From cybercrime to cyborg crime

van der Wagen, Wytske

Chapter 3

The other 'others': an explorative study of the processes of labelling of, by and among hackers*

* Published in Dutch as: Van der Wagen, W., Althoff, M. & Van Swaaningen, R. (2016). De andere 'anderen'. Een exploratieve studie naar processen van labelling van, door en tussen hackers. *Tijdschrift over Cultuur en Criminaliteit*, 6(1), 27-41.

Abstract

While in the sixties hackers were the heroes of cyberspace, they are nowadays often perceived as the archetype cybercriminal. From the perspective of labeling theory, this empirical study examines how hackers feel perceived by society at large, how they perceive themselves as 'others' and how they view themselves in relation to 'others'. Our research shows that hackers – despite of an experienced negative labeling – view themselves as positive 'others'. We conclude that the features of the hacking phenomenon itself (skillset, mindset, own morality) in combination with the digital context in which they operate, enable hackers to avoid a 'spoiled identity'.

Keywords: hacking**,** cybercrime**,** labeling, othering

3.1. Introduction

The development of the phenomenon of hacking can be regarded as the textbook example of the socially constructed nature of crime (e.g., Yar, 2005b; Steinmetz, 2015). While hackers in the 1960s and 1970s were seen as 'positive others', as skilled technical whizz-kids who like to explore the possibilities of technology and possess 'magical powers' with computers, they are nowadays merely considered to be vandals or the archetype cybercriminals (Skibell, 2002; Yar, 2005b; Steinmetz, 2015). Quite frequently news reports appear about hackers who have gotten completely off track, turning to cybercrime and sometimes also causing considerable damage. An example of this is the hack of KPN in 2012, in which a 17-year-old hacker hacked hundreds of KPN servers and was potentially able to (by manipulating the fixed-line network) make the emergency number 112 unavailable. More recent was the DDoS attack on the Internet provider Ziggo, which caused millions of users to lose access to the Internet for days. In both cases, the police had the impression that the teenage hackers wanted to show that they were capable of doing 'big things' and perceived their actions merely as a 'boyish prank.' The media, however, are also increasingly paying attention to so-called ethical or 'responsible' hackers, who mainly want to expose the poor security of systems. A well-known example is the hack of the OV-chip card (2011), where the involved hacker journalist travelled on cracked OV-chip cards for three weeks, hereby showing how

easy the data could be manipulated on the card[29]. Similarly, the hack at the "Groene Hart Ziekenhuis" in 2012, in which a hacker was able to gain access to the medical records of half a million Dutch people (bringing attention to the poor security of the hospital), could fall into the category of 'ethical hacking'. Yet, in this case, the hacker in question was convicted of computer hacking since his actions did not meet the requirements of subsidiarity. Thus, on the one hand, we are dealing with a negative image of the hacker (as a 'criminal other'), but on the other hand we can also observe a certain 'reaching out' for 'ethical' or 'helpful' hackers because they are hacking for a greater social good (see Van't Hoff, 2015).

From a cultural criminological point of view, where the focus primarily lies on the interaction between the reaction of society, criminalization and deviant behavior, and which also seeks to shed light on the perspective of the 'other' or 'outsider', it would be valuable to see how these developments are conceived by contemporary hackers themselves. How do they experience the way they are depicted? To what extent do they find the prevailing image of themselves to be accurate? And how do they see themselves and other hackers? Such insights are important for our understanding of the extent to which hackers internalize or disregard the label that they are given.

[29] In 2013, as a result of these incidents and various governmental debates, a guideline named ''responsible disclosure' has been created which prescribes how a security leak can be dealt with and published in a responsible manner: https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html. This Dutch Policy is unique in the world.

