From cybercrime to cyborg crime

van der Wagen, Wytske

From Cybercrime to Cyborg crime

An exploration of high-tech cybercrime, offenders and victims through the lens of Actor-Network Theory

Colofon

Print: De Boekdrukker, Amsterdam

Cover design & lay out: Wytske van der Wagen

ISBN 978-94-034-0622-0

rijksuniversiteit groningen

From Cybercrime to Cyborg crime

An exploration of high-tech cybercrime, offenders and victims through the lens of Actor-Network Theory

Proefschrift

ter verkrijging van de graad van doctor aan de
Rijksuniversiteit Groningen
op gezag van de
rector magnificus prof. dr. E. Sterken
en volgens besluit van het College voor Promoties.

De openbare verdediging zal plaatsvinden op

donderdag 14 juni 2018 om 12.45 uur

door

Wytske van der Wagen

geboren op 21 mei 1983
te Oostdongeradeel

Promotores
Prof. dr. R. Van Swaaningen
Prof. mr. dr. B.F. Keulen

Copromotor
Dr. M. Althoff

Beoordelingscommissie
Prof. dr. G.P. Mifsud Bonnici
Prof. dr. R.J.H.M. Staring
Prof. dr. B. van den Berg

Acknowledgements

"It is good to have an end to journey toward; but it is the journey that matters, in the end" (Ursula K. Le Guin)

This dissertation is an exploration of high-tech cybercrime from an actor-network theory lens. When I started this research project some years ago, cybercrime was still a rather underexplored topic in criminology. This has changed rapidly within the last few years. Cybercrime has become an important research topic on the criminological agenda, both nationally and internationally, and this will probably remain so in the future. With my dissertation[1] I hope to make a valuable contribution to the criminological understanding of high-tech cybercrime and to stimulate further theoretical debates on the role of technology in crime.

This PhD research, like any other one I suppose, was definitely a journey, a metaphor that I also use in this dissertation. Throughout this research I found some new interesting paths and directions, but I also encountered some obstacles and delays on the road. One thing is for sure: engaging yourself with actor-network theory can be both a blessing and a curse. Apart from an intellectual challenge, a PhD project is a mental and even physical contest. The last few miles are, of course, always the

[1] This PhD research was funded by the University of Groningen, Faculty of Law.

toughest. I am therefore very delighted that this journey has come to an end. Of course, it should be underscored that this was definitely not a solo-journey. To speak in 'Latourian terms' already, various other actors were involved in enabling, shaping and accomplishing this PhD project. For now, I would like to mainly stick to the 'human' ones.

First of all, I would like to thank my promotores René van Swaaningen and Berend Keulen for their guidance, inspiration and patience throughout the years. I am particularly grateful for the fact that René, who actually got involved in a later stage of this PhD, gave the research project a new and positive boost. His enthusiasm and persistence encouraged me to successfully complete this PhD project and gave me the confidence to really 'carry on' and 'bring it on'. The exact same thing could be said for my co-promotor and daily supervisor Martina Althoff, on who I could always count. Apart from her enthusiasm, dedication and insightfulness, she gave me a lot of useful advice and guidance concerning how to manage and organize a PhD project. I would also like to take the opportunity to thank Wolter Pieters, who was co-author of two articles in this dissertation. It was a great pleasure for me to cooperate with him and his critical input I highly appreciate. I also would like to thank the members of the assessment committee for their time, assessment and constructive feedback. The final product, this dissertation, could not become 'a fact' without their effort and judgment.

My gratitude also goes to the Team High Tech Crime of the Dutch National Police for their cooperation, trust and enthusiasm. This team

provided me the access, sources and unique opportunity for conducting research on high-tech crime cases. In particular, I would like to thank Frank Bernaards and Floor Jansen, who were positive about this research project from the start. They definitely made the police file analysis run smoothly and made me feel at home at their team. The same counts for the Public Prosecutor's Office in Rotterdam, in particular Lisanne van Dijk, who also gave me the space and opportunity to analyze files. I would also like to thank the respondents who participated in the research. Without them, the research would simply not be as fruitful and valuable.

Next, I would like to say thanks to all my (PhD) colleagues from Groningen University that I worked with or spend time with throughout the years: Min Jung, Gerard, Anne, Kim, Karen, Eva, Annieke, Nicole, Rolf, Stephanie, Rick and also colleague and friend Eleonora. Groningen University was a great place for me to conduct the research. Although I was principally the only 'criminological' PhD candidate among the legal ones, I always felt at home and I enjoyed the various activities that were organized by the Graduate School (the formal and the informal ones). I also would like to thank all my current colleagues from Erasmus University, who gave me lots of valuable (criminological) input, encouragement and the space for getting this PhD 'really' done. I am very grateful for the fact that I am working and will continue working at this great department and university.

Last, but not least, I would like to thank the people in my private circle. First of all, many thanks go to my partner Artur, who witnessed the 'backstage' of this PhD research from start to finish. Moving with me from Amsterdam to Groningen and back, living in New York for some time, I could always count on him. During the multiple dog walks we had, we always came to the same conclusion: 'really, really, REALLY finish it soon!' Now the job is finally done and hopefully there will be space for many other important topics to discuss. Second, I would like to thank my parents, two sisters (Fenny and Tjitske) and brother (Eelke), who were always very confident about the fact that I would eventually complete the dissertation. It is really great that they have always supported me in all the (career) choices that I made and are proud of me no matter whether I succeed or not.

I also want to take the opportunity to say thanks to all my friends. I am very grateful for their encouragement and understanding for me being quite 'non-social' for the last couple of years. My first special thanks go to Sanne van den Tillaar and Eva Koppen, with whom I became very close friends during my studies. It is great to have the both of you as my paranymphs. The other special thanks go to my friends Janneke Dijkstra and Micha Kroese who always remind me of the fact that there are many other important things in life except for work. I suppose, at least I *hope*, that the post-PhD life offers more time for talks, trips, laughs, drinks and sports. However, in the academic world, the PhD is merely the start of it all. In that sense, the (academic) journey is actually just starting and much more work is left to be done.

Table of content

Chapter 1

Introduction: Cybercrime, the novelty debate and the frontiers of criminological theory*

* This chapter is partly based on:
- Van der Wagen, W. (2013). Een hybridisering van mens en technologie. Over nieuwe dynamieken in de studie van cybercrime. In A. Dijkstra, B.F. Keulen & G. Knigge (Eds.), *Het Roer Recht. Liber amicorum aangeboden aan Wim Vellinga en Feikje Vellinga-Schootstra* (pp. 323-336). Zutphen: Uitgeverij Paris.
- Van der Wagen, W. (2018). Het 'Cyborg Crime' - perspectief. Theoretische vernieuwing in het digitale tijdperk. *Tijdschrift over Cultuur en Criminaliteit*, (8) 1: 19-34.

1.1. Introduction

"Our machines are disturbingly lively, and we ourselves frighteningly inert" (Haraway, 1991: 152)

The Internet, computers, smartphones, Facebook, virtual worlds and many other contemporary technologies and applications are increasingly becoming an integrative part of our human existence (Brenner, 2007). We live more than ever before in, what Consoli and Hoekstra (2008) denote as a 'technologized context' in which technology is not merely omnipresent, but also has become indispensable in all facets of our daily lives, practices and experience. As a matter of fact, we become completely deranged when the Internet is not working and a life without a smartphone is almost unimaginable. Indeed, to some extent we have become, as Donna Haraway announced already more than 25 years ago, 'cyborgs': hybrid creatures of human and machine. With her 'Cyborg Manifesto' she wanted to emphasize that it is increasingly difficult to maintain strict boundaries between the human and the technical, but also between the organic and the artificial, the fictional and the real (Haraway, 1987; 1991).

Undoubtedly, digital technology has also become an integrative part of crime and deviant behavior. Technological innovations transformed or digitalized existing crimes, but also co-created various new more 'high-tech' types of crimes (Furnell, 2002; Holt, 2012; Wall, 2007) such as Distributed Denial of Service (DDoS) attacks, computer hacking, banking

malware and ransomware. While these crimes can be technically sophisticated, some of them are just a mouse click away. A good example is the recent series of DDoS attacks[2] (2018) on three Dutch banks and the tax administration, which paralyzed their systems for several hours. The arrested 18-years-old suspect declared that he carried out these attacks just for the fun of it, while the damage was immense.[3] These types of crime generally also have a rather automated nature, implying that they rely on an army of machines (also termed botnet) rather than on people. Hence, the 'rise of the machines' is not entirely science fiction any longer[4]; it is actually happening already. In addition, crimes have emerged that have a virtual, even fictional character. Virtual theft, virtual child pornography and virtual rape are the best-known examples. They take place in an artificial setting or are completely artificial in nature, but can have 'real' consequences. In other words, also in the criminal domain it becomes increasingly difficult to draw sharp lines between the human and the technical, the organic and the artificial and the fictional and the real. These developments in turn pose various new questions and challenges for the criminological understanding of offending and victimization and the ensuing applicability of existing criminological theories and concepts, which were mainly developed in the pre-digital age. For instance, should we start considering technology as an actor if

[2] DDoS stands for a distributed denial-of-service attack. These attacks seek to make (web) servers inaccessible by sending out an explosive amount of requests
[3] See:
http://www.omroepbrabant.nl/?news/274508962/Van+hack+op+school+tot+DDoSaanvallen+op+overheidsinstellingen,+Jelle+(18)+wist+niet+van+ophouden.aspx
[4] See also http://www.crimeur.nl/cyborg-crime-sciencefiction-of-sciencefaction/

its role is so significant and if crime gets increasingly automated and robotic? Must we extend our understanding of cyber offenders and victims beyond the human and adopt a more post-human approach in criminology? These are the type of questions that lie at the heart of this dissertation.

Throughout this first chapter I aim to sketch the background, central objective, focus, relevance, theoretical framework and research strategy of this dissertation. First some definitions and classifications of cybercrime will be outlined in order to provide a brief picture of what kind of offenses fall into the category of cybercrime. Next, I will discuss some (a)typical or 'new' features of cybercrime pointed out in the literature, and why these features challenge the existing criminological theoretical repertoire. In this context, I particularly highlight the issues that have received relatively little attention in the novelty debate and outline why they need further theoretical consideration in light of current cyber developments. This theoretical context in turn sets the scene for presenting the research aim and central questions of this dissertation and its relevance for and contribution to criminology. The chapter continues by considering the core assumptions of actor-network theory (ANT), the central approach in this dissertation. I will explain why this particular theory plays such a leading role in this PhD research and also how the approach has been explored in the empirical chapters of the book. In the following methodological part, the chapter describes the overall research strategy, including its strengths and weaknesses. In the end of the chapter, a reading guide of the dissertation will be provided.

