Meanings that Hackers Assign to their Being a Hacker

Orly Turgeman-Goldschmidt[1]
Bar-Ilan University, Israel

Abstract

This study analyzes the ways in which hackers interpret their lives, behavior, and beliefs, as well as their perceptions of how society treats them. The study was based on unstructured, face-to-face interviews with fifty-four Israeli hackers who were asked to tell their life stories. Analysis of the data reveals differences in the hackers' self-presentation and the extent of their hacking activity. Although these differences imply the importance of informal labeling since childhood, it seems that hackers succeed in avoiding both, the effects of labeling and secondary deviance and that they feel no shame. Furthermore, they structure their identities as positive deviants and acquire the identity of breakers of boundaries, regardless of the number and severity of the computer offenses they have committed.

Keywords: hackers; crackers; hacking; labeling; positive deviant; construction of identity.

Introduction

Computer-related deviance has not been sufficiently studied, especially from the perspective of the perpetrators themselves (Yar, 2005). The present study analyzes the ways in which hackers interpret their lives, behavior, and beliefs, as well as their perceptions of how society treats them. The study examines hackers' life stories that explain who they are and what they do, which provides a deeper, sharper picture on the complexity of the phenomenon than a survey could (Lieblich, Tuval-Mashiach & Zilber, 1998). The focus is on the social construction of deviant identity among hackers and on the meanings they assign to their reality (Charmaz, 2000).

The computer underground forms a worldwide subculture (Holt, 2007; Meyer and Thomas, 1990). The symbolic identity of the computer underground generates a rich and diverse culture consisting of justifications, highly specialized skills, information-sharing networks, norms, status hierarchies, language, and unifying symbolic meanings (Meyer & Thomas, 1990). The "hacker" label is often used to refer to the computer underground as a whole. Hackers have a distinct image, an imagined identity that binds them, even if they never meet each other (Jordan & Taylor, 1998).

But there are also differences between subgroups that are classified depending on their expertise, areas of interest, and behavior patterns (Voiskounsky & Smyslova, 2003). The perplexity surrounding the label "hacker" has to do with the fuzzy definition of the term and the vague boundaries between computer experts and hackers (Jordan & Taylor, 1998), as well as those characteristics that differentiate between various types of hackers. Hackers

[1] Interdisciplinary Department of Social Sciences, Bar-Ilan University, Ramat Gan, 52900, Israel. E-mail: turgemo@mail.biu.ac.il

themselves suggested different terms and meanings to define hackers and hacking (Holt, 2007; Coleman & Golub, 2008). The best-known members of the computer underground are hackers/crackers (usually referring to those who break into computer systems), phreaks (those who use technology or telephone credit card numbers to avoid long distance charges), and pirates (those who distribute copyrighted software illegally). As there are differences in the meaning and practice of being a hacker, it is essential to examine if and how it is represented by differences in the hackers' self-presentation. This research outlines the differences between deviant and less deviant computer hackers.

The term hacker has evolved through the years (Jordan & Taylor, 2004). From the beginning, hacking has raised serious concerns on the misuse of the powerful, new electronic technology (Hannemyr, 1999). Yet, initially the term had connotations of honorable motives of virtuoso programmers overcoming obstacles. Sterling (1992, p. 53) says, "Hacking can signify the free-wheeling intellectual exploration of the highest and deepest potential of computer systems. Hacking can describe the determination to make access to computers and information as free and open as possible." This is hacking as defined in Levy's (1984) history of the computer milieu, *Hackers: Heroes of the Computer Revolution*.

Hacking has evolved into unauthorized access to computer networks (Jordan and Taylor, 1998). The label hacker has acquired has the negative connotation of computer criminal and electronic vandal (Chandler, 1996), a national security threat and a threat to intellectual property (Halbert, 1997). However, Skibell (2002) calls the computer hacker a myth (2002) and stated that few computer hackers possess sufficient skills or desire to commit more than nuisance crimes.

Hackers developed the Internet and personal computers (Wall, 2001), and "it might, in fact, even be suggested that the personal computer would never have existed without the computer hacker" (Chandler, 1996, p. 229). The earliest generations of hackers (Jordan and Taylor, 2004; Levy, 1984) passionately wanted computers and computer systems designed to be useful and accessible to individuals, and in the process pioneered public access. Hannemyr (1999) concludes that the hackers have successfully created several usable and unique software programs, ranging from text editors to the Internet. Furthermore, the open-source movement, an alternative and successful way of developing and distributing software (Ljungberg, 2000), has rooted in the hacker culture since the early 1960s (Levy, 1984). And it seems that in recent years the positive connotation of hacking has been partially returned in connection with the involvement of hackers in the open source movement and their influence on it.

In its short history, the "hacker" label has changed from a positive to a negative one. Most sociological knowledge on the stigma focuses on what Goffman called *information management* rather than on the contested nature of stigma (Kusow, 2004). The focus here is on the contested nature of stigma and show that hackers not only reject the stigma attached to them, but go further and empower themselves as "positive deviants", regardless of their specific practices as hackers. Therefore, the theoretical framework that seems productive for understanding these behaviors is Labeling Theory (Becker, 1963; Lemert, 1951).

