From cybercrime to cyborg crime

van der Wagen, Wytske

Chapter 4

The Cyborgian Deviant: An Assessment of the Hacker through Actor-Network Theory*

* This chapter will be published as: Van der Wagen, W. (2018/*forthcoming*). The Cyborgian Deviant: An Assessment of the Hacker through Actor-Network Theory. *Journal of Qualitative Criminal Justice Criminal Justice & Criminology*.

Abstract

When we think of technocrime, it is immediately 'the hacker' who comes in mind, a somewhat mystical figure who can do magical things with technology, though malicious things too. Throughout history various scholars, including criminologists, have sought to grasp the hacker phenomenon, unraveling their techno-culture, identity and mentality. The current study is one of them, yet it does so from a novel, less anthropocentric angle. Drawing on the cyborg-lens of actor-network theory – which considers the human and the technical as non-separable – this study conceives the hacker as a 'cyborgian deviant': a transgressive blend of human and technology. Such perspective puts the human-technology relationship more in the frontline of the analysis, enabling to gain a more nuanced understanding of how hacker's (deviant) relationship with technology can take shape. Based on 10 hacker interviews, the article reveals that being and becoming a hacker cannot be understood in separation from how they interact, with, through and against technology. Whether engaged in licit or illicit hacks, hackers seek to set, explore and extend simultaneously the boundaries of technology and themselves, blurring also the boundaries between good and evil on the way.

Keywords: hackers, cyber deviance, cyborgs, actor-network theory, human-technology relationship

4.1. Introduction

Over the last few decades hacking and other forms of technocrime have become a major public concern. Almost on a daily basis, we are confronted with cyber incidents that lead to severe technological and financial damage for companies, organizations, governments and people. In the Netherlands, e.g., in 2012 a 17-year-old hacker was arrested and prosecuted for hacking several servers of a major Dutch telecom company. He was potentially capable of making the national emergency number completely unreachable. [34] In 2013 a 19-year-old hacker was arrested for hacking at least 2000 computers and webcams by means of a so called 'remote access toolkit' (RAT), an easy online to purchase tool on the Internet that enables to remotely take over a computer. He stole nude photos from the hacked computers and spread them through social media. The involved hacker claimed in court that he was "hypnotized by the opportunities of technology."[35] Apparently, for some youngsters, ICT has become an interesting new field or toy to play with (Turgeman-Goldschmidt, 2005), also for illicit activities. Moreover the Internet nowadays provides the tools, information and videos on how to do it anonymously, basically bringing no restrictions regarding the (malicious) usage and exploration of computer technology.

[34] https://nos.nl/artikel/339192-hoogste-alarmfase-na-hack-kpn.html
[35] https://tweakers.net/nieuws/98247/rotterdamse-hacker-krijgt-een-maand-celstraf.html

At the same time, a large part, or even the majority of the hacker community, (still) consists of hackers who do not intend to cause any harm (Steinmetz, 2015) and who explicitly dissociate themselves from the above types of 'hacks' or 'hackers' (Van der Wagen, Van Swaaningen & Althoff, 2016). For instance, so called 'white hat' or ethical hackers search for leaks or 'bugs' in security systems in order to get them fixed and have their own specific ethical believes (Van't Hof, 2015). The same counts for those active in 'hacker spaces', offline meeting places where people gather to tinker with hardware, software and electronics. Hence it is worth to keep in mind that the hacker landscape consists of different hacker groups with various skills, moral perceptions and 'usages' of computer technology (Holt & Kilger, 2008), both licit and illicit or somewhere in between (Blankwater, 2011; Steinmetz, 2015).

Over time various scholars, including criminologists, have sought to grasp the hacker phenomenon, unraveling the features of hacker culture and ethics (e.g. Levy, 1984; Taylor, 1999; Himanen, 2001), hacker's relationship with technology (e.g. Turkle, 1984; Jordan & Taylor, 1998) and how hackers construct their deviant identity (e.g. Turgeman-Goldschmidt, 2008; Van der Wagen *et al.*, 2016). The current study is one of them, yet it does so from a novel approach. It departs from the notion that hackers, whether they are engaged with technology in a deviant or non-deviant manner, require an approach that puts the human-technology relationship more in the frontline of the analysis. It argues that we can obtain a more nuanced view of their drives, perceptions and beliefs, when we move beyond the anthropocentric lens of existing

approaches (e.g. Becker, 1963; Katz, 1988; Matza, 1969), which ultimately place human agency in the center of inquiry and treat technology in a rather passive way (see also Brown, 2006). Against this background, this study uses the cyborg-perspective of actor-network theory (Latour, 2005), which presumes that human actions, decision-making and sense making cannot be separated from the objects, technologies and artifacts that they use or engage with. It offers a framework that enables to grasp the various ways in which the human-technology relationship can take shape. Accordingly, this study conceives and studies the hacker as a 'cyborgian deviant': a transgressive blend of human and technology. In this context the article builds on the 'cyborg crime' perspective outlined by Van der Wagen & Pieters (2015), which proposes a hybrid understanding of agency in the course of deviant action[36]. In the current study this perspective is used to study and interpret the manner in which the human-technology relationship manifests itself in the hacker phenomenon. The main question the article seeks to answer is: how do hackers give meaning to themselves and their actions and how is this co-shaped by their (deviant) relationship and engagement with technology?

For this study ten in-depth interviews have been conducted with both hackers that were engaged in illicit hacking activities and those that mainly act(ed) within the boundaries of the law. The findings reveal that hackers - whether engaged in licit or illicit hacks - perceive themselves

[36] See also Suarez's study (2015), which considers the cyborg concept valuable for a thorough understanding of cybercrime.

as actors with a specific skillset and mindset that sets them apart from ordinary people and criminals. Through their engagement with hacking they seek to set, explore and extend simultaneously the boundaries of technology and themselves, blurring also the boundaries between good and evil on the way. Hackers embody (and believe to embody) various features of the cyborg figure, which is visible in the way they describe their relationship with technology, but also with regard to how they see themselves in relation to others.