The role that labelling plays in the lives of hackers, has hardly been examined in criminology. One of the few empirical studies in this area is the study of Turgeman-Goldschmidt (2008), which shows that labelling may have a different effect on hackers compared to the classic ‘‘outsiders’’ described by Becker (1963). She finds that hackers resist their stigma as criminals, but do not or barely experience negative social psychological implications of labelling; whether they regard themselves as ‘good guys’ or ‘bad guys’. Rather, they view themselves as so-called positive deviants – as talented people who possess unique and special skills and attributes. This raises the question whether the assumptions from the labelling approach, which mainly emphasize the negative implications of labelling (negative self-esteem, secondary deviance and social exclusion), apply to hackers. Does labelling have a less negative, or even more positive effect on hackers than for conventional or ‘pre-digital’ others and if so, how can that be explained? Are there any other processes or effects involved that play a role? In this contribution we seek to answer these questions on the basis of the findings from ten interviews with hackers and five criminal case files. We attempt to comprehend these findings using a conceptual framework based on the labelling approach (Becker, 1963; Goffman, 1959; 1963).

At first glance, consulting the symbolic-interactionist thinkers from the pre-digital age may seem an odd choice for the analysis of a group of contemporary others. After all, the theory was developed at a time when the own group and community were defined rather locally and in which identities were much less fluid (Bauman, 2000) and hybrid (Turkle,

2005). In fact, the original aim of the research for which the data was collected, was to expand the criminological theoretical framework with a cyborgian dimension. It departed from the standpoint that, in order to understand cyber-deviant behaviour, we have to assign a more active role to non-human actors in (deviant) acts (Van der Wagen & Pieters, 2015). During the data collection and analysis, however, it appeared that labeling plays a surprisingly important role in the way hackers give meaning to their reality. Hence, the findings 'provoked' to further explore this theme in particular.

The primary purpose of this article is therefore to explore the processes of labeling of a small but diverse group of hackers to understand the world of this group of 'others' a little better. Consequently, we also want to consider whether the labeling approach is still applicable in the Internet age or whether it is ready for theoretical renewal, a digital impulse. After a brief overview of the literature on hacking and labeling, the collected empirical material is discussed and the research findings are outlined. The findings focus on three questions: a) How do hackers think they are perceived by the outside world?; b) How do they see themselves as 'others'?; and c) How do they see themselves in relation to others? The final discussion reflects on the findings more closely and discusses the applicability of the labeling approach to this group of digital others.

3.2. Hackers: from 'hero' to 'criminal'

In the 1960s and 1970s, hackers were still considered to be the 'heroes' of cyberspace (Levy, 1984) or at least whizz-kids who wanted to explore the possibilities of computer technology. However, since the 1990s, they have increasingly been seen as criminals, dangerous anarchists or terrorists (e.g., Halbert, 1997; Nissenbaum, 2004, Skibell, 2002). In the literature, various explanations are provided for this shift. The first explanation is that the meaning of the term 'hacking', which originally referred to solving obstacles or problems, changed over time (Nissenbaum, 2004). Because computer technology became accessible to a larger public and on a grand scale, a new generation of hackers appeared for whom hacking entailed cracking or sabotaging a computer system – although their professional ethics still strongly mirrored the ethics of the former generations of hackers (e.g. Halbert, 1997; Turgeman-Goldschmidt 2008). A second explanation is related to the commercialization of the Internet, the fight against cybercrime and the conflicting and distrustful relationship between the hacker underground and the computer industry (see Skibell, 2002; Taylor, 1999; Yar 2005b; and Jordan & Taylor, 1998). A third explanation is connected with the fact that media and films portray hackers as pathological, computer-addicted or dangerous nerds (see e.g., Halbert, 1997; Nissenbaum, 2004). While the hacker in movies like WarGames (1983) was still romanticized (Halbert, 1997) or pictured as the one who outsmarted the state, in later movies the hacker is increasingly depicted as a dangerous cybercriminal (Wall, 2008).

Although hackers have gained an increasingly negative image over time, they do not see themselves as 'misfits'. Halbert (1997: 363) finds that, despite the scapegoating and demonization, hackers see themselves as positive others: "[they] tend to embrace their differences as setting them apart from others." Turgeman-Goldschmidt (2008), who conducted interviews with 54 Israeli hackers, comes to a similar conclusion. According to her, hackers see themselves as positive deviants: they are talented, superior and genius. The respondents in her research succeeded in avoiding the negative consequences of labeling and secondary deviance, were able to convert their deviant background into social capital and could gain a good place in the labour market. Possible explanations that are mentioned are the fact that hackers often come from a higher social-economic segment of society (and therefore may be better able to handle stigma) and that hackers also oppose social conventions or moral boundaries more quickly, which might increase their ability to deal with labeling (*Idem*). Holt (2010), in this context, points to the fact that hackers put their own (moral) demarcations between themselves and other hackers, leading to categories such as 'hackers' versus 'crackers' and 'black hat' versus 'white hat' hackers'.