Davies and Tanner (2003) contend that labeling theory has three different concerns. The first is secondary deviance: deviant behavior that goes unnoticed, undetected, or hidden is said to be less generative of further deviant behavior than behavior that is publicly sanctioned; the second pertains to the social-psychological effect of labeling, with

labels changing the individual's self-conception for the worse; the third examines the effect of labeling on life opportunities, specifically in the area of employment. These concerns will be addressed in the present paper.

Positive deviance is a controversial term (Goode, 1991), but seems useful for the construction of deviant identity among hackers. Dodge (1985, p. 18) defines positive deviance as "those acts, roles/careers, attributes and appearances… singled out for special treatment and recognition, those persons and acts that are evaluated as superior because they surpass conventional expectations." Heckert (1989), who applies the relationships of labeling theory to positive deviance by examining the labeling of the French Impressionists, claims that the genius or an exceptional athlete should be examined similarly to negative deviants. Becker (1978) has also utilized labeling theory to show how geniuses were once defined as mad. Ben-Yehuda (1990) argues that the label of deviant can be negative or positive, position that is implicit in the labeling approach and more explicit once we accept the relative view of deviance, the negotiated nature, its emergent quality, and fluidity.

Hackers are a good example of Becker's (1963) approach whereby labeling an activity as deviant is based on the creation of social groups and not the quality of the activity itself. Becker (1963) uses the term "outsider" to describe labeled rule-breakers or deviants who accept the label attached to them and view themselves as different from "mainstream."

Method

This study is based on interviews with individuals who constitute a subculture by virtue of their membership in a self-defined subculture. Based on the phenomenological-interpretive approach (Geertz, 1973), the objective of this research is not to reveal the actual reality but to describe how self-defined hackers' experience, explain, and interpret reality.

The starting point for this study was the grounded theory (Strauss, 1987; Strauss and Corbin, 1990, 2000), a data-driven method that produces theoretical propositions and concepts, and systematically processes them. The outcome of grounded theory is "a social construction of the social constructions found and explicated in the data" (Charmaz, 1990, p. 1165). In this respect, the researcher's text is itself an interpretive structuring of reality. The hackers' narrative are reconstructions of experience, they are not the original experience itself (Charmaz, 2000).

Table 1: ***Locating Interviewees***

Media reports (one interviewed on TV show, and the rest were interviewed in magazine reports)	7
Israeli hacker conferences (one called Movement, a demo scene party, and the other called Y2Hack)	5
Israeli conference about information security	1
Through the Internet (arranging a face-to-face interview in ICQ)	2
Other informants (journalists, a radio broadcaster, and the owner of a computer company)	6
Interviewees approached me when I was lecturing on computer crime (each at a different lecture)	2
Acquaintances and family members and friends	6
Snowball or chain referrals; I asked interviewees to refer me to others	25

Finding interviewees required intensive efforts to establish connections and make the acquaintance of various informants and of suitable potential interviewees (see table 1). The interviews were conducted in 1998 and 1999, yet it seems that they are still meaningful as

the practices and perceptions which were reported by the interviewees coincide with reports on hackers today. The interviews were conducted in the hackers' homes or in public places such as coffee shops, according to the interviewee preference. I took notes during the interviews, recording the words of the interviewees almost verbatim. Each interviewee assigned an identification number, without any identifying details.

Fifty-four unstructured, in-depth, face-to-face interviews were conducted with Israeli self-defined hackers using the narrative interview technique (Rosenthal & Bar-On, 1992). The interviews lasted an average of three hours (the shortest was two hours, the longest eight). At the end of the interview I asked whether there was anything they wanted to add or felt that they had missed, then thanked them and ended the session. Later, usually the following day, I sent them a thank you note (by email). Many of the interviewees responded positively. For example, Eran (all names are fictitious) said, "One of the reasons for sitting here and talking to you today was the opportunity to recall, think, and understand. Each of these conversations is an introspection, which eventually helps me understand myself."

Having established a robust set of categories that covered the hackers' self-perceptions and behaviors, and uncovered their life stories, a series of theoretical propositions was generated (Strauss & Corbin, 1990). These propositions started from a conjecture or an idea (jotted down as memos), based on relationships between categories and sub-categories, for example between general behavior patterns and hacking activities. I tested these theoretical propositions by constantly referring back to the data for impressions.

Table 2: ***socio-demographic characteristics of interviewees***

Variable	Frequency
Gender	Female 5.5%, Male 94.5%
Age	Range 14-49 years, Avg. age 24 Common age group 20-30
Marital status	Single 78%, married 13%
Education	12 years and above 74%
Income	Above average 74%
Origin	European or American 74%
Religion	Secular 83%

Fifty-one of the fifty-four interviewees were men (see table 2). Only six reported having a criminal record, five of which were computer related. The interviews provided an opportunity to study successful lawbreakers outside an institutional context (uncaught deviants). The interviewees tended to be young, single, educated, above average income, of European or American origin, and secular. This profile is consistent with the literature, which reports that hackers are mostly non-violent, white, young, middle or upper class men with no criminal record (e.g. Hollinger, 1991).