1.2. Cybercrime: terminology, definition and classification

While 'cybercrime' is generally the prevailing term used to refer to cyber-related offenses (see Wall, 2007 for a discussion on the term and its roots), we can also find various other terms in the literature that refer to the same phenomenon (or a subset of offenses) including 'netcrime' (Mann & Sutton, 1998), 'Internet crime' (Burden & Palmer, 2003; Jewkes & Yar, 2010; Jaishankar, 2011), 'hypercrime' (McGuire, 2008), 'virtual criminality' (Capeller, 2001; Grabosky 2001), 'high-tech crime' (Van der Hulst & Neve, 2008), 'computer crime' (Casey, 2011) and 'technocrime' (Steinmetz, 2015; Steinmetz & Nobles, 2017). This dissertation uses the term cybercrime as a general term that covers all cyber-related forms of crime and deviance and adds the adjective 'high-tech' when it specifically concerns the more technical crimes.[5] As the dissertation title also displays, this dissertation mostly focuses on the analysis of the latter type of crimes (see further section 1.6).

The fact that the phenomenon of cybercrime involves a broad variety of offenses, explains that most definitions are rather broad. Yar (2013: 9), for instance, defines cybercrime as: "a *range* of illicit activities whose 'common denominator' is the central role played by networks of ICT in their commission." Similarly, Gordon and Ford (2006: 14) define it as "any crime that is facilitated or committed using a computer, network, or hardware device." The definition of Thomas and Loader (2000) is not

[5] Chapter 4 uses the term 'technocrime' as this article will be published in a special issue on 'technocrime on the margin.'

that much different either, although they emphasize that it can also involve non-criminalized activities. They consider cybercrime as: "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (p. 3). As these definitions are quite all encompassing, it might be more constructive to look at some of the classifications of cybercrime and the various offenses that they capture.

The most commonly used classification in criminology is the distinction between 'computer-enabled' and 'computer-focused' crime (Furnell, 2002). The first type refers to traditional forms of crime, that are conducted by means of ICT (e.g. cyber stalking, fraud) and the second type concerns crimes which are not merely executed by means of ICT but also targeted against it (e.g. the spread of viruses or hacking). In this way, cybercrime is basically considered as a "continuum ranging from crime which is almost entirely technological in nature and crime which is really, at its core, entirely people related" (Gordon & Ford, 2006: 15). Koops (2010) provides a typology in which the Internet is considered as either the object, the instrument or the environment. This categorization is based on how the Council of Europe's Cybercrime Convention has criminalized cybercrime. The Council distinguishes the following categories (*Idem*: 738):

1. Offences against the confidentiality, integrity and availability of computer data and systems (e.g. hacking, spreading viruses, distributed denial of service attacks)

2. Computer-related offences (e.g. forgery and fraud)
3. Content-related offences (e.g. child pornography) and copyright offences (e.g. music piracy)

The last typology to consider is Wall's (2007) classification, which depicts three subsequent generations of cybercrime. This classification is based on the 'level of novelty' involved, denoted as the 'transformation thesis' (p. 4). The first generation concerns crimes in which the computer is used to commit traditional crimes. These crimes are basically 'old,' yet take place with new technologies. Examples of these crimes are cyber stalking, hate crimes and (small-scale) cyber fraud. The second generation includes traditional forms of crime, which now have a more global character. They are old when it comes to the basic offense itself, but new with regard to the employed instruments and their scope. Examples of these crimes are large-scale fraud or scams in which multiple victims are targeted at the same time. In these crimes, technology acts as a 'force multiplier,' referring to the principle that one individual can potentially commit crime on a large scale (Yar, 2005a; Wall, 2007). The third generation points to the so-called 'true' cybercrimes, crimes that are fully generated by network technology. They have a distributed and automated character, are not restricted by time and space and would completely disappear if the Internet would cease to exist. Examples of this category are (banking) malware, hacking, spam, DDoS attacks and the creation of botnets. In these crimes, technology is not only a force multiplier, but also the target of the crimes. As these crimes fully take place in a cyber context, Wall (2007) calls them

sui generis ('from their own kind'). He also includes crimes in this generation that take place in virtual worlds, such as cyber rape or cyber theft (see further subsection 1.3.5). In addition, he suggests (but not extensively specifies) the emergence of a fourth generation, involving crimes that take place through the opportunities generated by so-called 'ambient intelligent networks' (see Wall, 2007: 48).

Now we have an overview of which offenses fall under the heading of cybercrime, it is fruitful to consider if and in what way cybercrime is different than traditional crime. This is important in relation to the question whether traditional criminology's framework will (still) have theoretical potential in the cyber world.

1.3. (A)typical features of cybercrime: a brief literature overview

While earlier technological innovations and revolutions also had a significant impact on crime and its commission[6] (McGuire, 2008), it can be argued that the Internet had an impact that was far more profound (Wall, 2007). The intensity of the Internet transformation most likely explains why we never spoke of a 'telephone space', 'telegraph space' or 'postal space', while these technologies also increased the opportunities for social interaction (McGuirre, 2008). Various scholars have discussed

[6] As Wall (2007: 2) points out: "Some of the nineteenth-century wire frauds perpetrated by tapping into the early electric telegraph systems, for example, bear an uncanny resemblance to modern day hacks."

the implications of the digital revolution upon criminal activity and the criminogenic features of cyberspace itself. In the following I will outline some of the main new features that are discussed in the literature. Some features apply to all forms of cybercrime, while others apply more specifically to the high-tech crimes or the virtual crimes.

1.3.1. The collapse of spatial-temporal barriers

Deterritorialization and globalization are key dimensions characterizing the nature and scope of cybercrime (Wall, 2007; Sandywell, 2010; Yar 2005a; 2013). Cyberspace is basically a borderless world without the restrains of time and space typical for the terrestrial world (Cairncross, 2001). One of the most important implications of this 'time-space compression' (Harvey, 1989) is that it enables offenders to target multiple victims around the globe without ever leaving their home (Koops, 2010; Wall, 2007; Yar, 2005a; 2013). Crime and victimization can therefore take place on a rather different scale. According to Wall (2007), the seriousness of many forms of cybercrime lies in their globalized aggregate impact or volume: a principle of low-impact crime with multiple victims. For instance, rather than stealing a large amount of money from one victim, digital technology enables to carry out millions of thefts of one euro. This principle of 'de minimism' might not only "affect the way we construct victim profiles" (Wall 2007: 19), it also challenges an adequate response from law enforcement agencies. As the harm per victim is so small, the incentive to investigate and prosecute these crimes decreases substantially (see Koops, 2010). A similar, though

different principle we can observe in the earlier mentioned botnets. This involves a network of infected computers (often located all around the globe), which all together (not individually) serve as a powerful tool to launch a (devastating) cyber-attack on one or multiple targets. The fact that cybercrime is by nature so international, global and distributed also goes hand in hand with various other challenges for law enforcement agencies, including jurisdiction problems and challenges in the scope of cross-border cooperation (*Idem*). Yet, not all cybercrime is per definition international. Various cybercrimes, including hacking, can also take place in a more local setting (see e.g. Leukfeldt, Domenie & Stol, 2011).

1.3.2. Force multiplier effect, automation and amplification

The technical dimension of cybercrime is obviously another important key characteristic of cybercrime. As pointed out above, technology enables that an offender can target manifold targets instantaneously with minimal efforts, hereby putting quite "some power in the hands of the individual" (Wall, 2007: 39-40). The notion of 'force multiplier' also goes hand in hand with the automation of criminal activities or processes: "One piece of software launched on the Internet can replicate and attack millions of computers at the same time – but also over longer periods of time" (Koops, 2010: 740). Some forms of crime require basically just a few mouse clicks and the tools to carry out such attack are also widely available. The earlier mentioned DDoS attack is perhaps the clearest example of this. The distributed and automated nature of (high-tech) cybercrime also entails that it is not predictable at forehand how much

damage the crime eventually may cause, which is e.g. also clearly visible in the context of the spread of viruses, which 'by nature' have a contagious character. This in turn might "blow up the *scale* of a crime from a minor nuisance to major harm" (Koops, 2010: 740). In that sense, technology might give a person a lot of power, but he or she might not be able to fully empower technology (see chapter 2). Speer (2000) speaks in this context of gray areas in cybercrime, as offenders might not be fully aware of the possible consequences of their actions. As Hayward (2012: 17) puts it: "digital technology creates what one might describe as porous spaces of subjectivity in which moves made via the rhizomatic, hyperlinked internet appear materially or spatially insignificant but, in reality, have tangible consequences."

A similar principle of unpredictability and amplification counts for the spread of (criminal) ideas. As Deibert and Rohozinski (2010) point out: "Once released into cyberspace, the distributed properties of the network help [criminal] ideas and information circulate, duplicate and proliferate." In this respect Wall (2007) argues that networked technology is actually more than 'just' a force multiplier. Computing power does not only enable that ideas for committing crime are spread on a global scale, but also on an ever-increasing speed. This also brings us to another important technical dimension of cybercrime: the rapid innovation cycles involved. The tools and methods used to commit cybercrimes develop and improve in an extremely fast tempo (Koops, 2010).

The same counts for the manner in which vulnerabilities are exploited. One of the most recent developments is that personal information (e.g. banking details) can be stolen or accessed by hacking into someone's brain. By hacking neural devices so-called 'neurocriminals' are able to get "illicit access to and eventually manipulate information in a manner that resembles how computers are hacked or cracked in computer crime" (Ienca, 2015: 51). As this example clearly reveals, some offenders know exactly how they can exploit the devices and technologies we are attached to, as they know how the underlying technologies work and we (users) do not (Goodman, 2010). Cyber offenders are also innovative when it comes to the techniques they can employ for operating and trading off the grid. Offenders can use e.g. VPN and proxy-servers[7], TOR/Onion Router[8] and encryption[9] (see e.g. Van Hardeveld, Webber & O'Hara, 2017), making it extremely difficult for law enforcement agencies to identify, detect, arrest and prosecute the offenders (Koops, 2010).