3.3. Labeling, self-image and a spoiled identity

The labeling approach focuses on the way in which society's reaction, whether formally through sanctioning/punishment or informally through stigmatization, negatively affects the self-concept and social identity of the labelled person (Becker, 1963). We can distinguish

different implications for the labelled one, such as negative self-esteem, exclusion from community and social networks and failure to find work. When the labelled person internalizes the attached label, this can, according to Erving Goffman (1963), lead to a spoiled identity. This in turn can result in deviant group formation and further delinquent behavior, also known as secondary deviance. According to Edwin Lemert (1967), who introduced this concept, the process of secondary deviance begins with the feeling that the attached label is unjust, which then forms the basis of one's new identity, that of deviant. In that sense, by exhibiting secondary deviance the person also solves his or her identity problem. The strongest variant of a secondary deviant identity is the detainee, which involves an identity from which it is socially impossible to escape. However, Lemert also sees more fluid forms of secondary deviance, in which, for example, members of a subculture 'drift' from a deviant to a socially accepted identity. In particular, this latter form of secondary deviance could be relevant in the case of hackers. However, in the literature, there is barely any attention paid to the influence of the digital context on the occurrence of secondary deviance. In this article, we also want to take this dimension into account by checking whether the Internet makes it easier for hackers to escape from negative labeling or to "drift" between a deviant and a non-deviant identity.

Since the empirical material that is used for this study merely provides insights into the self-image of hackers and, to a lesser extent reveals aspects such as exclusion, job opportunities and secondary deviance, we take the concept of the deviant self (as "other") from symbolic

interactionism (Mead, 1934; Goffman, 1959; Goffman, 1963, etc.) as the starting point for this study, in order to analyze the self-image of hackers. We distinguish three complementary dimensions of the deviant self concept. First, there is the dimension of how hackers (as "others") think they are perceived by the outside world and what attitude "normal people" have towards them (Goffman, 1963). The second dimension is how hackers see themselves and how they judge their own actions. This dimension includes aspects such as competencies, self-esteem, identity and morality. The interaction between these two dimensions is an important topic in the work of Erving Goffman (1959; 1963) because a person is always aware or imaging how others (the audience) observe or classify him or her and this in turn also influences the self concept or social identity. Goffman (1963) talks about a process in which someone learns that he has been stigmatized and becomes aware of the ensuing consequences. In Becker's work (1963), a "technical" dimension is also addressed: for example, one has to first learn how to smoke a joint before you assign yourself the identity of a marijuana user. As a third dimension, there is the question of how hackers, as 'outsiders', see themselves in relation to the good citizens and to other (groups of) outsiders (Goffman, 1963: 130-131). For example, David Matza points out that others often make categorizations themselves within the group to which they are counted. "From the outside, deviant persons (...) tend to look alike. From the inside, there is bound to be assortment and variety, observable, known, and usually designated by those who inhabit that world" (Matza, 1969: 28). There may also be a comparison with other ('external') groups, a dimension that could possibly play an important role for

hackers. Bruno Latour (2005: 32) states in this regard: “It is always by comparison with other competing ties that any tie is emphasized. So for every group to be defined, a list of anti-groups is set up as well.”

3.4. Research method

For this article, data have been analyzed that have been collected in the context of the PhD research of the first author. In that research, Bruno Latour’s actor network theory (ANT) is used as a central approach for grasping the hacker phenomenon. Within the ANT approach, a research methodology is prescribed that closely mirrors the ‘*verstehende*’ approach of cultural criminology (Ferrell, 1997). In his actor network theory, Latour advocates that the perspective of the research subjects themselves should be the centre of the inquiry as much as possible if we want to understand phenomena. According to Latour (2005), not only are the subjects able to construct and define their own social reality, but a more ‘agnostic’ research approach may provide more insight in their world than a pre-established framework would (Latour, 2005). At this point Latour places himself in the tradition of symbolic-interactionism, from which the labeling approach has also emerged. For the research, ten semi-structured interviews have been conducted, in which various (general) themes were discussed with the respondents, such as motives, learning processes, self-image, moral perception and their perception of their own hacking activities. The theoretical element that is central in

this article, labeling, originated from the interviews, but was not a priori the central subject of the interviews or of the research itself.