Different Meanings that Hackers Assign to their Being a Hacker

The self-defined hacker in this study is someone who commits any of the 12 computer offenses in one or more of the following three areas:

(1) ***Software piracy*****:** unauthorized duplication of pirated software; unauthorized distribution of pirated software, cracking software or games, selling cracked-pirated software

(2) ***Hacking*:** unauthorized accessing of computer systems, using illegal Internet accounts; development and/or distribution of viruses, browsing or reading other users' files, stealing computer-stored information, causing computer systems to crash, using stolen credit cards from the Internet
(3) ***Phreaking*:** cracking the phone network mainly to make free long-distance calls. These offenses are similar to those identified by Hollinger (1988), who differentiated between pirates, browsers, and crackers who had the most technical ability and were the most serious abusers, as well as to the offenses studied by Rogers, Smoak, and Liu (2006). These offenses match the attacks detected by the 2006 CSI/FBI survey (e.g., unauthorized access to information, system penetration, theft of information, and sabotage).

Hackers assign different meanings and interpretations to operating as a hacker. They showed different self-presentation according to differences in the variety and extent of their hacking activities. The reported differences are manifest from early childhood through adulthood. Those who reported mischievous behavior since childhood (not related to computers), and presented themselves as talented and gifted since childhood, committed statistically significantly more numerous and diverse computer offenses (practicing piracy, hacking and phreaking) than those who reported normative good behavior and who did not report as diagnosed with high intellect (for the full analysis see Turgeman-Goldschmidt, 2002). In other words, the "bad" hackers (also referred to as crackers) were much more likely to present themselves as having a wild and gifted persona, than the "good" hackers who reported good behavior since childhood.

The hackers' report of computer-related or hacking activities fits their basic self-image. Kevin Mitnick, perhaps the most famous hacker, also describes his desire and ability to learn and discover going back to his childhood (Mitnick & Simon, 2002). The actor fits "his/her self into the dominant character of the situation or structure: adjusting to an obdurate reality" (Fine, 1993, p. 78). These moral constructions are precarious social constructions rather than essences. Gad, for instance, portrayed himself as the eternal iconoclast, mentioning having quit his BA studies and an advertisement course, and frequently changed jobs. He states, "I don't like to do things that I have to". However, a careful look into his life story reveals that he successfully completed several serious undertakings like, schooling, a scriptwriter course, and military service as an officer. Gad, as others, chooses to construct his life story around a certain theme, as a non-conformist and eternal iconoclast. As Stryker (1968) contends, individuals with highly salient identities enact these identities over others that are less salient, even when both may be appropriate in a given situation.

"Good" Hackers

The hacker term was originally defined as:
1. A person who enjoys learning the details of computer systems and how to stretch their capabilities, as opposed to most users of computers, who prefer to learn only the minimum amount necessary.
2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming (Raymond, 1991). *Ami*, a 19 year old, third-year student of computer science, working at the computer help desk of a university, describes what it is like to be a hacker:

> I define myself as a hacker. A hacker can cope with technical details… A hacker is someone with: a knack for the technical, usually having something in connection with

computers, someone who has the ability to improvise and be resourceful... It's not a matter of breaking the law. It's a fact that there's this system and you can manipulate it.

Although *Ami* clearly sees himself as a hacker, he does not perceive hacking to necessarily include unauthorized penetration of computer systems (break-in) or viewing others' files without permission, but as having technical capabilities. He says, "It is not just the end result - the maximal change in improving software, but how you got there." By referring to programmers who demonstrate virtuosity in their ability to overcome obstacles, his usage of the term "hacker" differs from the prevailing definition and matches the previous usage (Levy, 1984).

As computer hobbyists, the good hackers described their development and progress in computers as the natural outgrowth of their basic good identities. Ami suggests a positive connotation of the term hacker: a computer technology expert who "does the impossible," proves his/her ability and superior expertise, and belongs to an elite subculture of experts in the field who are leading society toward a better technological future. According to the metaphor used by Na'ama, who practiced only authorized hacking, hackers see themselves as deviants who ultimately became leaders: "I like the image of ants; there are those that join a trail and those that leave the trail. That's always been my image of the marginal types, who are actually those who discover alternative paths, and thanks to them the rest of society discovers alternative paths."

Good hackers have been involved primarily in copyright violations such as copying and distributing software. Although they negotiate their label by using a moral construct, they are usually involved in software piracy to a higher extent and with a greater commitment than non-hackers individuals. As Ami said, "I feel a moral commitment to screw Microsoft." In Idan's words, "It's the way to a better world not letting companies like Microsoft control the market."

Furthermore, as their narratives reveal, they have usually tried both hacking and phreaking, but were not interested in ongoing break-in career. "Technically, I know how and could actually penetrate a remote computer belonging to someone else, but I have no reason to do so. I'm not interested," says Ami. Yoni tells of a break-in he committed once just to see what it was like. "Before I knew what it was like, like lots of kids, I thought it was cool." This sheds light on the process of becoming a hacker, which is not only a matter of technical learning but one must learn to enjoy it. As Becker (1953, p. 235) said about marijuana users, "the motivation or disposition to engage in the activity is built up in the course of learning to engage in it and does not antedate this learning process." Yoni, who also reported having written viruses to learn a new skill, says: "What made me stop [break-in] was not because I cared what people think, I simply lost interest in it. I can laugh afterwards at someone who wasted his time, when I didn't." In Becker' words, during the sequence of his social experiences, Yoni has not acquired a conception of the meaning of break-in activity, which makes it desirable.