The article starts with a short discussion on the social construction of hackers, in which the inseparability of hackers with the world of computer technology is an element. Hereafter the article discusses how existing studies capture the hacker-technology relationship and why the cyborg-perspective of ANT is a valuable alternative. The empirical part firstly provides a description of the data and research method and hereafter presents the research findings. In the final section the article summarizes the main findings and also reflects on the value and future potential of ANT's cyborg-perspective for grasping hacking and other forms of technical deviance.

4.2. Hackers and technology: two inseparable worlds

Historically, hackers have always been perceived as figures that have a specific relationship with the worlds of objects and computer technologies. In the 1960s and 1970s, hackers were viewed as computer enthusiasts or 'whizz-kids' who explore and expand the boundaries and

potential of computer technology (e.g. Levy, 1984; Chandler, 1996). Hackers were admired for having an almost organic relationship with computers (Skibell, 2002) and to be a hacker "was to wear a badge of honor" (Rheingold, 1991 in Chandler, 1996). Hackers were also considered as members of a specific subculture who stand for particular technology-related believes and values, including being supportive of the idea that information should be free, viewing software in terms of art and beauty and placing an emphasis on skill (Levy, 1984; Nissenbaum, 2004; Thomas, 2005). Their ethics also promoted distrust in authorities and the resistance to a conventional lifestyle (Taylor, 1999, Yar, 2005b; Blankwater 2011; Steinmetz & Gerber, 2014; 2015). Although hackers were not part of the mainstream establishment, the public attitude towards them was generally positive in the early days (Nissenbaum, 2004).

This more positive perception of hackers shifted gradually to a considerably more negative one. In the 80s hackers were more and more perceived as pathological computer addicts, who were better able to socialize with machines than with people (Turkle, 1984; Skibell, 2002; Sterling, 1993; Yar, 2005b) and their 'magical' power with computers relatively quickly became a source of fear and danger (Skibell, 2002; Wall, 2008). Of course, there were also developments within the hacker community itself that affected both the meaning of hacking and the public perception. For example, hackers (or 'crackers') entered the scene for whom hacking involved the breaking or sabotage of systems (Wall, 2007; Chandler, 1996). The term cracker actually emerged in the hacker

community itself to differentiate between hackers that create code or use something in an unconventional way and crackers who break things (see Holt, 2010), although crackers can be divided in various subgroups as well (see Wall, 2007). Crackers were (and still are) however a minority within the hacker community at large (Taylor, 1999; Steinmetz, 2015). Important to stress is that also other categorizations exist that distinguish 'good hackers' from 'bad hackers'. The most known one is the division between white-hat, gray-hat and black hat hackers, the one the current study applies (see method section).

From the 90s onwards, hackers were mainly viewed as criminals, an image that was further reinforced by the security industry (Taylor, 1999), the government (Yar, 2005b) and the media alike (Halbert, 1997; Nissenbaum, 2004). Indeed, as Churchill (2016) points out, the social construction of the hacker shows quite some similarity with that of the professional burglar. Their (perceived) skills, intelligence and sophistication attracts both fear and admiration and they are also viewed and treated as the representatives of the dark side of technical progress. Paradoxically, hackers have also been important enablers of the same technical progress themselves (Levy, 1984; Chandler, 1996; Blankwater, 2011) and perhaps also (unwillingly) co-produced the construction or 'myth' of hackers as dangerous criminals (see Skibell, 2002).

That hackers have a specific relationship with technology is also displayed in studies that seek to understand hacking from the perspective of hackers themselves (Levy, 1984; Taylor, 1999). The work

of psychologist and sociologist Sherry Turkle (1982; 1984), is perhaps most prolific on this topic. She pictures hackers as figures that are deeply engaged with the world of machines and technology. Rather than a gifted and beautiful body, hackers believe to possess a gifted mind, a mind that gives them the mastery over technology. Mastery is generally considered as a key element of hacker culture (Holt & Kilger, 2008), but also conceived as a valuable concept for understanding how hackers relate to technology. It refers to the "extensive breadth and depth of technical knowledge an individual possesses that is necessary to understand and manipulate digital technologies in sophisticated ways" (Kilger, 2010: 208). According to Turkle (1984), mastery over technology is also strongly intertwined with how hackers view themselves. Some of the hackers she interviewed had an image of themselves as 'non-persons' or 'non-real people' because they like to be more engaged with 'machine things' than with 'flesh things' (humans), which they consider as two separate domains. Hackers feel proud of their ability to master their medium perfectly or by winning the battle from the machines, rather than through their engagement with humans (*Idem*).

The hacker-technology relationship has also been understood through the notion of 'craft' (Nissenbaum, 2004; Holt & Kilger, 2008; Steinmetz, 2015). Like mastery, craft deals with the manner in which hackers are able to manipulate technology, although it puts more emphasis on skills, labor and creativity than on the dimension of control, outlined by Turkle (1984). Holt and Kilger (2008), for instance, make a division between 'tech crafters' and 'make crafters'. The first type of hacker is considered

as the consumer of existing materials and the latter as the one that is engaged in producing or creating materials (e.g. new scripts, tools). Steinmetz (2015) conceptualizes hacking as 'craftwork', considering hacking as a specific kind of late modern work in which process is more important than the result. The study also shows that hackers are driven by technological challenges, feel the urge to explore and control systems and also possess a specific technology-orientated mentality. Other scholars underline the importance of 'ego' in relation to mastery and hacker motivation, which refers to the "internal satisfaction that is achieved in getting the digital device to do exactly what one intended it to do" (Kilger, 2010: 208, see also Nissen, 1998). Turgeman-Goldschmidt (2005) draws on Katz's (1988) work on the seduction of crime to grasp the hacker-technology relationship. She considers fun, thrill and excitement as the most essential features of the hacker experience and argues that all the aspects brought up by her respondents, e.g. curiosity, power, revenge and the interaction with machines, can be associated with feelings of fun. Like Turkle (1984), Turgeman-Goldschmidt (2008) also highlights the fact that hackers feel proud of themselves when it comes to their computer talent. While the outside world views them as deviants or criminals, hackers consider themselves as positive deviants: they have no shortcomings, but something *extra* (see also Van der Wagen *et al*., 2016).