From the ten interviews, eight interviews were conducted face-to-face, one took place through Skype and one via e-mail. The first five interviews have been conducted between May 2013 until May 2015 by the first author[30]. The second five interviews took place in April and May 2013 in the scope of a course on cybercrime at Groningen University. They were conducted by a group of students, under the supervision of the first author. Although the interviews have been conducted by different people and in different contexts, the topics discussed during the interviews were largely overlapping. The respondents were found through 'hackerspaces'[31], via (student) contacts and by 'snowballing'. Finding hackers willing to participate in an interview was difficult. This appears to be due to the many interview requests that hackers get and their ensuing tiredness with regard to media and research. For example, through hacker spaces, we were told that they receive requests from journalists or researchers on a daily basis. Secondly, there was a feeling of: 'here is yet *another* researcher who does not understand anything about our world'. This feeling played an important role in the low interest in participating, something we heard from people who mentioned that they knew some hackers. Thirdly, there was the fear of being associated with cybercrime. For instance, from one of the hackerspaces we received

[30] Two of these interviews have been conducted together with a criminology student from Leiden University who asked a couple of questions for her master thesis.
[31] Probably different than the name suggests, hackerspaces are offline meetingplaces where hackers gather to tinker with computers and electronics.

the answer: “To be clear from the beginning, what definition of the word ‘hacking’ are you using? A large part of the general public associates hacking with different forms of online and computer-oriented crime. Depending on the type of hacker you are looking for, we will gladly spread your message and reply to our participants.” In short, negative attributions and labeling already seem to have a negative effect on the data collection and possibly affected the composition of the group. Eventually, one respondent was recruited through the hackerspace, three respondents have been recruited through the snowball method and the rest of the respondents were found through (student) contacts.

All the respondents are (young) adult males of Dutch nationality (except for one Australian) who completed an ICT-related study (i.e. average to high level of education) or were still studying. The group is, however, rather diverse when it comes to their experience and motivations. Five out of ten respondents consider themselves to be ethical or white hat hackers. For example, they search (either for themselves or on behalf of a company) for system vulnerabilities, report them and in some cases also publicize them. The other half of the group has been more or less active in the black hat circuit. Two respondents hacked several large companies or organizations and have also been imprisoned for their involvement in those hacks. Now they consider themselves to be (ex) black hat or gray hat hackers; they occasionally explore the edges of what is allowed and do not associate themselves with the white hat scene. Two other respondents have also been active as black hat hackers but claim to no longer be active in illegal hacks. The last respondent, who does not

consider himself to be a 'prototype hacker', has been involved in virtual theft for four years. He was hacking the accounts of fellow players. He is the only respondent who admitted to having a (at least partially) financial motive for hacking.

In addition to these interviews, an analysis was conducted of five criminal case records in which computer hacking was the central charge[32]. This research took place at a later stage, namely in July and August 2015 at the Public Prosecutor's Office in Rotterdam[33]. In four of the cases an individual hacker hacked one or multiple larger companies or organizations and in one case the hacks were committed by a hacktivist group. The files include police hearings or conversations with the suspects (for example, with the parole officer) and sometimes also extensive informal conversations between hackers. Since each file provided information on how the hackers viewed their committed offense and how they saw themselves as hackers, this aspect could be included in the present study. Of course, we have to take into account that police hearings take place in the context of criminal investigations and consequently may not reflect how the suspects give meaning to their actions and themselves. In the findings discussed below, we therefore explicitly mention which information we abstracted from the files.

[32] Cases which involved criminal networks engaged in the spread of large-scale (banking)malware were not included in this study.
[33] These were obviously not the cases in which the interviewees were involved.