1.3.3. Social and technical interconnectivity

Cyberspace or the Internet enhanced the opportunities for social interactions significantly, also in the criminal domain (McGuirre, 2008). As Wall (2007) points out, in the Internet era various communication

[7] See chapter 2 for an explanation of this technology.
[8] This involves a browser that offers anonymity see: https://www.torproject.org/projects/torbrowser.html
[9] "Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it" (https://digitalguardian.com/blog/what-data-encryption).

technologies converged, broadening the number of technologies that enable to globally connect (deviant) individuals, more than ever before. In the Internet era everything and everyone can interact anytime with anyone anywhere instantly, also termed 'many-to-many connectivity' (Yar, 2005a: 411). According to Goldschmidt and Brewer (2015), the Internet hereby produced a completely new or different criminal interactional order. For instance, while pedophiles in the pre-digital age used to operate locally, isolated and secretly, communicating only with a few others, the Internet (e.g. web forums, newsgroups, chat rooms and file sharing) enables to have and maintain multiple anonymous contacts simultaneously. In other words, the features of technology come along with a certain usage of it and can also transform the frequency and the manner in which offenders meet and interact. Soudijn and Zegers (2012) introduced the concept of 'virtual convergence offender settings' in this context to pinpoint that offenders also have particular locations in the online world where they gather. These online settings differ however from their offline counterpart when it comes to anonymity and the manner in which trust has to be established. Another important feature or aspect of co-offending in cyberspace is the fact that offenders are highly dependent of one another for gaining access to the right knowledge and the various tools and services that are necessary to organize and execute cybercriminal activities. The cybercriminal underground basically works as a 'tool as a service' (Tropina, 2016) or a 'crime-as-a service' model (Odinot et al, 2016). This also goes hand in hand with a high level of specialization. Some actors develop the code of the malware and others are specialized in its distribution (Choo, 2008;

Leukfeldt, Kleemans & Stol, 2016; Odinot et al, 2016). In other words, not only the offenders, but also the crimes are rather interconnected, forming a chain of different activities (Brenner, 2002; Wall, 2007).

1.3.4. Anonymity and plasticity of the online identity

Another important aspect featuring cyberspace and cybercrime is anonymity. The Internet enables people to use pseudonyms, to manipulate their identity and (again) to stay hidden for possible arrest (Yar, 2005). Being anonymous also comes along with certain psychological aspects that are worth discussing in the context of crime and deviant behavior. Suler (2004) in this context introduced the term 'online disinhibition effect', referring to the notion that anonymity takes certain behavioral restrictions away. This inhibition can manifest itself in a positive or negative way. On the one hand, online anonymity permits the exploration of new frontiers of one's social identity, to reinvent it (e.g. Yar, 2005a; Turkle, 1995; Stryker, 2012) and/or to more freely express oneself and her or his emotions (Hayward, 2012). The Internet can then be considered as "a tool for individual and social transformation" (Vicini & Brazal, 2015: 150) or even as a 'mental prosthesis' (Gaggi, 2003). On the other hand, anonymity can have a rather toxic affect. People can say or do things they would ordinarily not do and seek to explore the 'dark side' of themselves (Suler, 2004). Toxic disinhibition definitely plays a role in phenomena such as cyber bullying (see e.g. Kerstens & Veenstra, 2015), although it could play a role in all kinds of cyber-related offenses. In cyberspace offenders are generally not directly (face-to face)

confronted with their victim and the harm they (might) impose on them. They may even experience that they are active in a world that is less 'real.' As Suler (2004: 323) explains: "Consciously or unconsciously, people may feel that the imaginary characters they "created" exist in a different space, that one's online persona along with the online others live in a make-believe dimension, separate and apart from the demands and responsibilities of the real world. They split or dissociate online fiction from offline fact." This brings us to the last feature to discuss: virtualization and hybridization.

1.3.5. Virtualization and hybridization

Virtualization is another important feature of (crime in) cyberspace. The Internet has given rise to the emergence of virtual worlds or so-called role-playing games where virtual people build a virtual community or society together. "Second Life" is perhaps the best-known example (Vicini & Brazal, 2015: 150). While one might expect that such a virtual community enables Utopia – as it is a (bodiless) space without institutional and spatial limitations - it is far from being that (*Idem*, see also Castells, 2009). In these virtual contexts different forms of deviant behavior take place. The first example is virtual theft, which refers to the theft of virtual goods. As these goods have 'real' value, virtual theft is criminalized. This is a heavily debated topic among legal scholars (e.g. Guinchard, 2010; Moszkowicz, 2009; Strikwerda, 2012). Cyber rape, "the rape of an avatar (a person's virtual representation) in a virtual world" (Strikwerda, 2015: 491), is another example of virtual cybercrime. Unlike

cyber theft, cyber rape is not criminalized in the Netherlands, although some argue that it could fall into the legal category of 'sexual assault' (*Idem*). Virtual child pornography is a somewhat different example of virtual cybercrime. It refers to pornographic images that are not produced with 'real' children. Although there is no actual sexual abuse, the material (only if the virtual children look realistic) is forbidden to produce, to possess or to distribute. The protection of children is one of the underlying reasons for the criminalization.[10] In all three examples we can observe that these crimes are actually not exclusively virtual in nature. They always have a 'real' dimension when it comes to its (possible) consequences, either financially or emotionally. That is why they are also somewhat hybrid (see further chapter 5).

In short, cybercrime has some features and dimensions - globally, technically, socially, psychologically and virtually - that we cannot or to a lesser extent observe in traditional crimes. These features in turn bring various new questions and challenges concerning the sustainability of criminology's theoretical repertoire in the digital age.

[10] See for a full argumentation on this matter:
https://zoek.officielebekendmakingen.nl/kst-20012002-27745-299b.html

1.4. Criminology and the novelty debate

Already since the very beginning of the information age, criminologists debated whether cybercrime should be seen as an old or new phenomenon and to what extent existing criminological theories (still) have sufficient explanatory power (Van Erp, Stol & Van Wilsem, 2013; Yar, 2012; Holt, Bossler & Seigfried-Spellar, 2015). Grabosky (2001), for instance, considers cybercrime as 'old wine in new bottles' and does not see the urge for developing new theory. He claims: "technologies may change rapidly, but human nature does not" (p. 248). Yar (2005) and Mcguirre (2008) on the other hand, presume that the transformations that have been set in motion by digital technology, definitively require some adjustments or theoretical renewal.

Yar (2005), in this context, particularly elaborates on the environmental aspect; how criminologists should understand and conceptualize cyberspace as a 'space' or realm for crime. Based on the described features above (time-space compression, force multiplier effect, interconnectivity, anonymity and so on), he proposes to view cyberspace as a distinct space where a set of different interactional rules and principles apply. In turn he questions the applicability of the routine activity theory (RAT) (Cohen & Felson, 1979), which is strongly based on temporal and spatial notions. RAT explains offending and victimization through the convergence in time and space of the following three elements: the motivated offender, the suitable target and the absence of capable guardianship. Although these separate elements can be

translated to the cyber world; their convergence in time and space is rather challenging in cyberspace since this 'space' is not only 'anti-spatial' but also non-linear in nature. Despite of such criticism, RAT as well as the closely associated (online) lifestyle theory (Hindelang, Gottfredson & Garofalo, 1978), are to this day the most widely applied approaches in the predominantly positivistic orientated cyber criminological discourse (see for an overview Holt & Bossler, 2014). Criminological theories such as the labeling approach (e.g. Turgeman-Goldschmidt, 2008) and (other) cultural criminological perspectives (e.g. Steinmetz, 2015) received considerably less consideration.

Unlike Yar (2005a), McGuirre (2008) does not consider cyberspace as an ontologically distinct space, but views it, following McLuhan (1964), as an extension of the physical world, which he denotes as 'hyperspace'. He takes a critical stance towards the notion that cyberspace is some sort of lawless 'wild zone', existing separately from the physical world. According to him, such vision clearly reflects the (criminological) failure of not being able to adequately embed technology in the social world. Also various other authors point out that it is not fruitful to consider the offline and the online world as two separate realms, but to pay attention to how cyberspace is rooted in the 'real world' (Castells, 2001) and how these worlds are intertwined (e.g. Franko Aas, 2010; Brown, 2006; Giese, 2008; Turkle, 2005). As Greer (in Franko Aas, 2010: 551), for example, points out: "To continue considering, as many criminologists have, the cyber – and the crimes that take place there – as a distinct realm with distinct rules, is to fail to recognise the 'hybridity' of reality and the

varying degrees of virtuality discernible in many contemporary forms of crime and control."

1.5. Adding another layer to the conversation – the theoretical context

It can be argued that a similar discussion is taking place, or more precisely, should take place when it comes to the ever-increasing interconnectivity or entanglement between the human and the technical. Also here it is questionable whether it is still desirable to treat them as two separate entities, domains or worlds. At the same time, this dualism raises some other issues. Apart from the question whether it is still desirable to maintain a binary division between the human and the technical, it also becomes relevant to consider whether criminology's theoretical repertoire is not too anthropocentric and instrumental (substantivistic) in nature when it comes to the understanding of the human-technology relationship (see also Brown, 2006). These three aspects or limitations - criminology being too instrumental, anthropocentric and dualistic – have received relatively little attention in the context of the novelty debate. In the following I will reflect on these three aspects more deeply, assess whether and how they have already been dealt with in (cyber)criminology and which dimensions need further consideration and theorization.

