that the image portrayed of the hacker subculture, by the media, is one that the hacker subculture itself strongly disagrees with.

There are several reasons for the fact that media and hackers themselves both have and portray a different image of the hacker subculture. The way in which media (as a part of and spokesperson for mainstream society) incorporates the hacker subculture could well be one of these reasons.

I believe the first form of incorporation that Hebdige distinguishes, the *commodity form* is not particularly used to incorporate the hacker subculture into main stream society. Hacker style and other characteristics of the hacker subculture are hardly things one could package and sell. It is the goal of such incorporation to "*defuse*" or "*freeze*" the threat posed by the subculture and I don't think this way of incorporation applies to the hacker subculture as the hacker subculture mainly exists digitally, on the internet. In cyberspace. The second form of incorporation mentioned by Hebdige, the *ideological form*, seems to be better applicable to the hacker subculture. As became obvious in some of the news articles that I analyzed for this paper, some media tend to portray

hackers as social misfits, outcasts and computer nerds. As people who aren't very good socially and who don't get out much. This can be seen as a way to trivialise the members of the hacker subculture and thus as a form of ideological incorporation.

Douglas Thomas, however, in his book "*Hacker Culture*" explains that hacker subculture has proven incredibly resistant to most forms of incorporation. He explains that through the years the developments in user interfaces for computers have made the gap between the knowledge of how computers work and the end-users bigger and bigger, which actually reinforces the idea of hackers being different because they do possess such knowledge. Thomas explains that yes, there are ways in which mainstream society or parent culture have tried to incorporate the hacker subculture, but that these ways never "defused" or "froze" the threat that the hacker subculture poses to mainstream society. (Thomas 2002) Moreover, and this is crucial to understand media's portrayal of hackers, making sure that hacker subculture kept being seen as a threat, is what sells computer security services and products. Corporations and businesses in the legitimate, mainstream society thus take advantage of the hacker subculture by keeping the idea alive, that they pose a threat. Indeed this could be seen as a form of commodity incorporation, but, it doesn't defuse the subcultures threat to society, it even strengthens the idea of the hacker subculture posing a threat.

Thomas also mentions, just briefly, that some companies, like Microsoft, have tried to trivialise the threat hackers pose. However, this method seems to have been rather unsuccessful. (Thomas 2002)

And so, Thomas's conclusion seems to be that a combination of both the *commodity form* and the *ideological form* are used to incorporate the hacker subculture into mainstream society but that society needs difference between the subculture and parent culture to exist, to be able to successfully incorporate it. Whereas with other subcultures threat is defused, in the case of hacker subculture threat needs to be continuously re-invented and kept alive. Which has allowed the hacker subculture to sustain a powerful form of resistance and to keep its meaning. (Thomas 2002)

5. Conclusions

It has become clear that media in the form of online news articles and Hollywood films and the subculture itself each have different views of the hacker subculture. I feel that it has also become obvious throughout this paper, that several reasons exist why media and hackers themselves have completely different views of the hacker subculture, of who hackers are and what it is that hackers do. Hollywood films seem to portray hackers as people who have an extraordinary understanding of technology and who use this skill to do good. In films hackers are portrayed as heroes.

However, in online news articles a completely different view of hackers is given; that of cyber vandal, digital criminal and social misfit. There seem to be a number of reasons for this.

First there is the problem of semantics. Media and members of the hacker subculture attribute completely different meanings to the words hacking and hackers. Media tend to use the word "*hacker*" as a synonym for cyber vandal, digital criminal and basically any person who uses digital

means to perform criminal or malicious activities. Whereas members of the hacker subculture use the word "hacker" in a more traditional sense, meaning a person who has a thirst for knowledge, who is curious and has a desire to learn and figure out how things work. A definition of the word that resembles that of the older generations of hackers in the 1960's. This also shows a certain ignorance or disinterest of computing and hacker history on the part of mainstream media, since news sources like Wired News do use the term "hacker" in its original meaning.

Secondly, we have seen that mainstream society incorporates subcultures in different ways, to defuse or freeze the threat they pose. And that however, in the case of the hacker subculture, keeping this threat alive, is mainstream society's way of dealing with the subculture. Foreman's article showed that the media are the spokesperson for parent culture / mainstream society and thus it is they (the media) who keep the threat of hackers alive. This was also very clear when analyzing the news articles in the beginning of this paper. Other instances in news articles, where hackers get portrayed as social misfits can be explained by Hebdige's ideological form of incorporation, which means members of a subculture get portrayed as clowns or misfits, to show that they are no threat to society. In the end we should also not forget that although media might be a spokesperson for mainstream society, media also have a product to sell.