The description above of the empirical material (interviews and criminal records) makes it clear that we are dealing with a very small and diverse respondent group, whose common denominator is that they see themselves as hackers. Furthermore, their ethics, their normative position on hacking and their criminal antecedents vary widely. Generalized statements about the 'hacker community' as a whole therefore cannot be made based on the findings of this study. However, we do aim to provide some insights into the world of perception of hackers. The great diversity of the respondent group also serves the theoretical purpose of this research, as it helps to make the mutual labeling of hackers transparent. The following analysis presents, based on statements of the interviewed hackers, the manner in which they construct their reality. The findings are clustered into three sections. The first section deals with the manner in which hackers think they are seen by the outside world and labelled as 'others'. The second section explains how hackers see themselves as 'the other'. Finally, in the third section we discuss how hackers look at other hackers, in other words, how they label each other as 'the other'. To ensure anonymity, we assigned fictitious names to the interviewed hackers and, where necessary, we left out case-related information.

3.5. How hackers think they are perceived by the outside world

With regard to how they think the outside world sees hackers, the respondents immediately mention misunderstanding. They indicate that outsiders do not understand 'their world' and may not be *able* to understand it either. Some of the respondents explain that this incomprehension is due to the difference between the level of digital knowledge between hackers and average citizens. According to the respondents, this difference in knowledge in turn can lead to different responses. Eric (an ex-black hat hacker) has the impression that there is a lot of societal fear and he thinks that it [hacking] is a big mystery for people. Others point to prejudices and believe that many people think that hackers use their skills by default for malicious purposes, by breaking in everywhere they can. In addition, some respondents indicate that, because of this misunderstanding, various stereotypes have emerged, ranging from hackers as nerds to hackers as dangerous people; and those stereotypes are confirmed or reinforced by the media. According to Paul (an ex-black hat hacker), hackers are portrayed as: *"Nerdy types sitting in attics, in the dark, breaking things all day long behind the computer. There are media that really present it this way. I think the media and most people think of hackers as anti-social nerds with bad intentions, who do nothing else the whole day. However, I also believe that the image is beginning to change as well because it's getting more public, for example because hackers themselves expose themselves in the media."* Jack (the hacker from the hackerspace) points in this context to

the negative imagery in the media and in movies when it comes to hacking. Nevertheless, the respondents also note that it is difficult for outsiders to understand 'their world'. Hence, they seem to say that the incomprehension and fear also has a genuine basis. The respondents describe the hacker scene as a separate community and they sometimes also describe it as "mysterious", "underground" and "difficult to access." If hackers were more visible, as Paul pointed out, the negative stereotypes that exist would dissipate and the world of the hacker would be less mysterious and frightening.

Apart from the feeling of being seen as a mysterious or dangerous other, the hackers experience, actually much more, being seen as *criminal* others. The idea that hackers are viewed as criminals or as criminal organizations is a central theme, which is unanimously expressed by respondents. An important factor that they consider as a possible explanation for this negative image is the increase in cybercrime. David, a white hat hacker who works at a security company, claims, e.g., that in recent years many new actors and criminal organizations have emerged who are involved in hacking, giving all hackers a bad name. In addition, some respondents argue that the media, through their selective messages – portraying hackers as criminals – further enhance this image. Paul states: *"You do not read: 'hacker finds holes in every version of Windows'. You do not find that in the media. In the media you find 'hacker hacks company X and steals 3 million credit card data.' That is what you will find. Yes, of course this creates a negative image. I understand that too.*

People then think of hackers as those bastards who try to rob my bank account."

The respondents further indicate that they are not only seen as criminals, but also treated accordingly. According to Jan (an ethical hacker), hackers are always approached with suspicion, even if they have good intentions. *"Instead of the benefit of the doubt, the Public Prosecutor always gives them the disadvantage of the doubt."* Jan also experiences that there is a role reversal here. It is actually the companies that are being hacked that are acting in a more criminal manner, since they do not properly take care of the security of their data, which is made visible by the hackers. The hackers, however, are the ones who risk 'serious criminal prosecution'. According to Jan, ethical hackers can get extremely upset about the bad security of systems and often experience not being taken seriously. This can even lead hackers who had good intentions to go too far. Jan gives the example of a hacker who finds out that he can order free items at a web shop. If, after reporting, nothing is done, the hacker could for example (as a kind of prank) order a couch (free of charge) and then deliver it to the office of the company in question.