1.5.1. An instrumental view on technology's role in crime

The idea that criminology could be too instrumental is the first issue I would like to address. It can be argued that criminology traditionally perceives the relationship between the human and the technical in rather instrumental terms. Technologies (objects, tools, infrastructures, software) are merely seen as instruments, recourses or means to commit and to organize crimes or to prevent them, for which they obviously also serve. However, by considering and conceptualizing technology (or any 'thing') in merely an instrumental or functional manner, goals and intentions remain exclusively the domain of the human and technology the realm of the (neutral) means or instruments, also referred to as a substantivistic vision (Verbeek, 2005; 2008). It is however questionable whether such an approach is still sustainable in light of crimes that have a rather automatic and robotic character (see also Deseriis, 2017). As pointed out earlier, in these types of crime a part of the criminal act is carried out or outsourced to machines and it is also doubtful whether the human (offender) is still fully in charge and in control. At the same time it is too limited to view the (deviant) human merely as a (passive) 'user' of technology, as technology is so interconnected with what we/they do, think and experience (Brenner, 2007; Verbeek; 2008). A deterministic vision on the other hand, which views technology as an autonomous force, hereby making human agency far less relevant, is not very fruitful either. It would, for instance, argue that certain technologies are intrinsically evil. Viewing technology in terms of *mediation*, a vision that can be placed between these two extremes, is therefore a more prevailing vision within philosophy of technology (see e.g. Verbeek,

2005; 2008), where actor-network theory can also be positioned (see section 1.7).

That an either instrumental or deterministic view or treatment of technology is no longer adequate for understanding (cyber) deviant behavior and crime, is obviously not something that is completely ignored by criminologists. While theory development in this particular scope is still quite limited (Franko Aas, 2015), some studies have appeared recently, that explicitly look at and speak in terms of the mediating role of technology. A good example is the recent study of Wood (2017) on the effect of social media on deviant behavior. Following Kitchin and Dodge (2011), he claims that websites such as Facebook are equipped with a so-called 'technological conscious': "the unintended, unrestrained, and often harmful forms of gratification-seeking behavior that the site's architecture promotes in its users" (p. 170). According to Wood (2017), the algorithms that are used by such sites not only determine the content the users get to see, but they also co-shape the process in which deviant identities are formed. This concept in turn offers leads or a starting point to consider technology as a mediator or actor and also to put the interaction between the human and the technical more central.

The study of Hayward (2012) draws attention to a more subjective dimension. He focuses on the question how digital technologies can generate a context in which people experience reality. Concepts such as 'virtuality' and 'telepresence' can e.g. shed light on how communication

technologies can change the way online offenders experience their environment, ideas that can already be traced back to the work of Ervin Goffman. Goffman's notions of 'front stage and 'back stage', for example, are able to capture quite well the fluidity of online identities and deviant identity formation (Pinch, 2010). Goffman has also drawn already particular attention to the question how the materiality of (offline) technology can shape social interactions, e.g. visible in his work on the merry-go-arounds as a technical system shaping the relationship between riders and fellow riders and their audience (*Idem*). Hence, we can find examples in criminology where things or technologies are not merely treated and theorized in instrumental terms. Yet, as I will argue later, more work can be done.

1.5.2. Placing human agency in the center of the criminological inquiry

Apart from an instrumental vision, it can be argued that existing criminological frameworks are also (still) rather anthropocentric in nature. It is mainly the human agent who is placed in the center of the criminological inquiry. Non-humans (objects, tools, technologies, etcetera) are treated as passive, marginal and insignificant (Brown, 2006). Especially in the cyber domain, where technical agents play a rather important role in the offending process, such vision might no longer be adequate. Yet, also here some nuance would be appropriate. We can actually point out different places in criminology where the central position of the (individual) human as the offender or victim has been

debated already. For example, in green criminology various kinds of non-human victims are addressed, including animals, plants and ecosystems (Hall, 2013; Halsey & White, 1998). Exactly in this field the anthropocentric character of criminology is denounced (see further chapter 5). In addition, some subfields in criminology deal with non-human actors as offenders. A prominent example in this context is organizational criminology, which not only considers and studies persons, but also corporations or organizations as criminal entities (Tombs, 2017; Van Baar & Huisman, 2012). Yet, this body of literature does not particularly contest the non-human nature of the corporation as an entity, but rather its collective nature (read: 'collective of humans'). Hence, it is merely the individualistic, rather than the anthropocentric character of criminology that is called into question (Michalowski & Kramer, 2007).

Furthermore, cybercriminologists themselves have taken non-human offenders or victims into consideration, especially the latter. For instance, we can find studies that focus on companies as victims (e.g. Veenstra, Zuursteen & Stol, 2016) or on computer systems as targets (e.g. Maimon, 2015). As Yar (2005a) also points out, targets in cyberspace are more informational rather than physical in nature, which also highlights the digital nature of the victim as an entity (see also Smith, Bennet Moses & Chan, 2017). However, as will become clear throughout this dissertation, the (eventual) 'cyborg crime' perspective does not propose that non-human entities should be labeled as offenders or victims. It rather pleas for a more hybrid understanding of crime and victimization, in which

offenders and victims are considered in terms of networks (or collectives) of human, technical and/or virtual elements. This automatically brings us to the third point: the maintenance of dualisms.

1.5.3. Maintaining dualisms in an era of hybrids

As pointed out before, maintaining binary oppositions is no longer productive for a criminological understanding of cyberspace and the crime that takes place 'out there.' As Brown (2006) stipulates: "Criminology's traditional bifurcatory paradigms are peculiarly unsuited to the analysis of the complex technosocial characteristics of criminological phenomena" (p. 224). A principle of hybridity would be much more desirable when it comes to grasping the relationship between cyberspace and 'meatspace' (Pease, 2001: 23), but also between the human and the technical. Although this dimension has not received much theoretical consideration in criminology (see also Luppicini, 2014), we can find places in criminology where hybrids of humans and technology have already been discussed.

This is especially the case in the field of surveillance and security studies (see e.g. Franko Aas, 2006; Haggerty & Ericson, 2000; Schuilenburg, 2015). Haggerty and Ericson (2000), for instance, argue that in the digital age not the 'human' body is the subject that is under surveillance, but rather a hybrid composition or 'cyborg-entity' consisting of biological, technical and virtual elements: "First it is broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of dataflows. The result is a decorporealized

body, a 'data double' of pure virtuality" (p. 611). The associated concept of the 'surveillant assemblage,' particularly seeks to look at the relationship between the human and the technical or virtual in a networked manner. The notion of 'assemblage' (Deleuze & Guatarri, 1987), which also stresses the hybrid and complex nature of reality, therefore has quite some resemblance with the line of thought of ANT. It comes then to no surprise that ANT itself has also been applied in surveillance studies (see e.g Douillet & Dumoulin, 2015). Lastly, we can find some places in criminology where hybrid types of victimization are discussed. An example is the study of Whitson and Haggerty (2008), in which the notion of the 'datadouble' (the digital doppelganger of the human) is applied in the context of identity fraud victimization. The authors argue that the increasing digitalization not only has implications for the manner in which we become a victim, but also for the (lengthy) aftermath (see further chapter 5).

In short, while it can be argued that criminological frameworks are generally quite instrumental, anthropocentric and dualistic in nature, we can find examples that move away from such a view. Even the cyborg figure has appeared on the criminological stage (see also Suarez, 2015). Nevertheless, we can point out certain (hybrid) dimensions, which have not received much consideration, while they definitely deserve this in the cyber age. Firstly, as pointed out already, cyber criminologists have not drawn much attention to the question how an instrumental view (the goal-means-end rhetoric) stands in relation to the automatic and distributed nature of certain cybercrimes. Should we not assign agency

to technology or at least seek to conceptualize technology in more active terms?

Secondly, criminologists have not paid much attention to the conceptualization of the relationship and mutual interaction between offenders and objects or technologies. Although there is considerable attention for the question how technology, communication technology in particular, mediates in the mutual interaction between (human) offenders, there is barely consideration for how offenders interact with the tools themselves and give meaning to their relationship with technology. We have 'socially constructed deviants' (Becker, 1963), 'drifting deviants' (Matza, 1964) and 'voluntary risk-takers' (Hayward, 2002; Lyng, 2004) in criminology, but no hybrid or 'cyborgian' deviants (yet). How do offenders give meaning to the (malicious) software that they use, buy, rent or create? Can the tools that are employed in cybercrime be considered as entirely neutral? Also here a dimension pops up that has criminological relevance, yet is still theoretically underexposed.

Thirdly, the before mentioned hybrid 'network thinking', as we can mainly find in surveillance and security studies, has not gained much foot on the ground in cybercriminology, with a few exceptions. Should we not apply a similar (hybrid) way of thinking when it comes to cyber offending and victimization, where human, technical and/or virtual elements also come together? Would such view not better be able to grasp the hybridity and complexity that is featuring various forms of cybercrime? These

issues all together made me consider the ideas of actor-network theory (hereafter ANT), in particular the work of Bruno Latour. ANT presents itself as an anti-dualistic perspective, which also looks at the human-technology relationship in a more hybrid, symmetrical and interactive fashion. Therefore it could be able to counter some of the conceptual problems that criminology is facing in the digital age.

1.6. Research aim, central questions and relevance of the dissertation

1.6.1. Research aim and central questions

This dissertation aims to take a closer look at some of the main theoretical challenges criminology is facing in the digital age and to explore, by conducting four different case studies, how the conceptual framework of ANT can counter these challenges and offer a valuable alternative or addition. By exploring ANT theoretically and empirically, the dissertation eventually attempts to develop an alternative approach – denoted as the 'cyborg crime' perspective - which enables to grasp and analyze certain aspects of cyber offending and victimization more profoundly than a traditional approach.

The following two related research questions will be addressed in this dissertation:

1. What are the (a)typical features of high-tech cybercrime and which theoretical challenges derive from those features for criminology?
2. In what way can actor-network theory (ANT) counter these challenges and offer a valuable alternative or addition?

Research question 1 has been taken up in the current chapter, but is also dealt with more concretely throughout each single chapter in the dissertation. Every chapter (differently) focuses on certain (a)typical features of cybercrime (ranging from automation to hybridization) and how they challenge existing criminological theories or concepts. Each chapter also looks at the explanatory power of different criminological theories or set of theories. Chapter 2 critically assesses certain notions of the routine activity theory and the rational choice perspective. Chapter 3 assesses the explanatory potential of the labeling approach. Chapter 4 does the same for (cultural) criminological approaches and concepts used in existing hacker studies and chapter 5 considers (again) the routine activity theory, but also takes the lifestyle approach and some traditional victimological concepts into account.