Schwartau explains this as follows:

"If you read about hackers in the national media, you get a quite distorted view of what hackers are really about. Only criminal hackers make the front page of the paper, which follows the media dictum, If it Bleeds, It Leads. (...) "The sound-byte-laden popular opinion that hackers are criminals is just plain wrong. (...) you will see that the hacker/techno/computer community is merely an echo of the spectrum of society as a whole. Each with its evil dark side as well as its baldancing and more prevalent benevolent good side."(Schwartau, 2000)

In the end one must wonder whether the media actually have any reason to portray the hacker subculture correctly....

6. Bibliography

Books

Dreyfus, Sulette. Jullian Assange. Underground; Hacking, Madness & Obsession on the Electronic Frontier. (1997)

Hebdige, Dick. Subculture; The meaning of style. (1979)

Levy, Steven. Hackers; The Heroes of the computer revolution. (1984)

Mungo, Paul. Bryan Glough. Approaching Zero; The extraordinary Underworld of Hackers, Phreakers, Virus Writers and Keyboard Criminals. (1992)

Schwartz, Winn. Cybershock: Surviving Hackers, Phreaks, Identity Thieves, Internet terrorists and weapons of mass disruption. (2000)

Sterling, Bruce. The Hacker Crackdown; Law and Disorder on the Electronic Frontier. (1992)

Thomas, Douglas. Hacker Culture. (2002).

Manuscript

Lieberman, Bernhardt. Computer Hackers An intractable problem and what to do about it.

Journal Articles

Forman, Murray. "Betrayal and Fear: Press Coverage of Canadian Skinheads". Canadian Journal of Communications. 17.2 (1992)

Websites

Pitre, Shawn. Cultural Studies & Hebdige's Subculture; The Meaning of Style 07/12/2003
<http://www.mediamusicstudies.net/tagg/students/Montreal/Tendances/PitreHebdige.html>

Löwgren, Jonas. Hacker Culture(s). 23/02/2003.
<http://webzone.k3.mah.se/k3jolo/HackerCultures/newethics.htm>

Middleton, James. Welsh hacker faces jail sentence. 29/03/2001.
<http://www.vnunet.com/News/1119903>

Associated Press. Russian Hacker Sentenced to 3 Years. 08/10/2002.
<http://www.computeruser.com/news/02/10/08/news6.html>

Niccolai, James. Analyst puts hacker damage at \$1.2 billion and rising 10/02/2000.
<http://archive.infoworld.com/articles/ic/xml/00/02/10/000210icyankees.xml>

Two arrested in Wales for credit card theft costing \$3 million 24/03/2000. CNN.
<http://www.cnn.com/2000/TECH/computing/03/24/hackers.wales/>

Glave, James. Cracking the Mind of a Hacker 20/01/1999 Wired News
<http://www.wired.com/news/technology/1,1282,17427,00.html>

Poulsen, Kevin. Modern psychiatry takes another crack at "diagnosing" hackers. 12/06/2000
<https://lists.wi2600.org/pipermail/2600/2000-June/000164.html>

Mentor. The Hacker Manifesto. 1983
<http://www.phrack.org/show.php?p=7&a=3>

Raymond, Eric. Jargon file 4.4.7
<http://www.catb.org/~esr/jargon/>

Capello, Valerio Hacker Being; On the meaning of being a hacker 23/01/2000
<http://www.elfgrin.com/docs/BeingHacker.html>

Stallman, Richard. MEME 2.04

<http://memex.org/meme2-04.html>

Films

Softley, Ian. Hackers. 1995

<http://www.imdb.com/title/tt0113243/>

Robinson, Phil. Sneakers 1992

<http://www.imdb.com/title/tt0105435/>

Gray, Gary. The Italian Job 2003

<http://www.imdb.com/title/tt0317740/>

badham, John. Wargames. 1983

<http://www.imdb.com/title/tt0086567/>

Sena, Dominic. Swordfish. 2001

<http://www.imdb.com/title/tt0244244/>

APPENDIX 1

1. Hacker attacks: You can never be too safe

CNN.com, November 1, 2000

Web posted at: 10:25 a.m. EST (1525 GMT)