While these and other studies provide valuable insights on hackers as a deviant group, including their specific relationship and engagement with computer technology, they keep looking at the hacker-technology

relationship from a rather anthropocentric angle. Concepts such as mastery, craft, ego and fun ultimately place human agency in the center of the inquiry and treat technology itself as a more passive and subordinate element in the deviant process. Existing studies and frameworks also treat the human-technology relationship in a rather dualistic manner. Goals or intentions are attributed to the human agent and the means is the domain of tools and technology. It can be argued that this dualism might work counterproductive for grasping the various and hybrid modes the hacker-technology takes shape. This brings us to the discussion of the cyborg-perspective of actor-network theory, the central approach of this study.

4.3. The cyborg-perspective of Actor-Network Theory

"If action is limited a priori to what 'intentional', 'meaningful' humans do, it is hard to see how a hammer, a basket, a rug, a mug, a list, or a tag could act. They might exist in the domain of 'material' 'causal' relations, but not in the 'reflexive' symbolic' domain of social relations" (Latour, 2005: 71).

Actor-network theory (ANT) can be regarded as a constructivist and critical approach that explicitly assigns a more active role to non-humans (e.g. technologies, objects, animals) in the course of (inter) action (Latour 1992; 2005). ANT does not consider humans and non-humans as two separate agents or entities, but speaks of heterogeneous alliances or hybrid collectives of both (Latour 1993; Van der Wagen & Pieters, 2015;

Verbeek 2005). In this respect there is a clear parallel to draw with the more familiar notion of the 'cyborg,' the term that is also used in this study. The term 'cyborg', short for 'cybernetic organism', was introduced in the 1960s as a term for 'artifact-organisms' or 'man-machine systems' in the context of space travel (see Clynes and Kline, 1960). The cyborg signified the idea that the human body could be extended with technological artifacts in order to accomplish greater things and/or to explore new frontiers, a theme that we can obviously find in many science fiction movies. In her 'Cyborg Manifesto', Donna Haraway (1987) used the cyborg figure as a metaphor to overcome the boundaries or dichotomies between science and (science) fiction, human and animal, organism and machine, physical and non-physical, which she perceived as Western dualisms that lie underneath the "logics and practices of domination of women, people of colour, nature, workers [and] animals" (Haraway, 1987: 32). Hence, she presented the cyborg figure not as a physical melt of humans and technology, but much more as a post-human[37] metaphor for questioning the extent in which we are human or technological ('constructed') (see also Verbeek, 2008). This particular interpretation of the cyborg figure we can also find in ANT's notion of the 'hybrid', which not only seeks to abandon dualistic modes of thinking, but also offers a framework that can grasp the various ways in which the blend of the human and the technical can concretely take shape. We can roughly distinguish three main ways in which ANT defines the cyborgian relationship between the human and the technical.

[37] Note that this is not the same as the 'transhuman' view, which considers the cyborg as a new life form rather than merely as a metaphor (Verbeek, 2008).

Firstly, ANT presumes that humans and non-humans not merely interact in a functional fashion (e.g. when we write we have to use a pen and paper). They are also intertwined and shape one another's actions. To give a concrete example, driving a car is seen as a performance of the driver and the car since both enable and complete the action: the driver needs to have the skills and the car the functionality to drive (see also Dant, 2004). This dimension closely resembles the original meaning of the cyborg, the notion that the tool enhances or augments the bodily functions of the human (see also Wells, 2014; Suarez, 2015). Driving also involves an interaction between the driver and the car and a process in which the driver has to gain control over the car. Both of these aspects humans consciously experience when they have to learn to drive and both change or partly disappear once they are able to drive. [38] Accordingly, for ANT, the relationship between humans and non-humans is not merely and continuously one of master and slave. It can be also interactive and mutual (see also Van der Wagen & Pieters, 2015). Latour (2005: 59-60) himself draws in this context a parallel with the manner in which puppeteers interact with their puppets: "Although marionettes offer, it seems, the most extreme case of direct causality – just follow the strings – puppeteers will rarely behave as having control over their puppets. They will say queer things like 'their marionettes suggest them

[38] Once you learn to drive, driving becomes a routine and takes place in a more automatic fashion (see Verbeek, 2005; Ihde, 1990). Of course, with the emergence of today's self-driving cars, the relationship between the driver and the car again has changed. In this case the car is the main (primary) driving agent while the role of human is secondary.

to do things they will have never thought possible by themselves." This dimension might be also relevant in the manner in which hackers engage with computers. As Turgeman-Goldschmidt (2005: 20) points out: "Despite (or because of) the fact that the computer is a machine, it invites play and movement."