The stories sometimes touched upon morality. Udi, who talked about the fun in doing the impossible with computer systems, was raised as an orthodox Jew. "Much of my religious life still remains in me with respect to values. The fact that I've never committed a crime may be related to this. I'm a good boy, in whom the good side survived." Udi did not acquire the perceptions and judgments of unauthorized hacking that make the activity desirable. Rogers et al. (2006) found that self-reported computer deviants scored lower on social moral choice than non-computer deviants, yet when Rogers, Seigfried and Tidke (2006) replicated Rogers's study they failed to find any significant effect for moral choice.

The good hackers remain open to finding alternatives to penetrating computer systems, in order to achieve their desire for recognition (Taylor, 1999). Good hackers do not feel the desire to engage in computer break-in because they are usually engaged in other activities that yield the same results, recognition and esteem for their abilities. They are engaged as gamers or as demo sceners. Demo is a short, computer-generated multimedia production that demonstrates its creator's talent and creativity in computer music, graphics, and animation. For example, Yoav, an 18 year old, who is about to be drafted into the army's Intelligence Corps, achieved recognition for his activities as a gamer when he invented and produced a network game that gained inspired admiration: "We eventually turned it into a film with a plot and an ending, we released it, and people liked it. It made us very popular."

"Bad" Hackers

The bad hackers described themselves as having a wild and gifted persona. They described their computer-related activities as a natural outgrowth of their childhood behavior. Their mischievous image followed them through childhood, school, military service, work, and so forth. Hackers, like others, seek to have their identities verified by others, whether the identity is positive or negative (Swann, Wenzlaff, and Tafarodi, 1992). Whereas good hackers are involved as gamers or demo sceners, the bad hackers are members of hacking or cracking groups.

Meir, a 24-year-old founder of a high-tech start-up, reported committing eight types of computer offenses in the areas of software piracy, hacking, and phreaking. He mentioned testing into genius range as a child, his effortless science-related capabilities, and his ability to "rapidly assimilate information is a gift from God if there is one, or maybe from my parents". Meir portrayed himself in various contexts as mischievous. At school "they were always sending notes home to my parents. I was considered as one of the troublemakers. Not disturbed but misbehaved. I wouldn't do my homework, I would cut classes or make a mess in the computer lab or hack into the school's computers." In the army too, "I was a terrible conscript. I blew off my commanders, and there was nothing they could do." He attributed his being different and special both to original thinking ("Lots of people think I'm strange") and to original actions, such as having a tattoo in an unusual place on his body. He wanted to convey that he was not an ordinary person. "I like the fact that I'm different, I'm more in love with myself for having done the impossible".

Neli, a sixteen year-old, describes the process of becoming a hacker as part of the progress he made in computer knowledge, describing achieving a university degree and hacking into a website in analogous terms: "My approach has always been that, if someone else can do it, so can I. That's been my motivation ever since I can remember. If others can finish university in three years, so can I. If others can hack into Web sites and sabotage them, so can I. After a while, the excitement fades and you go on to something else." Neli moved on to cracking computer systems as a 'sneaky thrill' (Katz, 1988, p. 53). Katz views young property criminals as committing sneaky crimes for the thrill; hackers take on hacking as a social entertainment that usually excites them (Turgeman-Goldschmidt, 2005). Hacking becomes just another skill to acquire, if not the most exciting one as far as they are concerned. Neli first expressed his excitement in building websites, then studying programming, and eventually hacking. According to him,

> Hacking was the thing that's taken me the longest to learn. The nicest thing was simply finding the answer. That's the thing that excited me the most, and for one reason:

> HTML. You create and change things that are yours, you recreate yourself. You control something outside yourself. It creates a feeling. It's incredible. You have access and the door's wide open. The possibility to change and destroy others—you, yes, you! It's a turn-on. It is the exact opposite of being in a mall where you want a certain store to open and another one to close. You can, and it's soooo nice.

Like others, Neli disavows the label of deviant and negotiates his identity by portraying hacking as just another realm to conquer, that is, demonstrating mastery and knowledge. Neli chooses to portray himself as a troublemaker ("the bad boy, the wild child, whatever you want to call it") who is academically successful without even trying. But beyond disavowing the label of deviant, Neli negotiated his identity as morally "better" by choosing the target, which is penetrating computer systems of Israel's enemies, such as the Hamas and neo-Nazis. He portrays himself as a guardian of the state. He says, "I see myself the state's guardian. If the government isn't doing anything, I feel I should, and I do something." His story was in the papers, and received a lot of attention:

> First of all, I didn't go to school on the first day because I was all over the papers. When I went to school everyone asked, "How's it going?" even though they knew all about my whereabouts and what I had been up to. Students pointed at me stating, "I saw you on television. It was like a party. The whole school was really nice to me. I had to turn the kids away, they were all over me". Their admiration was deserved because I did something unique, I learned something specific, so why not? I know it probably sounds like I'm full of myself, but according to the Walla [an Israeli portal] poll, they admired me for it. Except for a scathing article against me in Ma'ariv l'Noar [a teen magazine], most of the coverage was supportive. I like to make a scrapbook of all of the articles. After the publicity I got, it gained momentum.

Neli's story is an excellent example of the experienced fame and recognition that go with hacking in the hackers' eyes, even when it crosses the publicity line from being news among hackers to the general public domain. Neli, who regularly committed computer offenses, won fame for his hacking activities. He also succeeded in translating fame and recognition into a different type of prestige by accepting an after-school job at a leading computer company.