Research question 2 is also addressed in different chapters in this dissertation. In each chapter the theoretical potential of ANT will be

explored in a different empirical context and will be compared with the potential of a traditional approach. In chapter 3, however, the ANT perspective is less central. This serves the purpose of showing how a more traditional lens will capture the phenomenon (hacking in this case), while the following chapter 4 will explore the phenomenon through the ANT lens (see also section 1.8.3). Since each chapter deals with another cyber theme and/or dimension, they also include a more topic-specific research question (see section 1.9), eventually leading back to the central research questions of the dissertation. In that sense, the two research questions are overarching, but also have a 'generative' nature: they "invite a series of more specific questions" (Agee, 2009: 433).

1.6.2. Focus and relevance

As the research questions show, this dissertation predominantly focuses on 'high-tech' forms of cybercrime. The reason for selecting and studying these crimes is that they hold features and dynamics that cannot or to a lesser extent can be observed in traditional crime, as was discussed in section 1.3. As Wall (2007) puts it, these crimes contain the highest level of 'newness', which is why they are particularly worth assessing in light of the earlier mentioned novelty debate, but also for exploring ANT's theoretical potential. Accordingly, this dissertation seeks to make a scientific contribution to the field of (cyber)criminology in four main ways.

Firstly, the dissertation places the accent on theoretical exploration and renewal, which has not been a real priority of cybercriminologists so far. Most studies in the field of cybercriminology are positivistic in orientation and conduct empirical tests of existing theories, the opportunity theories in particular. While it is definitely essential to assess whether traditional theories can account for cybercrime, there is also a need for more research that examines the sustainability of criminology's theoretical repertoire from a more critical, constructivist angle. It can be argued that current digital developments, as already described, urge to take a closer look at many of the often taken for granted concepts in criminology such as 'agency', the 'offender' and the 'victim'.

Secondly, connected with the previous point, this dissertation seeks to make a contribution to criminology and the novelty debate by not only critically considering existing approaches and concepts, but also to search for alternatives. It reasons that the role of technology is so essential in cybercrime, that it demands criminologists to explore concepts outside of criminology that can provide valuable leads. This dissertation particularly assesses the potential of ANT and explores its (added) value across a broad spectrum of criminological dimensions and issues, ranging from the understanding of how certain crimes are carried out (chapter 2), what drives an individual offender (chapter 3 and 4) to how a victim becomes victimized (chapter 5). By applying ANT in various settings, it explores in which contexts the approach is valuable and for which aspects its (added) value might not be so particularly substantial.

In addition, ANT has not been applied in much (cyber)criminological empirical research yet. This research also makes a contribution to the filling of this gap.

Thirdly, the dissertation seeks to generate more criminological insights into the phenomenon of high-tech cybercrime. While the main objective and focus is to develop an ANT-based alternative (cyborgian) perspective that can be used to study and understand cybercrime, it would be too blunt to say that this dissertation is merely theoretical in nature and focus. On the contrary. The case studies that have been conducted also aim to shed light on specific aspects of cybercrime and the actors involved (see further section 1.9). The case studies, some more than others, provide a rich and detailed account of the actors under study, hereby also increasing the criminological knowledge of different cybercriminal phenomena: botnets, hacking, ransomware and virtual theft.

Fourthly, by concentrating on high-tech cybercrime, this dissertation also responds to the call for more research on the more technical crimes and the appeal for criminology to become more 'digital' (Smith et al., 2017). Until now, computer scientists and experts have been the main scholars investigating these crimes, since they have the knowledge, recourses and abilities to do so. It can however be argued that criminologists also have an important contribution to make to the understanding of these crimes, in particular when it comes to the study of its offenders, victims and the involved organizational structures (see

also chapter 2). This dissertation took up this challenge by exploring these more technical crimes from a criminological perspective, through the hybrid lens of ANT.

Before I will more extensively explain how ANT has been applied in the case studies, I will outline the core assumptions of ANT and why this particular 'theory' plays such a key role in this dissertation.

1.7. Actor-network theory as a central approach

ANT emerged in the 1980s in the field of science and technology studies (STS) and is commonly associated with the work of Bruno Latour, Michel Callon, John Law and Annemarie Mol. The approach is particularly well known for its ideas related to the agency of non-humans, although ANT, Latour's oeuvre in particular, covers a range of various other viewpoints as well (see for an overview e.g. Harman, 2009; Blok & Jensen, 2011). ANT's ideas are often considered as provocative (Wessells, 2007), impossible (Law, 1999), wild and creative (Mol, 2010), but also unique and groundbreaking (Blok & Jensen, 2011). ANT is also quite often misunderstood. For instance, some believe that Latour is attacking humanist thought as he considers non-humans as being part of the same ontological region as humans (e.g. Vandenberghe, 2002), while ANT is not anti-human(ist) at all (Kipnis, 2015; see also Latour, 2013). Others believe that Latour assigns mystical power to objects, while his vision is much more nuanced (Martin, 2005). Furthermore, ANT has often 'been accused of' or been associated with e.g. 'relativism',

'incommensurability', 'subjectivism' and 'postmodernism' (Latour 2000), while it does not really (claim to) fit in any of these paradigms. Latour sort of drifts across various theoretical traditions, thinkers and established scientific disciplines simultaneously (see Blok & Jensen, 2011).

The fact that the terms 'actor', 'network' and 'theory' (and the hyphen) also do not really represent where they commonly stand for (Latour, 1999), does not provide much clarity either. "ANT does not define these terms, but rather plays with them" (Mol, 2010: 253). Leaving some mystery and confusion around the very concepts it presents, I believe, is at the same time a typical Latourian or ANT 'thing'. It does not want to be a 'fixed' framework, but something adaptable. This also explains how Latour's ideas went through some changes over time (see e.g. Schinkel, 2007; Latour, 2013) and also that ANT itself underwent some transformations (see Law & Hassard, 1999; Gad & Jensen, 2010). Nevertheless, there are definitely some core ideas or lines of thinking that one gets to understand quite soon when he or she delves into the tradition denoted as actor-network theory, whether it is 'old school' or post-ANT. In the following I will provide a brief overview of what ANT stands for and then explain why and how ANT is applied in this PhD research. In the case studies themselves I will provide a more detailed account on some of its central ideas.

1.7.1. Actor-network theory: everything but a theory

"ANT's main shortcoming is that it is everything but a theory – which explains why it cannot explain anything!" (Callon, 1999: 182)

It should be made clear from the start that ANT is not a 'theory' in the 'hard' sense of the word. Rather than seeking to explain or predict things, it can be considered as a theory or methodology of *how* to study them. It provides a set of sensitivities that can guide the researcher, but does not offer a one-sided, fixed and strictly defined conceptual framework one can 'apply' (Latour, 2004; Mol, 2010). Despite of the fact that ANT is not easy to position paradigmatically, we can quite surely state that ANT more closely connects with constructivism rather than positivism. Constructivism is the label for a range of perspectives and ideas that have a critical stance or anti-position against more dominant perspectives in the social and behavioral science, positivism in particular. The issues they address generally led to a number of 'turns' such as the linguistic turn, the cultural turn and the contextual turn (see Lindgren, 2005). ANT is commonly associated with the so called 'turn to things'[11], as it is critical towards thinkers who consider things as being part of the (external) 'environment' and who consider the social merely as the sphere of interpersonal relations. Adherents of the 'turn to things' claim that things (whether it is a small tool or a large technical system) should be placed more in the frontline of sociological theory for the reason that they play

[11] ANT can be also connected with the so-called 'descriptive turn' in sociology as it adopts a critical stance on the methods and theories used in traditional sociology (see Krarup & Blok, 2011; see further 1.7.4).

an active role in the production of the social, ranging from dissolving social norms to falling in love (Preda, 1999). ANT fits in this line of reasoning as well as it "opens up the possibility of seeing, hearing, sensing and then analysing the social life of things – and thus caring about them, rather than neglecting them" (Mol, 2010: 255).

Latour (2005) himself is actually somewhat reluctant in the use of the term constructivism. The only meaning of the word 'construct(ivism)' he finds valuable is that it draws attention to how humans and non-humans are fused together in a certain setting. For instance, when we visit buildings 'under construction' or when we watch 'the making of' a movie, we truly get at the 'backstage'[12] of certain practices and the various actors that were involved in the whole process. They eventually 'disappear' as soon as the building is ready or the movie completed and edited to perfection. The same counts for scientific research and publications (see Latour, 1987; Latour & Woolgar, 1986). When reading the term constructivism this way, ANT definitely fits in this picture[13]. Latour however distances himself from the other meaning commonly associated with constructivism: the notion that reality or facts are constructed. Although he claims that scientific facts are (socially) constructed (Latour & Woolgar, 1986), he never meant that they are therefore 'not real' or 'false' (see Latour, 2005; 88-93). He never intended to question scientific objectivity (Van Loon, 2002). Hence, rather than

[12] Note that this is a different 'backstage' than the one Goffman (1959) is referring to.
[13] Here we also see the clear resemblance with Garfinkel's (1967) ethnomethodogy which also seeks to deconstruct 'the invisible' (see Lindgren, 2005).

speaking in terms of truth and false, Latour prefers to use the term 'blackbox' to "designate processes that were assumed to "yield" truth regardless of the extent to which one understood how the process worked" (Kipnis, 2015: 45). As Mol (2015: 255) explains quite clearly: "Its [ANT's] point is not to finally, once and for all, catch reality as it really is. Instead, it is to make specific, surprising, so far unspoken events and situations visible, audible, sensible. It seeks to shift our understanding and to attune to reality differently."

In his book 'We Have Never Been Modern' (1993) Latour addresses more specifically his anti-dualistic vision. He particularly condemns modern oppositions such as nature versus culture, object versus subject, agency versus structure and also argues that science and politics have never been unconnected. He illustrates this point by referring to the example of climate change, an example, which at the same time highlights his understanding of hybrids or hybridity (see also Brown, 2006: 228).

"On page four of my daily newspaper, I learn that the measurements taken above the Antarctic are not good this year: the hole in the ozone layer is growing ominously larger… the same article mixes together chemical reactions and political reactions. A single thread links the most esoteric sciences and the most sordid politics, the most distant sky and some factory in the Lyon suburbs, dangers on a global scale and the impending local elections of the next board meeting. The horizons, the stakes, the time frames, the actors- none of these is commensurable, yet there they are, caught up in the same story" (Latour, 1993: 2-3).