Secondly, alongside this principle of 'joint (inter)action' or 'human-machine cooperation,' Latour (1992; 2005) argues that non-humans are not passive, static or neutral entities. Based on their 'script' or 'prescription', they can provoke certain actions or usage (positive or negative), can make people do things they would ordinarily not do (e.g. shoot somebody when they have access to a gun[39]) and restrict human action (e.g. traffic lights or speed bumps that regulate traffic behavior) (Verbeek, 2005; Van der Wagen & Pieters, 2015). In other words, for ANT, non-humans (including their material features) can affect human thoughts, morality and behavior just like other humans do. Also here, the 'car-driver hybrid' is very illustrative. Lupton's (1999) ANT-based study on road rage shows that the car as a physical object also co-shapes the behavior of the (aggressive) driver: "The pleasure of mastery of the machine, of speed, the sense of power and liberation that movement in the car may bring, is conducive to travelling above the speed limit for example, and other reckless driving actions, such as running red lights or travelling too close to others' vehicles" (p. 63). The fact that drivers have to move in a heavy regulated space, does not completely match up with

[39] See for example the study of Bourne (2012) entitled "Guns don't kill people, Cyborgs do."

the emotions and sensations that come along with the act of driving. Both of these aspects are worth considering in the context of hacking as well, since hackers both interact (or 'become one') with the machine –and act or have to act in a certain legally restrictive context.

Thirdly, although Latour (2005) does not explicitly mention it in his work, we can also add here a more subjective or intimate relationship between humans and non-humans. For instance, when people (mostly men) speak about their car, they often speak in terms of love, passion, emotion and character, perhaps in a similar vein as hackers speak about their computer or technology in general. This dimension is also strongly present in the work of Turkle (1982; 1984) discussed earlier. To sum up, ANT does not view tools, objects and technology in merely functional or instrumental terms. Instead, it views them as an integrative element of human action, capabilities, (self) perception, meaning giving and even one's intent. Drawing on ANT, this study conceives and studies the hacker as a 'cyborgian deviant': a transgressive blend of human and technology. By adopting this approach it aims to gain a more nuanced understanding of how hacker's relationship with technology takes shape, functionally, perceptually and intentionally too.

4.4. Research method

The current study is part of a larger study on cybercrime, offenders and victims, which primarily draws on actor-network theory and its notion of hybrid agency or actorship (see Van der Wagen & Pieters, 2015). ANT's

methodological assumptions generally reflect viewpoints from both (symbolic) interactionism and ethnomethodology (Garfinkel, 1967), which also assert that social reality is composed of *interaction*s and should be studied as such (Latour, 2005; Law, 2004). ANT also prescribes an ethnographic approach that aims to grasp "the world-making activities" of the actors under study and to express and report *their* words, self-reflections and 'own theory of action' as much as possible (Latour, 2005: 57). In that sense, ANT's view also closely connects to the notion of 'verstehen' within the cultural criminological approach (Ferrell, 1997). However, ANT adds an extra theoretical and methodological dimension. As pointed out, ANT is also interested in the non-human participants of social reality, especially in the manner in which humans and non-humans interact and form alliances[40]. For this study, this theoretical (cyborgian) element is used to gain a more profound understanding of how hackers give meaning to themselves and their actions.

For this study, ten semi-structured interviews with hackers have been conducted, in which the respondents were asked to reflect on their definition of hacking, their drives and motivation, their skills, their experiences with hacking and how they view themselves. Of these interviews, eight interviews were carried out face-to-face, one was

[40] In this respect ANT is actually a very valuable approach for cultural criminologists to consider as they also aim to understand the practice of deviance itself and how deviants give meaning to that practice (see O'Brien, 2005).

conducted by email and one took place through Skype.[41] All face-to-face interviews, except for one, were recorded and transcribed. The interviews generally lasted one up to three hours. The interviewed hackers were found through hacker spaces, student-contacts and by means of 'snowballing.' As the small respondent group reveals, finding hackers and finding them willing to participate in an interview was extremely tough. The members of hacker spaces mentioned that hackers are generally tired of journalists and researchers that approach them for interviews and also fear to be associated with cybercrime or cybercriminals. The persons, who declared to know some hackers personally, also put forward that hackers generally have the feeling that: "Ah, again a researcher who does not understand our world."

The (small) respondent group that was willing to engage in an interview consists of (mainly Dutch) adult males who all completed an IT-related education or still study. Although they have in common that they view themselves as 'hackers,' they differ in terms of their hacking activities, their motives, their normative position towards hacking and their criminal record. Half of the respondents consider themselves as ethical or white hat hackers. They search for vulnerabilities in systems/networks (for example which hold privacy-sensitive information) and report it the company. The other half of the respondents perceives themselves as (ex) black hat or gray hat hackers

[41] From these interviews, 5 interviews I conducted in the period of May 2013 and May 2015. The other five interviews were, under my supervision, carried out by students from the University of Groningen in the scope of a course on cybercrime in the period April/May 2013. Although the interviews have been conducted by different interviewers and in different contexts, the discussed topics were mainly overlapping.

(or crackers). They also search for vulnerabilities in systems (which can e.g. be a website, a server, public Wi-Fi or a program), but did/do not inform the owner. Two of these five respondents have been imprisoned for their engagement in hacking and are now employed at a security company. Two other hackers have been active in the black hat scene, but assert not to hack illegally anymore. The last respondent was for four years involved in virtual theft by means of spreading malware and never got caught. He is the only respondent who pointed out to be motivated by financial drives (as well).

Having such a small and differentiated respondent group makes it hard, even impossible to produce general statements about the hacking community at large, which this study does not proclaim to do. The material is however rich and does enable to acquire a feeling and understanding of the world of (rather different) hackers, how they perceive themselves as actors and how they define their relationship with technology. In light of the theoretical approach of this study, the diversity of the respondents can be also beneficial for exploring whether the hacker-technology relationship varies across different types of hackers or hacks. The analytical or coding approach in this study can be considered as a combination of both inductive and deductive techniques (see Hennink, Hutter & Bailey, 2011). The concepts emerged throughout a structured though flexible and creative approach (Charmaz, 2006) in which the narratives of the interviewees were coded and interpreted in light of ANT's conceptualization of the human-technology relationship. This interactive cycle or process in turn produced themes, categories and

concepts, which reflect and highlight certain aspects of how hackers give meaning to what they do and who/what they are. In the analysis that follows now, I sought to represent the reality, thoughts and perceptions of the hackers as thorough as possible. In order to safeguard the anonymity of the respondents I assigned fictional names to each of them. In the findings itself is written down what type of hacker the interviewee 'generally' considers himself or in what type of hacking activities he was involved, to place their words a bit more in context.