Arik, a 22 year old student, who learns how to write viruses "only as a technical part of understanding," says, "Another common denominator of this underground is that what motivates us is not money. We despise commercialism. What motivates us is the fame and prestige that one receives." It seems that this motivation distinction enables hackers to feel superior tin comparison to traditional criminals.

Indeed, the manner in which hackers' activities should be treated has become blurred and uncertain. Sometimes, society functions as a reinforcing spawn factor of deviance for which at least the informal sanctions are more positive than negative (as in Neli's example). Occasionally, even formal reactions are positive. Yaron, the 30-year-old owner of a successful information security company, says, "The judge saw things the right way, unlike the police. A successful, talented kid who committed a prank, not for profitable gain," letting Yaron off with no punishment, and with a "recommendation from the judge." Yaron explains, "Compared to the other less sophisticated criminals, computer criminals get more sympathy. There's a certain favor for sophistication." It seems that Yaron's experience with labeling enabled him to succeed later in life, and to avoid secondary deviance, although he was initially labeled as a deviant.

When the Israeli Analyzer (Tenenbaum) penetrated the Pentagon, the headlines labeled him "The Israeli Computer Genius," and a degree of admiration and awe was discernible even amongst journalists. Israeli leaders also viewed him as a hero. The then Prime

Minister Benyamin Netanyahu called him superb, Industry and Trade Minister then, Dalia Itzik, said he is a wizard who should not stand trial because his knowledge could aid the state.

Exit (or Semi-Exit) from the "Bad" Hacking World

In most situations of loss, such as a change related to a loss of personal ability, individuals look for means to preserve their former identities or to establish new ones in order to regain a sense of continuity (Charmaz, 1994). Studies conducted on individuals who were "exiting the deviant career" focus on identifying the process whereby deviant individuals abandon certain behaviors, ideologies, and identities by replacing them with occupations in professional counseling (Brown, 1991). Brown claims that 'ex-deviants' do not 'leave it all behind' (p. 227) in order to replace their lifestyles with more conventional lifestyles, values, beliefs, and identities, but rather use remnants of their deviant background as explicit strategies for their occupations. In this regard, ex-hackers also suggest that ex-deviants tend not to shed or forget their pasts but reinvent them by transforming them into social capital that is, proclaiming membership in a group – which provides each of its members with the backing of the collectivity-owned capital. A "credential" which entitles them to credit, in the various senses of the word (Bourdieu 1986, p. 248). Meir, an ex-hacker, certainly does not "leave it all behind" (Brown, 1991):

> Once you know that everything's possible, it takes your desire away. The fact is that it no longer excites me… Hacking grew out of a high degree of expertise, from an attitude of "as hard as you try, you'll never be able to do it." It's truly a war. A lot of respect is at stake. It's competitive, the most competitive of people competing against each other. It's like two opposing countries' armies. Once I worked for an antivirus company. It was for my own interests, since I liked being the bad guy and engaging in [viruses]. At one point in time it was for fun. Now I just crack stuff that I need. I hack, but lawfully. I try to find the loopholes. The law places obstacles in my path, so I go around them. There are levels of risk that I used to take, but I don't today, and there are principles that you don't violate. Occasionally I'm tempted to hack into the Interior Ministry to see if the owner of my friend's apartment is the real one because certain things there look suspicious. But it's not out of evil intent, I do it only when there's no other recourse. Today, it's a profession. I do it because I need to, not for the same reasons I used to.

Meir explains this change in motivation as a moral responsibility that he did not feel previously, but it is also the result of a lack of interest that follows from the status definition of his role and from the burnout that now characterizes hacking. To this day, he perceives various hacking activities as legitimate, and therefore has not undergone a serious transformation. Ex-hackers occupying professional positions carefully consider the risks involved in hacking activities. There are, says Meir, "levels of risk that I once took but don't anymore." Moreover, the pleasure that accompanied committing computer offenses diminishes with time, particularly as hackers feel that they have reached the apex of their technical abilities: "There's no longer the fun of 'I can do it.' At the same time, their computer expertise remains. Hackers treasure this expertise, and sometimes check that it is still up to date. Ex-hackers still use their hacking skills when the need arises, albeit for different purposes, such as obtaining information that others cannot, or gaining an advantage over a competitor.

Ex-hackers are hackers who grew up, joined the establishment, and hold respected, lawful positions, in most cases owing precisely to their hacking abilities. Their crossing over to lawfulness is external and structural. They perceive themselves as especially gifted

people whose acts, branded by the law as computer crimes, do not cause damage and fall under the definition of pranks or mischief. They have no moral problem with hacking itself or with their status as ex-hackers. Consequently, their life stories are not those of reformed criminals but of heroes who gained the type of social recognition that places them at center stage. Fine (1986) maintained that as children grow older they view their former "dirty play" (such as aggressive pranks, sexual talk, and racist remarks) as morally offensive rather than fun. Contrary to claims by Arluke (2002) and Fine (1986), none of the ex-hackers present themselves as feeling guilty about their former hacking activities.

As Hollinger (1993) assumed, outsider hackers eventually become inside workers. The distinction between criminal hackers and hired ones is based on the perception that hired hackers are employed "to conduct hacking attacks to test security, while criminal hackers literally violate the law" (Jordan and Taylor 1998, p. 771). The computer security industry benefits from the hackers' technological knowledge, which motivates hackers to act. They had pursued and found social recognition and status in the hacker subculture (see also Holt, 2007), which had won them a coveted place in its hierarchy. Now they seek and obtain recognition in society, which offers them a profession with a high socio-economic status as ex-hackers. Says Omer: "You still look for and receive recognition, but in a different way."