3.6. How hackers see themselves as 'the other'

As mentioned before, many hackers consider their scene to be a separate community. They also consider themselves to be different (from others) – something they experienced already from an early age. Jan explains: *"As a child I wanted to push all kinds of buttons just to see what would happen.*

I think that there is an innate need involved when it comes to dealing with technology, that you have a certain connection with technology." This feeling of otherness often leads to an urge to search for likeminded others, online or offline. One looks for people like oneself or for people who have similar interests because one feels a stronger connection with them. In addition, the interviewees indicate that it is very important for them to share knowledge and to talk to people who understand what they are talking about or, as Paul says: *"Not like people who look at you in a sheep-like manner of 'what is he talking about'?"* Various interviewees also point out that they separate their online friends and their online world from their offline friends and world, or at least they consider them as two separate categories. With offline friends, they go out to the pub or play a game, but they rarely or never talk about computer-related topics.

In addition to the feeling of being 'different' and being part of a group of 'others,' the interviewed hackers see themselves as 'positive others.' Some respondents assert that hacking can be considered in terms of creativity, imagination, out-of-the-box thinking, art or ingenuity. For example, for Jack a hacker is someone who is "doing smart things playfully." Jan defines hacking as a "state of mind", the thinking beyond existing patterns and the picking up of signals which "normal people" do not see, which in turn creates a gap between hackers and society. *"Not being heard, things are not resolved or not taken seriously, not being understood. Why don't you see that the whole world is green? Why do I see it and you don't?"* For some (ex) black or gray hat hackers, such definitions are actually far too broad. They define hacking rather in terms

of “gaining control over another’s system” or “taking over a server”. The idea that, for example, “making a beer tap” [out of something else] can be considered as hacking is completely ridiculous for Eric (an ex-black hat hacker).

Another ‘capacity’ in which hackers see themselves is that of ‘helper’. That ethical hackers view themselves this way, is quite evident. They use their hacks to help businesses to eliminate their vulnerabilities or, in the words of Jan, “they reveal abuses in society” and also aim to alert society and to protect her from these abuses. The idea of the hacker as a helper, however, also sometimes plays a part in how black or gray hat hackers give meaning to their actions. Dylan, who has long been active in the black hat hacker scene, claims for example that he actually helped the companies that he hacked: *“If we, the more middle or low-level hackers were not there to educate companies about their safety, they would be eaten alive.”* The company that is broken into is thus not seen as a victim but as a company that has a poor security system and thus brings the hacking upon itself.

This is also an issue brought up by the suspects in all five criminal records. For example, a suspect in one of the criminal records states: “*It’s ridiculous for people to fill in their data and then for people like me to easily be able to find this information. Releasing is putting data online to shock people and make them aware of what can happen to your data. The goal is primarily to embarrass the company. A lot of money has been spent on beautiful pictures, but the security is apparently not important.”* Regarding

the proportionality of the punishment imposed (on him), Paul mentions the fact that hacking can also be positive for society. *"The condemnation is not wrong, but too heavy I think. Especially because I did not break those systems. In fact, I made them even better. So I felt that I actually helped those people."*

3.7. How hackers see themselves in relation to 'the others'

According to the respondents, not everyone can call him or herself a hacker. Although "it's not a protected title", there is some exclusiveness involved. A hacker must be able to do something genius or creative. However, "doing something brilliant" can also include illegal activities. According to Jan, some criminal actions may be also quite brilliant even though they are illegal. Daniel (a white hat hacker) refers to the difference between someone who cracks a safe at a bank and an intruder who simply finds the key under the door mat. According to the respondents, those within the hackers scene often view the so-called "script kiddies" in a negative way because they use existing tools. They basically find the key under the door mat and thus do not really know how the tools work. In this respect, the respondents seem to distinguish between the "real" hacker and the amateur or wannabe hacker. Eric, however, thinks that it is "fucking bullshit" that script kiddies are looked upon so negatively by hackers because everyone starts like that. Vincent, the respondent involved in virtual theft, actually distances himself from the hackers who want to know everything about the inner working of technology. *"They have nothing better to do; I find it nerdy and a waste of*

time." He also points out that he is more interested in what you can do with the program and especially how you can get control over someone's computer. Due to this interest he came across the so-called "Remote Access Tools", which enable hackers to take over the computer and webcam of other users.