Mike Hogan

<http://www.cnn.com/2000/TECH/computing/11/01/security.hackers.idg/>

2. Suspected hacker may face extradition requests

CNN.com, May 9, 2000

Web posted at: 12:49 a.m. EDT (0449 GMT)

<http://www.cnn.com/2000/LAW/05/09/internat.hacking.law/>

3. Computer hacker plants porno on Air Force Web page

CNN.com, December 30, 1996

Web posted at: 4:15 p.m. EST

<http://www.cnn.com/TECH/9612/30/air.force.porn/>

4. Hacker suspect called 'damn good ... and dangerous'

CNN.com, March 19, 1998

Web posted at: 12:33 p.m. EST (1733 GMT)

<http://www.cnn.com/TECH/computing/9803/19/hackers/>

5. Teen hacker faces federal charges

CNN.com, March 18, 1998

Web posted at: 10:40 p.m. EST (0340 GMT)

<http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/>

6. USIA Web site hit by hacker

CNN.com, January 21, 1999

Web posted at: 9:37 p.m. EST (0237 GMT)

<http://www.cnn.com/TECH/computing/9901/21/hackers.usia/>

7. Gates's Viagra hacker sentenced

CNN.com, July 6, 2001 Posted: 8:14 AM EDT (1214 GMT)
<http://www.cnn.com/2001/TECH/internet/07/06/hacker.fbi/>

8. Hacker accesses 5.6 million credit cards

CNN.com, Fred Katayama
Tuesday, February 18, 2003 Posted: 12:16 PM EST (1716 GMT)
<http://www.cnn.com/2003/TECH/02/17/creditcard.hack/>

9. Hacker exposes financial data at Georgia Tech

CNN.com, March 20, 2002 Posted: 8:40 a.m. EST (1340 GMT)
Brian Sullivan
<http://www.cnn.com/2002/TECH/internet/03/20/georgia.tech.hack.idg/?related>

10. Hacker forces banks to cancel Visa debit cards

CNN.com, September 7, 2001 Posted: 8:47 a.m. EDT (1247 GMT)
Dan Verton
<http://www.cnn.com/2001/TECH/industry/09/07/visa.debit.cards.idg/>

11. Jury: Hacker tried to shake down mayor

CNN.com, Thursday, February 27, 2003 Posted: 1454 GMT
<http://edition.cnn.com/2003/TECH/internet/02/27/internet.extortion.ap/>

12. FBI warns companies about Russian hacker attacks

CNN.com, March 8, 2001
Web posted at: 4:00 PM EST (2100 GMT)
<http://www.cnn.com/2001/TECH/internet/03/08/hacker.attacks/>

13. New version of hacker tool on the loose

CNN.com, March 24, 2001
Web posted at: 2:00 p.m. EST (1900 GMT)
Bruce Francis
<http://edition.cnn.com/2001/TECH/internet/03/24/hacker.tool/>

14. Angry hacker releases ISP customer data

CNN.com, January 5, 2001
Web posted at: 9:33 a.m. EST (1433 GMT)
Linda Rosencrance
<http://www.cnn.com/2001/TECH/computing/01/05/angry.hacker.idg/>

15. Government computers: The ultimate hackers' proving ground

CNN.com, March 23, 2000
Web posted at: 8:19 a.m. EST (1319 GMT)
Dan Verton
<http://www.cnn.com/2000/TECH/computing/03/23/hacker.feds.idg/>

16. Hacker steals huge credit card database

CNN.com, December 13, 2000
Web posted at: 10:29 AM EST (1529 GMT)
<http://www.cnn.com/2000/TECH/computing/12/13/credit.cards.com.hacked/>

17. Hacker unleashes updated backdoor program

CNN.com, March 15, 2001
Web posted at: 11:22 a.m. EST (1622 GMT)
By Douglas F. Gray

<http://www.cnn.com/2001/TECH/internet/03/15/updated.subseven.idg/>

18. Microsoft: big hack attack

CNN.com, October 27, 2000: 7:28 p.m. ET
Jamey Keaten
<http://money.cnn.com/2000/10/27/technology/microsoft/>