This same criticism – the construction of black boxes and the neglect of non-human entities - Latour (2000; 2005) applies to the manner in which (classical) social scientists deal with 'the social'. It is this particular strand of thinking that has become known as actor-network theory (Kipnis, 2015).

1.7.2. ANT as the 'sociology of associations'

In Latour's book 'Reassembling the Social' (2005) he presents his critique on traditional sociology alias 'the sociology of the social' – which he associates with thinkers such as Durkheim, Giddens, Habermas and Bourdieu (Krarup & Blok, 2011) - and presents an alternative vision denoted as 'the sociology of associations.' Latour's (2005) main criticism on the sociologists of the social is that they seem to presume that 'the social' is built out of 'social stuff' rather than other materials such as physical, technical, biological or economical matter. For Latour, the social cannot be conceived as a particular or distinct substance, but is the result of a gathering or assemblage of many different 'non-social' elements. Following Tarde (1895, in Tarde: 1999), he argues that "society explains nothing but has to be explained" (Latour, 2000: 113). His position is therefore not 'anti-social' but rather 'anti-blackboxing' (Kipnis, 2015: 45). Accordingly, the use of (macro-level) explanatory forces such as 'society', 'power', 'cultural norms' and 'organization' do not make sense from an ANT point of view. They are turned into "a thing that is much more stable and powerful than it has any right to be'" (Wessells, 2007: 352). They are also too broad and abstract to actually capture the local (micro) practices they seek to explain (Gad & Jensen, 2010). For ANT it

would be much more fruitful to study the separate elements (human and non-human) that constitute 'it' and how these heterogeneous elements come together as a (macro) thing. In other words, Latour (2005) makes a shift from 'the stability of the social' to the 'uncertainty of associations' (Wessells, 2007), by which he also seeks to move beyond the micro-macro dichotomy and the agency-structure dichotomy. The ANT researcher should deal with the question how certain ordering patterns emerge (by following the actors), rather than explaining something that is believed to pre-exist (Law, 1999). The way ANT views society, it would look at any 'thing', whether groups, individuals or machines. For instance, rather than studying a 'group' as a (pre-defined) stable unit, ANT concentrates on the activity of 'group-making'; how groups emerge, define themselves and how their members demarcate the boundaries of their group (Latour, 2005).

Another important aspect of Latour's respectively ANT's understanding of the social, related to the above mentioned point, is that it presumes that (human and non-human) entities (like words in a language) only get meaning, acquire their attributes and obtain their strength in relation to other entities. For this reason ANT is often considered as a "ruthless application of semiotics" (Law, 1999: 3). A semiotic understanding of reality not only dissolves dualisms (Gad & Jensen, 2015), it also offers an alternative for causal or (technological) deterministic explanations that seek to explain entities in relation to their environment. As Mol (2010) explains: "Causal explanations usually remove activity from what is "being caused". In a network, by contrast, actors, while being enacted by

what is around them, are still active. The actorship implied is not a matter of freedom, escaping from a causal force. Instead, actors are afforded by their very ability to act by what is around them" (p. 257-258). In a similar vein, Latour does not consider 'power' as something that one can 'possess', but rather as something that depends on the number of actors (the 'composition') that generate it or enable it (e.g. the number of people that obey the person) (Latour, 1986). Hence, it treats power and any other 'thing' that is often considered as a property or as a cause, as an *effect*. Successes and failures (and any other effect) can then only be understood when we look at the network of interrelated or associating entities (human and non-human actors) that produced it rather than by looking at some external causal force (*Idem*). In short, ANT seeks to understand things, actions, events, situations and phenomena in a complex and relational (networked) manner, rather than in a reductionist and linear or causal[14] way (see also chapter 5).

1.7.3. ANT and its engagement with non-humans

ANT is perhaps best known for its active treatment of non-humans in the understanding of 'the social.' It criticizes traditional sociology for treating non-humans in a passive and mundane way, a charge that also holds for criminology. ANT argues that objects have a crucial function in the interaction between people, but that they also interact with people

[14] This anti-reductionist vision of Latour can be also termed 'causal multiplicitation', which refers to the notion that one can unravel "all the connections folded into an object – that is by *unfolding* it" (Krarup & Blok, 2011: 46). This dissertation uses the related term of 'reversible blackboxing' (see chapter 2,4 and 5).

themselves. Apart from considering objects as active participants of the social, ANT also argues that the role of things or objects cannot merely be understood in functional terms. They are more than just 'instruments' or 'commodities' (e.g. Latour, 1992; Latour & Venn, 2002). As Dolwick (2009: 41) explains ANT's view: "Besides performing practical tasks, objects help to stabilise, mediate, frame, articulate, enforce, and give meaning to action. They even help us form identities. In this sense, 'we' (humans) are already hybrid collectives – we do not exist without things." In other words, ANT argues that the role of objects can be multifaceted, but they can be also crucial for understanding how and why humans act in a certain way.

This way of thinking also has implications for the manner in which certain ('social') problems are approached. For instance, rather than explaining the high number of weapon killings in the US by searching for 'cultural' explanations, it would draw more explicit attention to "the availability of guns and their person-transforming capabilities" (Krarup & Blok, 2011: 46, see also chapter 2 & 4). For this reason non-human objects (whether it is a gun, a hammer, an automated door or a computer) need just as much analytical attention as humans receive, at least *initially*. Concerning the latter Latour (2005: 76) underscores: "ANT is not, I repeat is not, the establishment of some absurd 'symmetry between humans and non-humans'. To be symmetric, for us, simply means *not* to impose a priori some spurious *asymmetry* among human intentional action and a material world of causal relations." In other words, ANT does not consider non-human agency more important than

human agency (or vice versa) nor does it deny human agency (Kipnis, 2015). In chapter 2 and 4 a more detailed account of ANT's understanding of non-human agency will be provided.

For now it suffices to say that we can position or connect ANT's understanding of non-human agency with the 'mediation approach' in philosophy of technology, mentioned earlier, which does not view the role of technology in either deterministic or instrumental terms (see Verbeek, 2005; 2008). ANT also has some common ground with Haraway's (1985) post-human notion of the cyborg (Verbeek, 2008; Gough, 2004). According to Haraway, the cyborg as a hybrid creature enables to transgress dualisms, e.g. the boundaries between male and female, black and white, but also the ontological division between humans and non-humans, the physical and the non-physical (Geertsema, 2006). ANT does not use the term 'cyborg' extensively, but rather speaks of 'actants' or 'hybrid collectives' of human and non-human entities. Since these concepts stand for the dismantling of dualisms, the dissertation uses the words 'cyborg', 'actant' and 'hybrid' interchangeably.

The post-human view held by Latour and Haraway should however not be confused or equated with a so-called 'trans-human' approach, which is occupied with "all kinds of artificial, machinic relationships with human beings" (Haraway, 2000: 128, in Gough, 2004). In light of current developments (e.g. the implementation of pacemakers and other artificial body parts) and possible future developments (e.g.

downloading the human spirit into a machine), trans-human thinkers (e.g. De Mul, 2002) claim that the human as a 'biological' creature is outdated by technology. They argue for a new approach to the human, which they denote as a 'trans-human life form' (Verbeek, 2008). Post-humans, on the other hand, merely believe that there is no stable fixed human essence (see Vicini & Brazal, 2015). They adhere to an "analytical stance that grant[s] agency to non-human entities and that downplay[s] the differences between human and non-human agency" (Kipnis, 2015: 44). Latour can be considered more a post-humanist rather than a trans-humanist. He flattens human and non-human agency by focusing on how humans and non-humans align and act in the capacity of (more than human) hybrids. In this view, the human and the non-human become one (a cyborg), yet do not lose their individual distinctness (see also Vicini & Brazali, 2015).[15]

To conclude this part, ANT and the various ideas that come along with it seem to correspond quite well with the challenges that criminologists are facing in the digital era: the proliferations of technology, the hybridity and complexity of current crime problems, the blurring of the virtual and the actual and so on. Conceptually it might also inspire alternative views for criminology's rather instrumental, anthropocentric and dualistic understanding of the human-technology relationship. This also explains why some criminologists (e.g. Brown, 2006; Hayward, 2012; Webber &

[15] The authors draw in this context a parallel with Mark Coeckelbergh's understanding of the spirit of the Internet, which also emerges as a network of humans and things and which in turn can be perceived in a cyborgian way (see further Vicini & Brazili, 2015: 154).

Vass, 2010) have mentioned or explored the theoretical potential of ANT already, also for the study of cybercrime. Yet a concrete translation, operationalization and application of its key concepts in criminological empirical research is still quite rare (see e.g. Robert & Dufresne, 2015). One of the few cyber examples is the study of Hinduja (2012), who applies ANT on the phenomenon of music piracy, mapping the various heterogeneous elements (economic, political, informational, etcetera) that constitute it.

1.7.4. How ANT will be used as a 'theory' in this dissertation

In this dissertation I mainly use ANT as a 'lens' or, following Mol (2010: 261), as a (sensitizing) 'repertoire'. Considering a theory as a lens signifies the idea that a theory enables you to "see certain things sharper while other aspects fade away or are underexposed" (Staring & Van Swaaningen, 2016: 39). Yet, it is not only a matter of seeing, but also of tasting, hearing, feeling and appreciating the world it observes (Mol, 2010). Note that a lens is not the same as a (theoretical) 'tool', at least not from the ANT angle: "tools are never 'mere' tools ready to be applied; they always change the goals as well" (Latour, 2004: 64). Indeed, as this dissertation will reveal, getting engaged with ANT is not a clear-cut or pre-definable path and destination. Its 'applicability' and value has to be explored along the way (see further 1.8). Whether a 'lens' is the same thing as a 'frame' (or framework) is also a relevant question to consider. Latour himself does actually not consider ANT as such. In a dialogue between a professor and a student, Latour (2004 alias the professor) formulates his position as following: "I have no patience for context, no.