4.5. Research findings: what it means to be a hacker

The interviewed hackers provide different definitions or descriptions of hacking, ranging from narrow to broad. The more narrow definitions are for example: "taking over someone else's computer" and "breaking into a system without informing the owner," definitions that also stress the illicit character of hacking, which not all interviewees consider as hacking or prefer to call 'cracking.' 'Moving beyond existing patterns,' a 'state of mind' or 'assigning a different functionality to an existing object or technology' can be regarded as broader and more neutral definitions and are shared by most interviewees. Whether engaged in licit or illicit hacks, the hackers immediately dissociate themselves from the criminal image - which they believe is predominant in the public discourse. Instead, they view themselves as (male) hobbyists who possess a very specific mindset and skillset, which sets them apart from ordinary people and criminals. We are now going to assess how they give meaning to their hacker reality throughout five sections: cyborg mind, cyborg

performance, cyborg identity, cyborg body and cyborg transgression. Each section highlights a different dimension of how the hacker-technology relationship takes shape, yet the sections are also complementary.

4.5.1. Cyborg mind – how hackers view their 'usage' of technology

The way hackers perceive their usage of technology is one of the key aspects that defines the hacker practice and mindset. Firstly, the interviewed hackers do not consider themselves as passive 'users' of technology, but claim to be interested in the underlying processes that operate a system; what makes it work or *not* work. To illustrate this point, Jan explains: *"Restart your computer. I find this the most deadly and annoying comment you can hear because then [if you immediately restart] you still don't know what is going on."* In this context respondents also highlight their ability to 'see through' and 'scrutinize' a system and stipulate their 'investigative attitude.' Paul (gray hat hacker) emphasizes that you have to be very analytical when you want to become a successful (black hat) hacker: *"You need to be able to estimate a network, to map a network, to map its employees, what they do, how they behave, before you actually start, if you don't do that and prepare yourself, you won't manage the hack."* In this respect, a hack also shares some similarity with the system of robbery, involving "discipline, preparation, planning and conspiracy" (Churchill, 2016: 864). Ex-black hat hacker Eric frames the analytical ability pointed out by Paul as 'empathy'. The word empathy is usually associated with being sensitive for the emotions of other people, yet Eric uses the same word in relation to technical systems.

Understanding the technical system so well that it can result in empathy for technology, very clearly illustrates the deep and almost inner connection some hackers believe to have with technology.

Secondly, most of the interviewed hackers point out that they enjoy the interplay with the goal-means-end rhetoric of devices or technologies, an aspect that is also stressed in the definition of hacking as: *"The use of systems or equipment for purposes for which they were not originally designed."* Jack, a hacker who is active in a hacker space and a skilled programmer, points out that hacking is not merely about being technically advanced, but much more about unconventional thinking, creativity and imagination: "*There are many kinds of hacks, for example using a cd-tray as a coffee stand, using plastic sealers that they use for bread as a way to clip cables. When you have these small playful things in your room, I will call you a hacker*." ANT's notion, that the functionality of objects merges with or connects with the human actor who uses them, also manifests itself here. Hackers seem to be consciously aware of the features and functionalities of the objects that they 'use' or engage with and are also sensitive to their construction. They do not see the object (e.g. a computer) as a singular and fixed entity, but consider it and treat it as a network of different interacting elements and mechanisms. Hackers are therefore engaged in the almost scientific practice of what ANT denotes as 'reversible blackboxing' (Latour, 1992). They not merely think outside of the box (see later), but are also able to deconstruct the (black) box (see also Forlano & Jungnickel, 2015), which in hacker terms is often called 'reverse engineering' (Nikitina, 2012: 143). Moreover, they

are able to change the functionality of the object in accordance with their own desire. This suggests that hackers not merely strive for mastering their machine perfectly (Turkle, 1984), but also seek to establish the perfect master-slave relationship, in which they are in control and the master of the object and every single component of it.

4.5.2. Cyborg performance – how hackers view their abilities in relation to the tools they use

Apart from their non-instrumental usage or relationship with technology, the interviewees stress the explorative and interactive nature of this relationship. They not merely act 'alone' but somewhat cooperate or form an alliance with technology in the process of becoming a skilled hacker. Firstly, some respondents point out that they not merely learn from other hackers, but also that they learn their skills in the interaction with technology, as a sort of trial and error or 'trying and trying again.' Paul describes the learning process as an 'interplay' and also points out that he receives 'feedback' from the system: "*I learned things from school and the Internet, but the majority was experimenting. At home I had several servers, I then downloaded software, installed it and just looked what would happen, to try things and check what will happen. I cannot break it anyway, or yes, I can, but then I can install it again. You have to learn it in a playful manner.*" A deeper understanding how technology works – referred to before as technical empathy - requires at the same time the constant exploration and interaction with technology. This aspect demonstrates (again) that hackers consciously experience an interaction with technology rather than merely consider themselves as

users of technology, perhaps in a similar vein as the puppeteers mentioned by Latour (2005) who received input from their puppets as well. For hackers the interaction with technology also seems to have a more continuous nature. Unlike (most) drivers, hackers never stop learning and never want to stop learning. Learning to hack is an ongoing process and the opportunities are endless. As Daniel (white hat hacker) states: *"The more you get to know, the more there will be to learn."* In other words, the earlier mentioned master-slave relationship occurs alongside or in alternation with a more cooperative, interactive and mutual engagement. Both of these processes hackers seem to experience and to enjoy.