Shared Meanings that Hackers Assign to their Being a Hacker

Regardless of the number and severity of the computer offenses they had committed, I found that both good and bad hackers explain their practices in terms of: "breaking boundaries", "shattering conventions" and "doing the impossible". It is known that hackers do not view themselves as criminals but as adventurers (c.f., Jordan and Taylor, 1998, 2004; Taylor, 1999). Yet, they all portray themselves in the same manner; as technological wizards, who break boundaries, adding new contribution to our knowledge regarding the differences between hackers. Both good and bad hackers perceived themselves positively, capable of insight into what "regular people" cannot grasp about that mysterious box called computer.

Many interviewees talk about the positive reaction their computer hobby has produced. Some even aspire to be hackers mainly to gain the prestige and mystery that surround hackers. Individuals learn how to classify the objects they come in contact with from interaction with others. In this process, they also learn how they are expected to behave in reference to those objects (Stryker, 1980). Dan says, "Maybe the drive [to learn computers] came from the environment. It contains a dimension of uniqueness. Also with in the milieu they treated those who dealt with computers as geniuses."

Hackers view hacking or penetrating computer systems as "pushing outside the envelope" or "breaking boundaries." Yif'at, a 19 year old female soldier, perceives hackers as ambassadors of intelligence, with the ability to oppose the establishment in a proactive manner. She can teach us about the desire to become a hacker, as she believes that,

> The thing about hacking is the excitement, the adrenaline, the fun of doing something illegal, unlawful. Like when we were kids, a group of us friends would wait together outside a mini-market and steal hot buns and cartons of chocolate milk. The fun is in the subversive act, in rebellion for its own sake. I don't think that governments and institutions should keep secrets and information from the public. Information should be free. So it's also a matter of principle. It's showing that I'm smarter, I'm in control, and I'll triumph over you. Learning hacking is the cutting edge. It's where the world is going, it's important. It counts as it's a good job, and a great living. It's knowledge.

> Today, women are learning computers because it's good money. The information is all there. It's for real. For example, the Analyzer, look what a good job he has. Hacking is doing the impossible, the unexpected, and the fun stuff. It's also a matter of proving that you can. In every area of my life, I like to test the limits, to go as far out on the edge as I can, and not bend to external restrictions.

Yif'at's words exemplify three of the general characteristics of symbolic interactionism (Blumer, 1969). Yif'at interacts with friends who feel and behave alike. Her response to this behavior is based on meaning and interpretation, in this case attributing positive meaning and interpretation to hacking activities. Hacking is perceived as a way not to bend to external restrictions, as the cutting edge, a good job, and "also a matter of principle" (information should be free). Ami, a good hacker, explains why hackers perceive themselves as capable of doing the impossible. It is, "Because of the breaking of boundaries. It's almost mystical, like a secret society with a certain aura. Security captures the imagination of the public. It is all about being smarter than the next guy ".

Their ability to hack is the key to a secure career path that promises status and respect. Indeed, the Analyzer is now a founding partner in a high-tech company that specializes in computer security. While labeling may restrict access to legitimate job networks (Davies and Tanner, 2003), hacking may be a rare instance in which a criminal record serves as a "resume" for gaining entry in legitimate, profitable, and respected occupations. This "occupational retrofitting" seems to support the idea that the line between hero and criminal is thin (Ben-Yehuda, 1992, p. 80).

Discussion

This study focused on the entire life story of the participants in a holistic way rather than on the object matter alone (hacking). The study enables us to learn the way in which hackers perceive themselves and how they think that others perceived them since childhood. The bad hackers (also referred to as crackers) presented themselves as having a wild and gifted persona, while the good hackers reported good behavior since childhood. The present study advances our understanding by showing that hackers base their current hacking practices (good or bad, authorized or not) on the way in which they perceive themselves and on their notion of how others perceived them since childhood (good vs. wild and gifted).

This analysis advances our knowledge on the differences between those hackers who practiced unauthorized penetration to computer networks and those who do not. As a social identity, the process of becoming a hacker could therefore be seen as a socially negotiated passage from primary to secondary deviance (Lemert, 1951). Cooley (1902) said that individuals' feelings about themselves are products of their relationships with others that have affected them since early childhood. This study has shown the importance of the informal early labeling of deviant individuals in addition to the formal labeling process.

Yet a process of social learning must take place in a context of social interaction to commit a computer illegal act (Skinner and Fream, 1997). The social construction of reality among hackers results from a process in which "the person develops a new conception of the nature of the object" (Becker, 1953, p. 242). The Analyzer said on a talk show, "Hacking is not something in your personality, it's a hobby." Not all those who possess the technical knowledge to hack have learned the "fun" of break-in, therefore they refrain from doing it.

Although shame is a key element in the labeling process (Hayes, 2000), the present study shows that hackers feel no shame, and this applies both for good and bad hackers. Even their crossing over to lawfulness is external and structural. They hold respectable positions, in most cases owing precisely to their hacking abilities, and none of them profess any guilty feelings about their former hacking activities. Indeed, the "possible relevance of labeling theory to behaviors that are not highly visible or easily stigmatized, challenges social scientists to discover how, if at all, labeling theory evokes social definitions of deviance and illuminates self-definition and feelings of potentially stigmatized individuals" (Hayes, 2000, p. 29).