A frame makes a picture look nicer, it may direct the gaze better, increase the value, but it doesn't add anything to the picture. The frame, or the context, is precisely what makes no difference to the data, what is common knowledge about it. If I were you I would abstain from frameworks altogether. Just describe" (p. 64). In other words, we cannot 'apply' ANT, but merely "follow its tenets" (Wessells, 2007: 353).[16]

However, ANT certainly gives directions for *how* to describe. As pointed out already, the lens of ANT is particularly sensitive for those things that are commonly underexposed or 'blackboxed' by existing or mainstream lenses or theories. It seeks to make those things visible that are often taken for granted, simplified or treated in a passive or singular manner. In this context, the role of non-human entities in shaping facts, events, processes and actors is an important focal point for the ANT lens as well as the networked and relational nature of entities, actions and actors. As Gad and Jensen (2010) point out, ANT provides "a constant reminder that research is always likely to encounter conglomerates or hybrids of action rather than pure entities" (p. 75). This sensitizing dimension has been in the frontline of each[17] single case study in this dissertation, e.g. by explicitly focusing (also) on whether and how non-human entities co-shape actions, events, decisions, intentions and perceptions.

[16] Some believe however that Latour's 'radical descriptivism' goes further than only describing (see Krarup & Blok, 2011). This issue will be further discussed in the concluding chapter 6.

[17] As pointed out already in section 1.6, in chapter 3 the role of ANT is much smaller.

Furthermore, the ANT lens seeks to capture what actors themselves have to say. By giving a stronger voice to the actors under study, it claims to get the closest to mere and neutral description (*Idem*). As Latour (2005: 23) puts it: "The task of defining and ordering the social should be left to the actors themselves, not taken up by the analyst." In this respect ANT follows, at least for the most part, other interactionist or ethnographic approaches, which also seek to produce a rich account of the world of the actors under study and to learn from them. Hence, unlike the sociologists of the social, who travel fast and take the shortcuts, ANT scholars need to travel slowly and take the small roads (Latour, 2005). They can be considered as the "backpackers among sociological fellow travelers, those who follow the making and breaking of associations and allow the vocabulary of "locals" to seriously influence the travel report" (Gad & Jensen, 2010: 63).

1.8. Research strategy: a case study approach

"Research without a theory is adrift – it has no direction – and at the same time theory needs research to further develop itself" (Staring & Van Swaaningen, 2016: 40).

As becomes clear from the earlier sections, this dissertation evidently has a theoretical explorative nature, yet it also includes empirical research. Especially since ANT is a rather abstract perspective, exploring its notions in a criminological empirical context could have added value

for both theoretical exploration and development (Blumer, 1954; Glaser & Strauss, 1967). At the same time, exploring ANT in different (empirical) cases fits well in the ANT tradition itself. As Mol (2010) points out: "The art is not to build a stronghold, but to adapt the theoretical repertoire to every new case" (p. 256) and "not to repeat and confirm, but to seek out cases that contrast with those that came earlier" (p. 261). Based on these considerations, this dissertation explores ANT in different empirical contexts and settings and chooses for the case study as the main research strategy.

In this section I will first explain what a case study defines and then reflect on its strengths and possible weaknesses. Thereafter I will explain how the case studies in this dissertation have been selected and conducted. Important to stress is that the chapters 2-5, which comprise the case studies, each include a detailed methodological section on how the data for that particular case study were collected and analyzed.

1.8.1. The (multiple) case study as a research strategy

The case study is a methodology or approach that is surrounded by quite some confusion, ambiguity and misunderstanding, both with regard to its definition, methodology and its scientific value (e.g. Flyvbjerg, 2013; Gerring, 2004; Verschuren, 2003). The most important or decisive feature when determining whether a study can be classified as such is that it involves the intensive study of one single example or bounded unit or set of multiple units. The selected unit (e.g. a person, an object or an incident) can be studied by different research methods, qualitative,

quantitative or a combination of both (Flyvbjerg, 2013). Using multiple sources and methods enables that the case is not "explored through one lens, but rather a variety of lenses which allows for multiple facets of the phenomenon to be revealed and understood" (Baxter & Jack, 2008: 544). The chosen methodology is however not a criterion for classifying a study as a case study. The same could be said for the importance of context. Context alone does not define the case study, but each case comes with a (real-life) context. For a case study, the context is crucial to investigate and to take into account for obtaining the full picture (Flyvbjerg, 2013). The case study is also often associated with holism, the notion that the researcher seeks to attain a (w)holistic understanding of one particular case. Yet, what is exactly meant by the term holistic is not very clear. While for some it merely refers to the study of a 'single unit of analysis', for others it means 'looking at everything there is' (see Verschuren, 2003: 124). The latter would fit more in the ANT point of view. A case study is also believed to be sensitive for complexity, diversity and uniqueness of cases (Stake, 2008; Verschuren, 2003). This makes the case study particularly suitable for criminological research into hidden and hard to reach populations and sensitive topics (Leys, Zaitch & Decorte, 2016) or the 'backstage' of social phenomena (Flyvbjerg, 2013).

Taking these features all together, it would be too limited to merely define the case study as the study of one single case or multiple cases. It comes with certain philosophical assumptions, specific research questions and also (not discussed here) with a choice for certain

theoretical frameworks. It can thus be considered as a research strategy in its own right (Verschuren, 2003), which also has its own strengths and (possible) weaknesses.

1.8.2. The strengths and (possible) weaknesses of the case study

The main strengths of case study research have more or less already been outlined above, and can be summarized as "depth-detail, richness, completeness, and within-case variance" (Flyvbjerg, 2013: 197). Its main weaknesses, include "a weak understanding of occurrence in population of the phenomenon under study" and "no clear picture of statistical significance" (*Idem*: 198). These issues are not a major source of disagreement, since the (qualitative) case study simply does not aim to study and produce numbers. There are however issues or features of the case study that are considered by some as a weakness, while by others they are conceived as a strength. Flyvbjerg (2013) labels them therefore as 'misunderstandings'. I will now briefly discuss these misunderstandings, since they are relevant in light of assessing the value of the conducted case studies in this dissertation.

The first misunderstanding about case study research is that general, theoretical knowledge is more valuable than concrete case knowledge (Flyvbjerg, 2013: 172). This issue has already been tackled by the above description of the strength of case study research. Case study research does not serve to 'prove', but rather to learn something and to produce a rich account of the phenomenon under study. The second

misunderstanding involves the claim that a case study cannot contribute to scientific development, since one cannot generalize on the basis of an individual case. According to the Flyvbjerg (2013), this is case-dependent. For example, many major scientific discoveries and innovations in history were actually based on one single case or experiment, while formal generalization is not always a guarantee for scientific progress. The third misunderstanding, which is connected with the first misunderstanding, concerns the notion that "the case study is not suitable for hypotheses testing and theory building" (p. 179). This claim is also considered flawed. For instance, case study research can actually be able to trace links between certain causes and outcomes and is able to understand the sensitivity of concepts to context (see George & Bennett, 2005; see further section 1.8.2). The fourth misunderstanding involves that the "case study contains a bias toward verification, that is, a tendency to confirm the researcher's preconceived notions (*Idem*: 186), which obviously jeopardizes the scientific value. It can be argued that this is not completely inevitable in scientific research and not only applies to case study research either. In addition, the case study and other qualitative research strategies are often considered to be subjective in nature and less rigorous than quantitative methods. This critique can be countered by the argument that a case study has its own way of being rigorous. The fact that the researcher is located at or dealing with 'real-life' situations enables that he or she can verify or test the involved views and is also better able to develop new hypothesis during the research process, e.g. when a respondent brings up an issue that was not included as a variable yet (George & Bennett, 2005).

An additional issue or fallacy worth considering with regard to case study research, somewhat connected to the earlier issue of subjectivity, is that data and information can be simplified due to overinterpretation by the researcher. This in turn might for example lead to the masking of the "many-sided, complex and sometimes-conflicting stories that the actors in the case have told researchers" (Flyvbjerg, 2013: 192), but it also makes the findings less controllable and verifiable (Verschuren, 2003). One of the important ways of tackling these issues is 'thick description', involving that the research findings involve dense narratives rather than summarizing them and seeking to reach conceptual closure. In the context of the first issue Peattie (2001, in Flyvbjerg, 2013: 192) warns: "It is simply that the very value of the case study, the contextual and interpenetrating nature of forces, is lost when one tries to sum up in large and mutually exclusive concepts." This standpoint obviously corresponds well to ANT's call for a more descriptive approach, in which the researcher does not employ a 'meta-language' that is believed to capture the world of actors better than the actors themselves (Latour, 2005). In this dissertation, in chapter 3 and 4 in particular, I have sought to place the story of the respondents in the frontline and have tried to avoid overinterpretation. At the same time, the dissertation includes some 'conceptual closure' as well, which is connected with the theoretical explorative nature. It does not explore merely specific phenomena, but also the theoretical potential of ANT, resulting in new (sensitizing) concepts for the criminological study of cybercrime (see further chapter 6).

1.8.3. Case study focus and selection of the cases

As Flyvbjerg (2013) points out, when one chooses to conduct a case study, the choice of the 'case' or 'cases' is equally or even more important than the choice which methodology to use. This dissertation includes four different case studies: an analysis of a botnet, two small-scale ethnographic studies on hackers and an analysis of three types of high-tech crime victimization (ransomware, botnets and virtual theft). These studies are (inter)connected, but they can also be read or conceived as individual case studies in their own right. On the one hand, the case studies build on one another in the sense that each study applies ANT at another level (e.g. the offender or the victim), which is also explicitly mentioned in the chapters themselves. On the other hand, the cases also have their own specific focus, research question and theme, which is why they can also be considered as individual or separate studies. Therefore, the research does not involve a 'cross-case analysis' in the manner in which it is commonly carried out. Usually it involves an iterative cycle in which propositions, hypotheses and reflections based on one case are also tested in other cases for the purpose of validation (Leys et al., 2016). In this dissertation I also compare, even validate certain propositions, but in a somewhat different way. I seek to explore the ANT lens in different contexts, assess whether ANT is more suitable or applicable in certain cases or contexts than others and also aim to make visible what its added value could be. Hence, ANT itself (as a theory) can also be regarded as 'the case' under study.

It is, of course, also important to elucidate why these four particular empirical cases have been selected. In this context not one particular strategy of selection has been applied, but rather a blend of different ones.