Secondly, some interviewees mention that the tools and technologies they use co-shape their abilities and possibilities. For instance, they do not proclaim to "invent the wheel" by themselves all the time and also depend on the abilities or functionalities of the tools they use. According to Jeffrey (ex-black hat hacker), there is always a combination of existing tools and some input of your own: "*Every hacker has his weapons tank with his own tools he has chosen to use. Usually you use an already created and existing code someone else has written and you adapt it to your problem.*" This aspect also fits in Nikitina's (2012) claim that hacking is more a process of recycling and "rearranging the givens of existing systems" than true creativity (p. 144). Gunkel (2001: 6) speaks in this context about the parasitical nature of hacking in order to emphasize that hackers draw their "strength, strategies and tools from the system on

which and in which it operates," a claim that is rather similar to ANT's view that not all the credits should be granted to the human agent.

In this context, Vincent's story is also relevant to consider. He was involved in hacking the accounts of counter players in a virtual game. As these virtual goods have real value, he was able to earn large sums of money with the theft. Vincent explains that he (initially) made use of 'ready to use' tools. He points out that he never really was a 'computer nerd' who had this born fascination for computers and technology. He was merely curious about what he could accomplish with certain programs rather than unraveling how they work. He came across so called 'remote access tools' (RATs) which relatively easy enabled him to control someone's computer and webcam. Vincent asserts that: "*If these RATs would not exist, I would not be bothered to get involved in hacking in the first place."* Over time he got skilled in various malicious cyber activities including phishing and the use of botnets. The example illustrates that certain tools can bring new options and opportunities and eventually also new skills. At the same time something is occurring on the intentional level. Without the easy access to and existence of these tools, Vincent would, as he claims, not have been engaged in hacking. Like ANT's example of guns, a RAT seems to be not merely a 'neutral' tool to use, but might, at least for some youngsters, invite or encourage their engagement in cyber deviant conduct (see also Van der Wagen & Pieters, 2015).

4.5.3. Cyborg identity – how hackers view themselves in relation to others

In the previous sections we discussed already how hackers perceive their usage of technology, which is an important part of their specific mindset and how they view themselves. There are however also other elements that are important to consider, which particularly highlight how they view themselves in relation to others. Firstly, most of the interviewed hackers put forward that they have a rather natural connection with technology, which gives them the feeling of being different than other people. They experience to have an extreme fascination for how computers, systems or devices work, an interest, which they developed already from a young age. Jan, who considers himself to be an ethical hacker, explains for example that: *"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 affinity or special connection is also considered to be essential in the process of learning to become a (skilled) hacker. As some of the interviewees point out, hacking requires quite some time, energy and discipline. You are only willing to invest this time and energy if you are truly dedicated to it and love computers. They seem to say that: not everybody can become a hacker, even though he or she wants to or has the (technical) recourses and knowledge to do so. Technology needs to be your 'second nature,' an affinity you have to possess naturally.

Secondly, the interviewees do not only highlight their ability to unravel the inner workings of technology, as discussed already, they also define themselves as actors that have the ability to think outside of the box or beyond existing patterns. Eric for example explains: *"You need to be this kind of person who can come up with something weird, vague and new that no one ever thought about before. You need to think in a different way. I can sometimes enter a room and then immediately I know how to open the doors, while other people don't see it."* Although they generally dissociate themselves from criminals, some interviewees explicitly draw a parallel with professional burglars to explain what a hacker or hack defines. To rob a house by finding the key under the doormat, does not require skill and applies to 'wannabe' hackers or so-called 'scriptkiddies' who merely use existing tools. A *real* hacker would find an inventive way of breaking the lock and would not even need a key to be able to open it up. Additionally, in assessing whether a hack(er) can be qualified as a (good) hack(er), cleverness ultimately seems to be more vital than whether the act is legal or illegal. Jan for instance explains: *"Some criminal actions are also quite brilliant. If you in a smart way rob a store, for instance, by digging a tunnel underneath, that is what I find funny. It is a cool hack, even though it is illegal."* As pointed out by Nikitina (2012: 150): hackers somewhat seem to "blur the line between the creative and the criminal on the way."

Thirdly, the ability to think differently also applies to non-technical issues. Some of the interviewed hackers point out that they are critical and sensitive about 'the system', 'society' and the government in general.

This aspect is highlighted by respondent Jan, who perceives ethical hackers as whistleblowers who bring major abuses in society to light. He argues that many companies or organizations hold privacy sensitive information, yet have an extreme poor security. According to Jan, they are actually the real 'violators', while the hackers who expose their misconduct are treated as the criminals. This can lead to major feelings of frustration among hackers: "*Why don't you see that the grass is green? Why don't you see it*?" By stating that hackers 'pick up signals' other people do not, Jan seems to stress that hackers hold an extra 'sense', sensor or pair of glasses that enables them to see certain things other people are blind to. This particular image of the self, we could interpret as another appearance of the hacker as a cyborg figure, in terms of imagining oneself to have extra-sensory abilities. Hackers are not only gifted with a brilliant mind or a mind than enables them to master technology (Turkle, 1984), but perhaps also with an extended mind/body that enables them to track down injustice.

Connected with the ability to see certain things or wrongdoings, some respondents also highlight some heroic features of the hacker. The most prolific example is again provided by Jan, who compares hackers with members of the resistance movement in WOII who killed the Germans. He stresses that certain problems require extraordinary measures and ultimately those actions will be rewarded and appreciated. In a different vein, doing more good than bad or being a 'savior' or 'helper', is also brought forward by some of the black hat hackers. Dylan, who was involved in breaking into systems, e.g., points out that "*I did quite some*

bad things in my hacker career. Yet, the companies would be eaten alive, if we low or mid-tier hackers would not exist to educate them." Whether engaged in licit or illicit hacking, hackers generally adhere to their own moral rules or principles in which they strongly believe. This also involves that you can break rules or 'rip off the system' when you do not agree with it[42] or find it unfair. In this context Kevin (ex-black hat hacker) provides a rather different example: *"There was this "free-to-play" game where users could receive ingame advantages by paying money. I really hated the idea that someone can be better in a competitive environment just because he has money. So I've used what should really matter in gaming – skill. I've hacked into the site and generated retrievable codes for the ingame currency/advantages."* The notion of breaking rules and having your own ethical standards, is something that we can also connect with what Blankwater (2011: 47) refers to as "an attitude of *everything is possible"*: do not let barriers (like security, laws, copyrights) hold you back, but take it a step further." Hackers seek to explore new frontiers and go against existing ones. For them, "boundaries are seen as unnatural" (Turgeman-Goldschmidt, 2005: 20). According to Jan, hackers also feel the strong urge to prove that they are right, even if this requires that you have to do something illicit. In this context he refers to an example in which a hacker informed a web shop about a leak, which enabled to order goods for free. When the company refused to listen, the hacker ordered one of their couches and sent it straight to the office of