19. Cracking the hacker underground

BBCi, Last Updated: Friday, 14 November, 2003, 08:50 GMT

Jo Twist

<http://news.bbc.co.uk/2/hi/technology/3246375.stm>

20. US hacker accused of massive fraud

BBCi, Last Updated: Friday, 10 October, 2003, 10:55 GMT 11:55 UK

<http://news.bbc.co.uk/1/hi/business/3180358.stm>

21. Hacker compromised astronaut safety

BBCi, Monday, 3 July, 2000, 01:44 GMT 02:44 UK

<http://news.bbc.co.uk/1/hi/sci/tech/816510.stm>

22. 'Mafiaboy' hacker jailed

BBCi, Thursday, 13 September, 2001, 00:19 GMT 01:19 UK

<http://news.bbc.co.uk/1/hi/sci/tech/1541252.stm>

23. Notorious hacker pleads guilty

BBCi, Saturday, March 27, 1999 Published at 11:54 GMT

<http://news.bbc.co.uk/1/hi/sci/tech/305430.stm>

24. Hacker causes havoc for websites

BBCi, Last Updated: Thursday, 24 April, 2003, 12:07 GMT 13:07 UK

<http://news.bbc.co.uk/1/hi/technology/2967749.stm>

25. Teen hacker avoids jail sentence

BBCi, Last Updated: Monday, 2 February, 2004, 18:06 GMT

<http://news.bbc.co.uk/2/hi/technology/3452923.stm>

26. UK 'hacker' wanted by US

BBCi, Wednesday, 13 November, 2002, 06:06 GMT

<http://news.bbc.co.uk/1/hi/world/americas/2456403.stm>

27. Hacker hits UN website

BBCi, Thursday, 20 January, 2000, 21:36 GMT

<http://news.bbc.co.uk/1/hi/world/americas/612506.stm>

28. Huge piracy ring raided

BBCi, Wednesday, 12 December, 2001, 10:45 GMT

<http://news.bbc.co.uk/1/hi/world/americas/1705436.stm>

29. UK 'hacker' to fight US extradition

BBCi, Wednesday, 13 November, 2002, 16:29 GMT

<http://news.bbc.co.uk/2/hi/americas/2464593.stm>

30. Credit card database hacked

BBCi, Last Updated: Tuesday, 18 February, 2003, 19:30 GMT

<http://news.bbc.co.uk/1/hi/business/2774477.stm>

31. Hacker targets Lloyds site

BBCi, Sunday, 2 January, 2000, 17:15 GMT

<http://news.bbc.co.uk/1/hi/business/588331.stm>

32. Kournikova hacker suspect arrested

BBCi, Wednesday, 14 February, 2001, 14:03 GMT

<http://news.bbc.co.uk/1/hi/world/europe/1170139.stm>

33. Russians arrest 'CIA hacker'

BBCi, Monday, 26 June, 2000, 17:31 GMT 18:31 UK

<http://news.bbc.co.uk/1/hi/world/europe/806984.stm>

34. Suspected hacker bailed in UAE

BBCi, Thursday, 22 June, 2000, 11:05 GMT 12:05 UK

<http://news.bbc.co.uk/1/hi/world/europe/801475.stm>

35. Devious viruses set to grow

BBCi, Wednesday, 28 November, 2001, 11:21 GMT
<http://news.bbc.co.uk/1/hi/sci/tech/1680578.stm>

36. Hacker boys from Brazil

BBCi, Saturday, 22 December, 2001, 08:06 GMT
<http://news.bbc.co.uk/1/hi/sci/tech/1723356.stm>

37. Net thief grabs credit cards

BBCi, Monday, 10 January, 2000, 18:41 GMT
<http://news.bbc.co.uk/1/hi/sci/tech/597828.stm>

38. 'Trojans' open online accounts

BBCi, Thursday, 24 August, 2000, 15:21 GMT 16:21 UK
<http://news.bbc.co.uk/1/hi/sci/tech/894253.stm>

39. Web hackers strike again

BBCi, Saturday, 26 February, 2000, 10:28 GMT
<http://news.bbc.co.uk/1/hi/sci/tech/657783.stm>

40. Welcome to the era of drive-by hacking

BBCi, Tuesday, 6 November, 2001, 13:14 GMT
<http://news.bbc.co.uk/1/hi/sci/tech/1639661.stm>

41. Taliban website defaced

BBCi, Sunday, 26 August, 2001, 16:15 GMT 17:15 UK
http://news.bbc.co.uk/1/hi/world/south_asia/1510440.stm

42. Hacker threats to bookies probed

BBCi, Last Updated: Monday, 23 February, 2004, 18:21 GMT
<http://news.bbc.co.uk/2/hi/technology/3513849.stm>