Hackers construct themselves as positive deviants. They do so by portraying themselves as "extraordinary people" who are smarter than others, display unusual or superior behavior or a trait that is rewarded as such (Heckert, 1989), or see themselves as agents of social change (Ben-Yehuda, 1990). The manner in which hackers construct themselves as positive deviants is likely to be based partly on the historical change in the connotation of the hacker label, but also on their backgrounds. Hackers come from the established stratum of society, and social status mediates stigma differentially (Riessman, 2000). Furthermore, hackers contend that deviance constitutes a challenge to social conventions, leading to a legitimate debate about moral boundaries. As Bar says, "If there is a software that can make someone in the world do something good, why should he be deprived of it?" Perhaps this is why it is difficult to view them as criminals in the negative sense (Weisburd, Waring & Chayat, 2001).

The finding, that all the respondents portray themselves as technological wizards, breakers of boundaries, regardless of the number and severity of the computer offenses they had committed, is very intriguing and shows that hackers assign the "computer expert" label as "master status" (Becker, 1963) rather than the deviant label. Gil says, "In my eyes everything adds up, I mean between playing computer games, and being a Linux hacker, and being a cracker. Actually, all of these acts stem from the same place, the will to learn, to know, and the good feeling and satisfaction that this knowledge gives me." Future research could benefit from following quantity examination of the sociological differences between computer deviants and non-deviants.

Thus, the current study has shown that hackers, who are not easily stigmatized, succeed to avoid the effects of labeling and manage to avoid secondary deviance. Contrary to labeling theory, their self-conception does not change for the worse (if anything, it changes for the better), and their life chances in the domain of employment do not decrease (if anything, they increase). This particular kind of deviance illustrates that the labeling process is more complex than its portrayal in labeling theory and requires further inquiry. Of special interest are the conditions under which the process takes place and the directions it can take. Hacking, for example, seems to be a type of deviance where the labeling process works in the reverse direction.

Some of the limitations of the present study can be addressed in the future. The study was carried out in Israel years ago. Voiskounsky and Smyslova (2003, p. 173) claimed that hacking is a universal activity, showing few (if any) differences. The Israeli hackers' characteristics seem to be similar to those of hackers in other western societies. For example, Kevin Mitnick, perhaps the most famous hacker, also describes his desire and ability to learn and discover going back to his childhood (Mitnick and Simon, 2002). Holt (2007) found that a hacker's identity is built on knowledge and devotion to learn. Although the nature of cyber-crime is constantly changing, the basic characteristics of this

kind of hackers, such as their not-for-profit motivation persists and are similar to those described in the present paper. Woo, Kim, & Dominick (2004) found that 70% of the web defacement by hackers was pranks, while the rest had more political motives. We frequently hear about hackers who attack computer sites for ideological reasons. Recently for example, Russian hackers are attacking Georgian websites, and another hacker used a Trojan horse to hack into the computers of Bloomsbury Publishing to discover text of the new Harry Potter book before its publication.

References

Arluke, A. (2002). Animal abuse as dirty play. *Symbolic Interaction*, 25, 405-430.

Becker, G. (1978). *The mad genius controversy*. London: Sage.

Becker, H. (1963). *Outsiders*. Glencoe: Free Press.

Becker, H. (1953). Becoming a marijuana user. *American Journal of Sociology*, 59, 235-242.

Ben Y., N. (1990). Positive and negative deviance: More fuel for a controversy. *Deviant Behavior*, 11(3), 221-243.

_____. (1992). Criminalization and deviantization as properties of the social order. *Sociological Rev*iew, 40(1), 73-108.

Blumer, H. (1969). *Symbolic Interactionism*. Englewood Cliffs, NJ: Prentice-Hall.

Bourdieu, P. (1986). The forms of capital. In J. G. Richardson (Ed.), *Handbook of theory and research in the sociology of education* (pp.241-258). New York: Greenwald Press.

Brown, J. D. (1991). The professional ex-: An alternative for exiting the deviant career. *Sociological Quarterly*, *32*(2), 219-230.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law*, *24*(2), 229-251.

Charmaz, K. (2000). Grounded theory: Objectivist and constructivist methods. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp.509-536). Thousand Oaks, CA: Sage.

Charmaz, K. (1994). Identity dilemmas of chronically ill men. *Sociological Quarterly*, *35*, 269–288.

Charmaz, K. (1990). Discovering chronic illness: Using grounded theory. *Social Science and Medicine*, *30*, 1161-1172.

Coleman, E. G. & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*, 255-277.

Computer Security Institute and Federal Bureau of investigations, (2006). *CSI/FBI Computer crime and security survey*. Available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Cooley, C. H. (1902). *Human nature and the social order.* New York: Scribner.

Davies, S., & Tanner, J. (2003). The long arm of the law: Effects of labeling on employment. *The Sociological Quarterly*, *44*, 385-404.

Dodge, D. L., (1985). The over- negativized conceptualization of deviance: A programmatic exploration. *Deviant Behavior, 6*, 17-37.