[42] This element of resistance is actually also a theme in Latour's work, which is why the perspective is also valuable for the understanding of hacktivism (see Taylor, 2005)

the company. Jan reflects on this example by saying: *"As a hacker you want to be the master and ruler of the system. This is what I call: releasing the hacker inside of you."*

4.5.4. Cyborg body – how hackers (simultaneously) compete with technology and themselves

The hacker-technology relationship also manifests itself in a competitive way in the sense that hackers feel the urge to explore and extend their mental and physical capabilities and limits (e.g. *"Am I able to do it? "How much power do I have on the Internet?"*) as well as the technical ones (e.g. *"What can it do?"* and "*What will happen when I do this?"*). For most of the interviewed hackers, challenge is a necessary condition to enjoy hacking, which is why they are setting higher goals all the time. Paul, e.g., points out that he always selected the more challenging targets to hack rather than the easy ones. According to Eric, the challenge can also fade away once you are able to hack everything you already wanted to hack. Yet, the challenge he still considers to be important in his current work in the field of incident response. Eric explains: *"If something goes wrong and managers stress out, I perform perfectly. I like the feeling when you are in the middle of it, everything goes wrong, everything collapses, people cry and go home. Then you know, it is no time for joking, now it is serious. You are not allowed to make mistakes."*

The example that Eric provides clearly resembles Lyng's (2004) proposition that edgeworkers have to and like to rely on their body to 'instinctively' respond to the evolving and overwhelming circumstances.

Yet, in the case of hackers they count much more on their mind than on their physical body. In this context we can also draw a parallel with the robbers described by Katz (1988). He points to their 'ability to always know what to do' when facing chaos (p. 235). Robbers also have a superior ability in terms of being (street) smart rather that to rely on physical force, something that also counts for hackers. In addition, Katz speaks of game-like and sport-like features in the context of robberies, elements that are also highlighted by some of the interviewed hackers. Paul always took, what he calls, a 'cooling down period' after he managed a hack, a term used in sports. Speaking of sports, the capabilities of the physical body do still matter in hacking as well, e.g. hackers often exhaust their body without proper sleep (see also Turkle, 1984). Like sports and gaming, hacking also has a strong element of competition with peers: to be better and faster than other hackers. Paul states that he is proud of the fact that he was able to hack one of the largest companies in the world. *"Then you really think: I did it. There are hundreds of them out there, but I did it. Pride yes, victory."* Eric points out that he always left a sign on the servers that he hacked: *"I wanted to let others know that I was there, that they would think: ah him again. That is the feeling I wanted to generate."* Here we can also draw an equation with graffiti writers who also seek to leave lasting marks and images (see Ferrell, 1996).

Yet, as Nikitina (2012) and Turkle (1984) also point out, hacking also entails the desire to 'beat the system' rather than merely another person. In that sense they do not merely compete with themselves and with other hackers, but also with the machine. This aspect can be also found in Paul's

description: "*You can be busy for weeks and still realize that you won't manage, but still you keep looking for that one spot you might have missed.*" The importance of challenge and competition might also put the proposition that for hackers the process is more important than the result (see e.g. Steinmetz, 2015) into a different perspective. Perhaps for hackers, at least for those mainly active in illicit hacking, process and result might be of equal importance or could be intertwined.

4.5.5. Cyborg transgression – how hacker's experiences and intentions are co-shaped by technology

The interviewed hackers also refer to their relationship with technology in the context of emotions, decision-making and intentions. It is this (interactive) process that generates many aspects of the hacker's experience, feelings and emotions. Kevin for example explains: *"When I hacked the first time I was very well aware that it was illegal. However, when you do this the first few times you get in a sort of trance. You forget everything and are just amazed and pumped with adrenaline because you have just entered a system which might hold information you are not supposed to see, or the system has very big specifications (big hard drive, a lot of memory etc.) which you have never seen before."* The quote suggests that there is not merely 'the invitational edge' of doing something illegal, which produces 'the thrill', but that the features or 'beauty' of the system also co-produces the adrenaline rush. For Paul, managing the hack is actually more important than doing something illegal per se. He explains: "*You dedicate yourself to one particular thing you are good at [hacking], that is your passion. Whether it is legal or illegal, it did not bother me at all*

that time." Paul frequently uses the expression of "*going (completely) wild on the system*", which, as he puts forward, gives a feeling or sensation that nothing else can resemble. He also points out that there were periods in which he was not able to sleep without the sound of the computer on the background. Hence also through sound the hacker can become *one* with the machine.