43. Hackers catch World Cup fever

BBCi, Friday, 23 August, 2002, 09:40 GMT 10:40 UK
<http://news.bbc.co.uk/2/hi/technology/2210186.stm>

44. Q&A: The Bugbear e-mail virus

BBCi, Friday, 4 October, 2002, 11:50 GMT 12:50 UK
<http://news.bbc.co.uk/1/hi/technology/2299303.stm>

45. Questions cloud cyber crime cases

BBCi, Last Updated: Friday, 17 October, 2003, 17:44 GMT 18:44 UK
<http://news.bbc.co.uk/1/hi/technology/3202116.stm>

46. Web worm suspects bailed

BBCi, Friday, 7 February, 2003, 11:18 GMT
<http://news.bbc.co.uk/2/hi/technology/2733657.stm>

47. Can a Hacker Outfox Microsoft?

Wired News, 02:00 AM Oct. 18, 2002 PT
Peter Rojas
<http://www.wired.com/news/technology/0,1282,55807,00.html>

48. Hacker Arrest Stirs Protest

Wired News, 02:00 AM Jul. 19, 2001 PT
Declan McCullagh
<http://www.wired.com/news/politics/0,1283,45342,00.html>

49. Hacker Contest Mostly About Hype

Wired News, 02:00 AM Jul. 08, 2003 PT
Michelle Delio

<http://www.wired.com/news/infostructure/0,1377,59556,00.html>

50. Hacker finds hole in Netscape

Wired News, 04:25 PM Aug. 07, 2000 PT

Farhad Manjoo

<http://www.wired.com/news/technology/0,1282,38087,00.html>

51. Hacker Takes a Crack at TiVo

Wired News, 02:00 AM May. 31, 2003 PT

Elisa Batista

<http://www.wired.com/news/technology/0,1282,59028,00.html>

52. Netherlands No Hacker Haven

Wired News, 02:00 AM Mar. 12, 2003 PT

Daithí Ó hAnluain

<http://www.wired.com/news/digiwood/0,1412,58007,00.html>

53. Norway Cracks Down on DVD Hacker

Wired News, 11:20 AM Jan. 10, 2002 PT

Declan McCullagh

<http://www.wired.com/news/politics/0,1283,49638,00.html>

54. Russian Hacker Charges Dropped

Wired News, 01:38 PM Dec. 13, 2001 PT

Michelle Delio

<http://www.wired.com/news/politics/0,1283,49122,00.html>

APPENDIX III: Questionnaire Data

Statistics											
		sexe	age	relationship	friends	trojans	viruses	ddos	creditcards	defacements	media portrayal
N	Valid	14	14	14	14	14	14	14	14	14	14
	Missing	0	0	0	0	0	0	0	0	0	0

Frequency Table

Sexe					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	male	13	92,9	92,9	92,9
	female	1	7,1	7,1	100,0
	Total	14	100,0	100,0	

Age					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	15,00	2	14,3	14,3	14,3
	17,00	3	21,4	21,4	35,7
	19,00	3	21,4	21,4	57,1
	20,00	3	21,4	21,4	78,6

	23,00	1	7,1	7,1	85,7
	26,00	1	7,1	7,1	92,9
	28,00	1	7,1	7,1	100,0
	Total	14	100,0	100,0	

Relationship					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	6	42,9	42,9	42,9
	no	8	57,1	57,1	100,0
	Total	14	100,0	100,0	

Friends					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	normal	9	64,3	64,3	64,3
	a lot	5	35,7	35,7	100,0
	Total	14	100,0	100,0	

Trojans					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	7	50,0	50,0	50,0
	no	4	28,6	28,6	78,6
	positive	3	21,4	21,4	100,0
	Total	14	100,0	100,0	

Viruses					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	2	14,3	14,3	14,3
	no	9	64,3	64,3	78,6
	no harm	3	21,4	21,4	100,0
	Total	14	100,0	100,0	

(D)Dos					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	3	21,4	21,4	21,4
	no	10	71,4	71,4	92,9
	no harm	1	7,1	7,1	100,0
	Total	14	100,0	100,0	

Creditcards					
-------------	--	--	--	--	--

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	1	7,1	7,1	7,1
	no	11	78,6	78,6	85,7
	no harm	2	14,3	14,3	100,0
	Total	14	100,0	100,0	

Defacements					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	6	42,9	42,9	42,9
	no	8	57,1	57,1	100,0
	Total	14	100,0	100,0	

Media portrayal					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	wrong	14	100,0	100,0	100,0