Skills in turn play an important role in the hacker scene, also in terms of gaining access to the scene. In addition to the open forums in which they can be active, hackers will spend much more time on private chat channels, which are more difficult to enter. According to Kevin, it is a select group of friends with whom you exchange skills and exploits. Outsiders, also called 'the public,' are kept outside. For many channels, you must be specifically invited by other hackers. Kevin (an ex-black hat hacker) indicates that the limited access and the associated mystery attracted him most: "*They don't just let anyone in and certainly don't teach newbies ''how-to''. That made it extra exciting and interesting to do it myself.''* Paul notes that the criteria to be admitted are now different than at the time he was active in the black hat scene: *"Someone asks a question, no matter what kind of question, you can answer it. Then you show that you really know that! They are like 'wow!' He knows something about it. It was not bragging about the four hundred websites you hacked today, in order to become part of the group'."* In other words, hackers experience being an exclusive 'other' and being part of an exclusive group.

An at least as important way that hackers define themselves as a group, which we have seen before, is by distancing themselves from

cybercriminals (as an anti-group). In order to resist that label, they explicitly explain the differences between hackers and cybercriminals ("the assholes who rob your bank account"). The first difference involves the intention of the hacker. According to Paul, "*hackers are just people with a hobby who want to know everything about the system, how it works, how to break it, and what it does if they do this."* Sometimes the hobby can go out of hand – as was the case with him – but then you still cannot compare a hacker to a criminal who sells or steals things. For Paul and also for most of the other respondents, the line between the criminal and non-criminal depends on whether there was a financial motive involved. This brings us to a second difference that was brought up by most respondents, namely the thought that hackers are in any case not willingly and intentionally committing a crime and are also not "calculating" criminals.

One of the hackers from the police files remarks: "*You're just messing around with a couple of guys, but it's not organized crime! In my view, we should all have made plans in advance and considered how to do things and what we should do with the data. We do not do this; it's more just fun to do something about what you find but there is no plan"*. Some respondents, including one of the suspects in one of the files, also point out the role of group influence and that boundaries in a (black hat) group easily fade away. Eric reveals: "*There is no one who says to you 'hey, this may be criminal" and as a result "many boys get entangled in it"*. According to Simon, hackers are often talented boys who are "still searching" and do not know how to use their talent. However, in the end, according to

the respondents, a black hat hacker will end up on the "good side". For example, they point out that the fun and the challenge at a certain moment wears off, but also that you want a normal income at some point. Indeed, many (ex-blackhat) respondents reveal that their black hat past has actually made a positive contribution to their career. They found a job almost immediately after their imprisonment and can also use their skills well in their work. A third difference between hackers and criminals is the modus operandi, which according to the respondents is very different for a hacker than for a criminal. Eric says, for example, that hackers are usually very careless about taking security measures: "*Someone who is in it for financial gain will from the beginning ensure that there are no traces; he is not going to write his name all over it because he does not care about becoming famous. In contrast, boys who are exploring the technical possibilities, they make very stupid mistakes. They just put their name on something even while they're busy infecting people".* Hackers, unlike cybercriminals, are also eager to brag on chat channels, which, according to Vincent, gets them caught faster. Paul speaks of 'media-whores' who are so stupid that they just add their home address. He also thinks that this is specifically characteristic of the hackers of this age. According to him, the 'attention-seeking behavior' has increased dramatically in recent years and there are groups who only hack to 'brag about it'.