While black hat hackers are not always aware of the boundaries between licit and illicit hackers, do not care or like the thrill of doing something illegal, white hat hackers are more consciously aware of the legal context in which they operate. According to Jan, you have to strictly follow the rules of 'responsible disclosure', which entails that you should do nothing else than necessary for exposing the 'leak' alias 'the abuse by the company'. Yet, after you are (finally) able to enter a server, you have to stop and really need 'to control yourself', something that, according to Jan, is difficult for many young hackers. He explains that, once you are able to enter the system, you can become 'too curious', e.g. by reading all the information on the server you encounter. In other words, the original intention (to expose a leak) might change or, to speak in ANT terms, 'translate' into something more *illicit* once a hacker crosses the technical edge of entering the system. At the same time, like driving a car, the feeling that a hack generates does not match with the rules that you need to follow. Paul, who does not seek to hack illegally anymore, also brings up this issue. "*I want to do it good now, but I did it wrong as well. But I have to say that, I am often seduced to do it again when I look at certain*

systems. 'Breaking in' is still in my way of thinking, but I try not to do it. Once I will start I will drown in it again".

Last, alongside the legally restrictive context, hackers maneuver in an online environment where a different set of rules applies or where there is an absence of any rules. Eric explains how it works in the black hat scene: *"There are borders but they get blurry fast. If you are raised in a group where everybody carries guns, then you will find it normal after a while to carry one yourself".* According to Jeffrey (ex-black hat hacker), young hackers often do not know what to do with their computer talent. *"They are physically not in the right environment and there is no one to tell them that their actions might be malicious after all. There is no one to help them in their development and growth and to guide them in the right direction."* Hence, intentions and moral perceptions cannot be understood in isolation from the digital (anonymous) environment in which the hackers are 'flowing' and 'acting'. Some interviewees also point out that they consider their online life or identity as something secretive or a 'hidden side' of themselves. In other words, digital technology enables them also to be released *from* the body and to explore multiple identities simultaneously. Also this aspect we can link with the notion of cyborg (see also De Mul, 2002).

4.6. Concluding remarks

"What people do with computers weaves itself into the way they see the world" (Turkle, 1982, 173) and *"see themselves"* (p. 183).

This study aimed to shed light on how hackers give meaning to themselves and their actions, by drawing more explicit attention to the hacker-technology relationship. By employing the cyborg-perspective of ANT, this study was able to illustrate and explore the various ways in which this relationship takes shape, ranging from directive, functional and cooperative to more intimate, emphatic, competitive and mutually affecting. In accordance with Turgeman-Goldschmidt (2008), this study also found that the 'good' and 'bad' hackers, as far as you can make this division, show more resemblance than initially expected. The interviewed hackers generally perceive themselves as non-criminal actors who possess a very specific skillset and mindset, which sets them apart from others. They picture themselves as figures who possess an 'extended mind' or 'extra sense' that enables them to see and move through, beyond and against systems, not only technical ones. Whether black, gray or white, they all explore the boundaries and capabilities of technology and themselves simultaneously and all believe to do more good than bad.

To some extent they also view themselves as superior and somewhat superhuman, almost like the cyborgs we encounter in science fiction movies: superhuman rebels fighting evil (Wood, 1998). Yet, rather than

relying on the force or strength of the body, hackers seem to count on their 'innate' technological, mental and creative skill and consider themselves (or imagine themselves) as being equipped with certain abilities that most people do not possess. Hacking also seems to involve some hybrid type(s) of (embodied) experiences of its own, e.g. visible in the example of 'not being able to sleep without the sound of the computer.' Despite of their (perceived) difference, hackers also show resemblance with other deviant groups (e.g. professional thieves, robbers or graffiti writers) and other non-criminological phenomena such as gaming and sports. Hence, we should perhaps also not over-exaggerate their uniqueness, although they would probably not mind.

This study also aimed to make a contribution to the conceptual understanding of hackers, by applying the cyborg-perspective of ANT. It explored whether ANT's way of looking at the human-technology relationship enables to unravel aspects of hacking more comprehensively than a traditional criminological (anthropocentric) lens. While valuable studies have been conducted already to grasp the hacker phenomenon, ANT's cyborgian lens certainly brought a new layer to the conversation – theoretically and methodologically. Firstly, ANT draws attention not only to how humans relate to and learn from other humans, but also to how they interact with or relate to their device, computer or technology in general and what such an interaction entails and means for them. Rather than looking at the hacker as a human actor, ANT enabled to look at the 'hybrid' capacities in which a hacker can act, ranging from the 'hacker-tool', 'hacker-software' to 'the hacker-gun'

hybrid. By adopting this perspective, this study was able to reveal that 'interacting with technology' is intrinsically linked with becoming and experiencing to be a hacker and the associated intentions, perceptions and emotions.

Secondly, like Haraway's (1987) broader notion of the cyborg, ANT provides a perspective that seeks to eliminate dualistic thinking, an approach that particularly fits well with hacking as both a practice and a particular type of transgression. This study revealed that hackers somewhat drift across several boundaries simultaneously: the human and the technical, the online and the offline, the real and the virtual, the creative and the parasitic, the rational and the irrational, the licit and the illicit, the good and the evil and so on. At the same time, hackers seem to be engaged in establishing boundaries themselves. For instance, they have a clear view on who/what can call himself a (skilled) hacker and to which rules they should obey. The complexity and co-existence of boundary breaking and boundary fixing we were/are only able to capture more comprehensively if we do not *a priori* maintain any of such boundaries and only look at the boundary performing activities of the actors that we study.

To conclude, if we criminologists want to explore and understand the world of hackers and other high-tech cyber deviants more deeply and profoundly in the future we have to extend our focus *beyond* the human, gain more criminological knowledge on the (deviant) human-technology relationship and seek to dismantle existing dualisms and dichotomies

that still prevail in criminology. The cyborg-lens of actor-network theory provides a valuable and thought-provoking framework that can contribute to such endeavor. Future research could further enhance this perspective by conducting additional and more extensive fieldwork among different groups of hackers. The perspective is also worth considering in the context of other forms of technical deviance. As mentioned in the introduction, many tools that can be used to cause severe damage (e.g. RATs or tools for launching a DDoS attack) are ready at hand for the current young generations. It would be worthwhile considering whether the accessibility and commodification of such tools truly contributes to youth's engagement in technocrime.