Fine, G. A. (1993). The sad demise, mysterious disappearance, and glorious triumph of symbolic interactions. *Annual Review of Sociology*, *19*, 61-87.

Fine, G. A. (1986). The dirty play of little boys. *Society*, *24*, 63-67.

Geertz, C. (1973). *The interpretation of cultures*. New York, Basic Books.

Goode, E. (1991). Positive deviance: A viable concept? *Deviant Behavior*, *12*(3), 289-309.

Halbert, D. (1997). Discourses of danger and the computer hacker. *The Information Society*, *13*, 361-74.

Hannemyr, G. (1999). Technology and pleasure: Considering hacking constructive. *Firstmonday, Peer-Reviewed Journal on the Internet*, *4*(2).

Hayes, T. A. (2000). Stigmatizing indebtedness: Implications for labeling theory. *Symbolic Interaction*, *23*, 29-46.

Heckert, D. M. (1989). The relativity of positive deviance: The case of the French impressionists. *Deviant Behavior*, *10*(2), 131-144.

Hollinger, R. C. (1988). Computer hackers follow a Guttman-like progression. *Sociology and Social Research*, *72*(3), 199-200.

Hollinger, R. C. (1991). Hackers: Computer heroes or electronic highwaymen? *Computers and Society*, *21*, 6-17.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal*, *4*(1), 2-12.

Holt, T. J. (2007). Subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behav*ior, *28*(2), 171-198.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *Sociological Review, 46*(4), 757-780.

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyberwars: Rebels with a cause?* London: Routledge.

Katz, J. (1988). *Seductions of crime*. New York: Basic Books.

Kusow, A. M. (2004). Contesting stigma: On Goffman's assumptions of normative order. *Symbolic Interaction*, *27*, 179-197.

Lemert, E. W. (1951). *Social pathology*. New York: McGraw-Hill.

Levy, S. (1984). *Hackers*. Harmondsworth: Penguin.

Ljungberg, J. (2000). Open source movements as a model for organising. *European Journal of Information Systems*, *9*, 208-216.

Lieblich, A., Tuval-Mashiach, R., & Zilber, T. (1998). *Narrative research: Reading. analysis, and interpretation*. California: Sage Publications.

Meyer, G., & Thomas, J. (1990). The baudy world of the byte bandit: A postmodernist interpretation of the computer underground. In F. Schmalleger (Ed.), *Computers in criminal justice* (pp.31-67). Bristol (Indiana): Wyndham Hall.

Mitnick, K., & Simon, W. L. (2002). *The art of deception*. Wiley and Sons.

Raymond, E. S. (Ed.). 1991. *The New Hacker's Dictionary*. U.S.A.: The MIT Press

Riessman, C. (2000). Stigma and everyday resistance practices: Childless women in south India. *Gender and Society, 14*, 111–135.

Rogers, M., Smoak, N. D., & Liu, J., (2006). Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior. *Deviant Behavior*, *27*, 245-268.

Rogers, M. K., Seigfried, K., & Tidke, K., (2006). Self-reported computer criminal behavior: A psychological analysis. *Digital Investigation, 3*, 116-120.

Rosenthal, G., & Bar-On, D. (1992). A biographical case study of a victimizer's daughter's strategy: Pseudo-identification with the victims of the holocaust. *Journal of Narrative and Life History, 2*(2), 105-127.

Skibell, R. (2002). The myth of the computer hacker. *Information, Security and Society, 5*, 336-356.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*(4), 495-518.

Sterling, B. (1992). The *hacker crackdown: Law and disorder on the electronic frontier*. London, Viking.

Strauss, A. L. (1987). *Qualitative analysis for social scientists*. New York: Cambridge University Press.

Strauss, A. L., & Corbin, J. (1990). B*asics of qualitative research: Grounded theory procedures and techniques*. London: Sage.

_____. (2000). Grounded theory methodology: An overview. In N. K. Denzin & Y. S. Lincoln (Eds.). *Handbook of qualitative research* (pp.273-285). Thousand Oaks: Sage.

Stryker, S. (1980). *Symbolic interactionism: A social structural version*. Menlo Park: Benjamin Cummings.

Stryker, S. (1968). Identity salience and role performance. *Journal of Marriage and the Family,* 4, 558-564.

Swann, W. B. Jr., Wenzlaff, R. A., & Tafarodi, R. W. (1992). Depression and the search for negative evaluations: More evidence of the role of self-verification strivings. *Journal of Abnormal Psychology*, *101*, 314—317

Taylor, P. A. (1999). *Hackers: Crime and the digital sublime*. New-York: Routledge.

Turgeman-Goldschmidt, O. (2002). *Becoming deviant: The social construction of computer deviants (hackers, crackers, and others).*" Unpublished doctoral dissertation, Hebrew University of Jerusalem.

_____. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review*, *23*, 8-23.

Voiskounsky, A. E., & O. V. Smyslova, (2003). Flow-based model of computer hackers' motivation. *CyberPsychology & Behavior, 6*, 171-180.

Wall, D. S. (ed.), (2001). *Crime and the internet*. Routledge: London.

Weisburd, D., Waring, E., & Chayat, E. (2001). *White-collar crime and criminal careers*. Cambridge: Cambridge University Press.

Woo, H., Kim, Y., & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology*, *6*(1), 63-82.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *Howard Journal of Criminal Justice, 44*, 387-399.