In addition to processes of 'othering', regarding who and what a hacker can call himself, there are also processes of labeling between hacker groups. The clearest example of this is the way black hat and white hat

hackers look at each other. The majority of respondents indicate that a clear distinction can be made between these two groups. This distinction is mostly spoken of in terms of good and bad intentions or in terms of legality and illegality. Paul explains: "*A white hat is really somebody who wants to do good, do nothing wrong, nothing illegal; we found a bug and we report it to the person who has the bug; and a black hat wants to abuse it, who would say: well now, let's just look inside. We report nothing at all."* In this context, Kevin states that he finds the term 'gray hat hacker' to be nonsense. *"A person cannot be good and bad. Someone hacks either for money, keeps the information for themselves or sells it to the black market, or causes damage (black hat). Or he is a 'good guy' and hacks professionally."* However, this does not mean that a black hat cannot do good things (or vice versa). Jan refers for example to a mafia boss who gives money to a charity.

Eric argues that there is an ongoing battle between black and white hat hackers, which is linked to the hacker's negative image previously discussed: *"On Twitter or that sort of thing they are attacking each other. And all black hats hate the white hats and all white hats hate the black hats because they all do criminal things and that's not good for the image of hackers."* When we look at how the ethical hackers in the interviews describe the black hat hackers, we see that this is done in terms of good and evil, morality or damage. Black hat hackers are labelled as 'people who hack to annoy others' or 'cause damage,' 'bad guys,' 'burglars,' 'hackers with other moral standards' and 'malicious.' Conversely, when white hats are described not only are there references to 'good and evil',

but also to character differences and different emotions. Eric describes white hat hackers as 'obedient pussies', 'who adhere to the rules', 'very polite and civilized boys', who 'were born white', 'exaggeratedly good, 'screaming about every little leak they see' and 'seeing a clear boundary between what is allowed and what is not' while he regards black hats as the 'naughtiest boys of the group' who are looking for excitement.

3.8. Discussion

In this article we discussed the extent to which hackers as 'digital others' experience negative effects of their labeling as 'outsiders' and whether the classic labeling approach is still useful in the digital age. We examined three dimensions of the self-concept of a small but diverse group of hackers. In line with the findings of Turgeman-Goldschmidt (2008), the interviewees experienced negative labeling, but they mostly see themselves as positive others. According to them, they do not have significant shortcomings, but actually something *extra* compared to other people: skills, intelligence and a state of mind with which they can perceive things, comprehend, and do brilliant things. Thus, based on our analysis of empirical material, we cannot say that hackers have a spoiled identity.

The fact that labeling processes seem to have less stigmatizing effects for hackers than for 'traditional' deviants, appears to be largely related to features of the hacking phenomenon itself. The hacking phenomenon,

which is linked to one's own skills, mindset and morality, is the domain of an exclusive group of 'initiates', which is active as an online group on the World Wide Web. You must not only learn the skills to become this 'exclusive other', but you must also prove yourself. Without interaction with and confirmation from the others (your audience) in the scene, you're actually lost in cyberspace. If you manage to do brilliant hacks, you may be able to gain a hero status. What is then considered by the 'real world,' by less significant others, may be less important. In other words, the positive self-image that hackers have of themselves, the (online) community to which they belong and the clear moral framework in which they give meaning to their actions may explain why they can place themselves above the negative judgments of the (offline) world which cannot understand the hacker world. Our findings also suggest that some hackers make a distinction between online and offline identity, which allows them to manage two identities at the same time and/or to 'drift' between a deviant and a non-deviant identity. For some (black hat) hackers, hacking seems to be 'criminal role playing' rather than committing crime. Ultimately, they do something good for society by exposing the bad security of companies and organizations, which in their eyes are actually doing much more wrong.

Although the moral boundaries between black and white hat hackers differ, they agree that you cannot compare hackers with the real cybercriminals who go for the big money. This also brings us to the point that the difference is not just a matter of association with 'like-minded others', but also an explicit dissociation from other groups. In this sense,

Latour's term 'anti-group' seems appropriate to describe the relationship between hackers and criminals, but also the relationship between black hat and white hat hackers. The fact that labeling processes thus also occur within the 'others' group probably eliminates negative imaging. In short, in addition to a digital dimension, such an (anti-) group dimension could also enrich the labeling approach. Therefore, we do not conclude that the labeling approach is 'outdated', but that it could use an update in order to play a role in (cyber)criminological research in the future.