Firstly, the selected cases all represent examples of high-tech crime or the 'true cybercrimes', as denoted by Wall (2007). As pointed out before, these new crimes and the features that they represent, challenge existing criminological theories and notions of crime more, or at least differently than the earlier described computer-enabled crimes. The cases have therefore been selected for the reason that they are exemplary for certain key features of cybercrime that are at stake here in this dissertation. To specify, a botnet is illustrative for the automated and robotic nature of cybercrime, the hacker figure represents a deviant figure that has a distinctive relationship with technology, ransomware resembles quite clearly the 'human-machine victim hybrid' and virtual theft is the prototype of a type of offending/victimization where the real and the fictional merge. Hence, these cases represent or make visible the process of interest in this research. The strength of this particular strategy lies in what Flyvbjerg (2013: 179) denotes as 'the force of example' and transferability rather than formal generalization (p. 179).

Secondly, the selected cases can be regarded as so-called (a)typical or 'deviant' cases – the black swans (atypical crimes) among the white ones (traditional crime). According to Flyvbjerg (2013), deviant cases are much richer in information than 'average' cases. They "reveal more

information because they activate more actors and more basic mechanisms in the situation studied" (p. 181). Deviant cases are therefore "well suited for theory development, because they help the researcher understand the limits of existing theories and to develop the new concepts, variables, and theories" (*Idem*). In light of the theoretical explorative nature of this dissertation, this selection strategy seems to be a logical choice.

Before we move on to the research methodology employed in the case studies, it should be also clarified why the case studies have been conducted in this particular order. As mentioned before, the cases were not selected in advance, but during the research process. The research started with the analysis of the botnet phenomenon since these networks are the clearest example of the robotic nature of cybercrime. After this study, which involved the analysis of police files, it was decided to apply ANT in the context of a more ethnographic study on offenders and to examine their motivation, moral perceptions and experiences. The hacker was the most obvious choice since hackers are known for their specific (malicious) engagement with technology. I also presumed that gaining access to this particular group would be realizable, although eventually that seemed to be not that easy (see chapter 3 and 4). The third case study (the other 'others') was a follow-up study of the second. The empirical material gathered during the interviews invited to also focus on hacking from the perspective of labeling. For the purpose of this book (shedding light on the added value of ANT), the results from this case study are presented in chapter 3 and the results from the second

case study in chapter 4. By reading the studies in this particular order, the difference between the application of a more conventional lens (labeling in this case) and the ANT lens becomes more visible.

After these studies I realized that it would be suitable to also explore ANT in the context of the victim. Although the botnet study (chapter 2) touched upon victimization already, it made sense to dedicate one study to victimization only and to take a look at existing victim concepts in criminology. Hereby the four case studies would more or less cover the crime, the offender and the victim.

1.8.4. Research methodology and the data used for the case studies

The conducted case studies are all carried out by qualitative research methods: the analysis of police files, in depth-interviews or a combination of both. Each study also involves a review of the literature in the context of that particular theme (e.g. literature on botnets or hacking) and relevant literature on ANT. Conducting qualitative research fits best with the explorative nature of this dissertation. It explores the theoretical potential of ANT and at the same time it studies some rather underexplored forms of cybercrime. Furthermore, a qualitative research approach is obviously more compatible with the constructivist lens of ANT, which seeks to obtain a rich view of phenomena rather than searching for causal relationships between a pre-determined set of different variables. In addition, qualitative research is flexible in nature, which has the benefit that changes in focus or cases can be made during

the research process. I will now briefly discuss the empirical data that has been collected and has been used for the different case studies. A more extensive methodological section can be found in each of the chapters 2-5.

For chapter 2, the criminological analysis of a botnet, a large-scale police investigation [18] has been analyzed and also one detective was interviewed. At first sight, the study of secondary material such as police files does not appear to be the most preferable option for an ANT based research. As pointed out, ANT is generally supportive of a more ethnographic approach, e.g. by speaking with the actors involved. Police investigations are also characterized by a strong selection bias. They are not assembled for the purpose of scientific research, but for the investigation and prosecution of the involved suspect(s). This in turn determines what information is included and excluded in the files and how the information is written down. Hence, the files seem to be mere representations of how the police investigators view this particular case.[19] This however does not entail that the files do not contain valuable data for the ANT-researcher. As will be described in chapter 2 more extensively, the files provided quite a rich picture of the involved human and non-human actors that were participating in the creation, maintenance, use and ending of this particular botnet. In that sense, the

[18] The Team High Tech Crime of the Dutch National Police made this investigation available for criminological research (see further chapter 2).
[19] Although the manner in which the police constructs their (cyber)reality was not the main focus of this dissertation, the analysis of these files could also be analyzed for this purpose. This would actually be particularly interesting from an ANT point of view (see for example the research of Van de Port, 2001).

method very well served the aim of tracing the network of actors that were involved in the 'rise and death' of the botnet. The fact that these kinds of crimes are not easily observable (in real-time) and accessible for researchers, makes the choice for police files also more logical, even inevitable (see further chapter 2). In that sense practical considerations also play a role in the choice for analyzing police files.

For chapter 3 and 4, ten in-depth interviews with hackers have been carried out, involving a rather small, but diverse group of hackers in terms of their involvement in hacking, their motives and background. Interviewing as a qualitative research method obviously matches better with ANT's call for a more ethnographic approach. It enables to describe the reality of the actors under study and to describe their thoughts, perception and experiences in their own words. Chapter 3 also includes the analysis of five police files in which hacking was the central accusation. Those files were mainly analyzed at the public prosecution office. For this case study, not the complete files were examined, but mainly the interrogations where offenders reflect on the offenses they were involved in. Since this information was obtained in the setting of an interrogation it might, of course, not be completely 'truthful', which is why it has been merely used as an addition rather than as the main source of the inquiry (see further chapter 3).

Chapter 5 has a somewhat different approach. Like chapter 2, this case study also includes the analysis of a large-scale police investigation. It involved the investigation of a criminal network that was responsible for

taking computers remotely 'hostage' in exchange for a ransom. For this case study, also two detectives were interviewed. Since this case study was focusing on the victim side of cybercrime, victim statements and other information related to the victimization process were also analyzed. Concerning the analysis of police files as a method, the same possibilities and limitations count as discussed already.

During the research process, two additional cases were added for the reason that it would be fruitful to look at more than just one type of high-tech cyber victimization. Firstly, the earlier analyzed botnet case was added as a case, since it is exemplary for certain features that challenge existing notions related to victimization, the victim-offender duality in particular. Secondly, a case was distracted from the earlier hacker interviews. One of the interviewed hackers was involved in virtual theft and explained in great detail how he targeted the victims, both in the setting of the fictional game and by installing malware on their computer. The fact that he provided a detailed picture of this process (empirical argument) along with the presumption that virtual theft as a phenomenon provides new challenges for criminology (theoretical argument), were the main reasons for adding this case to the research. Consequently, the last chapter can be considered as a multiple cases study in its own right within a larger (multiple) cases study (this dissertation).

1.8.5. Some ethical considerations

Doing criminological research can go hand in hand with various ethical dilemmas (see e.g. Wouters et al, 2014; Van de Bunt, 2015). Rather than going deep into all kinds of general ethical matters in criminological research, I want to zoom in on one particular ethical consideration that was at stake in this research, namely the fact that I analyzed police files in combination with conducting hacker interviews. One could genuinely ask whether and how being present at a high-tech crime police team, a department that (also) seeks to investigate and arrest cyber offenders, can be done simultaneously with conducting interviews with hackers. Did this situation lead to any conflictive situations in relation to my role as a researcher and how did I try to prevent this from happening?

First of all, it should be emphasized that not all the interviews were conducted at the time that I was present at the police department and also that some interviews were conducted by others than me in a different setting (see chapter 3 and 4). Hence, this potential ethical dilemma only applies to a few interviews. Concerning the latter, my contact persons at the police department were informed about the fact that I was conducting some hacker interviews in the scope of my PhD. However, I did not disclose or share any specific details obtained from these interviews, nor did I inform them with whom I spoke. Obviously that would not be sincere towards the respondents, violate their trust and privacy and even put them at risk (see also Israel, 2004 on this matter). Yet, the illicit nature of the activities the respondents were or had been involved in, obviously raises some ethical concerns.

While conducting interviews with ex-offenders is not that problematic, also not with regard to my role at the police department, the situation can get more complicated when hackers are interviewed that are at that very moment active in crime or share with me plans regarding future crimes (see also Finch, 2001; Israel, 2004). Although most respondents in the research did not (claim to) hack illegally any more or operated (or claim to operate) in grey areas, I was not purposely excluding hackers that were involved in criminalized forms of hacking. On the contrary, the initial idea was to, as a criminologist, gain insights in particularly these types of hackers as well. This research aimed to make a contribution to obtaining more knowledge about this type of offending.

Of course, I am and was aware of the fact that a certain tension emerges here. On the one hand, in the interest of obtaining valuable research information, the assurance has to be given to the respondent that no information will be disclosed to third parties. If confidentiality is not guaranteed, no respondent will share any information or not provide reliable information (Finch, 2001). Hence, like any other researcher, I had to assure them that I would not disclose any information to the police or any other third party. The fact that I analyzed some cases at the police department did not change that. On the other hand, you do not want to make promises you cannot keep. Is the confidentiality you offer absolute? Criminologists, unlike journalists do not have the right of non-disclosure and could therefore be summoned by a court to appear as a witness, something that can become particularly an issue with participatory observation as a research method (Van de Bunt, 2015). In

addition, the researcher might for example face situations in which he or she wants to or feels obliged to disclose information. The latter might for instance be the case if the interviewed offender claims to be involved in certain serious or horrific crimes (or planning to be) (*Idem*; Feenan, 2002). According to Finch (2001), the decision on maintaining confidentially in these situations is ultimately an ethical one. The researcher should make an evaluation of the situation and make a balanced decision. There is no straightforward set of rules on how to concretely deal with this matter, even not in criminological ethical codes of conduct (see Finch, 2001). In my research I could, of course, also have been confronted with these types of dilemmas. Yet this dilemma does not seem to be much different than in the context of any other criminological research involving interviews with offenders.

The matter could be different when it concerns the interviewing of concrete *suspects*. During my research I planned an interview with a person who claimed to be a black hat hacker. A couple of days before the interview would take place, the respondent informed me about the fact that (s)he was a suspect in an ongoing investigation. Although (s)he probably could have given me valuable research information, we decided immediately to cancel the interview. It could lead to undesirable situations for the both of us, especially if (s)he would provide me with information related to the investigation. Although this dilemma might also apply to criminological research in general, I considered this issue (even) more complicated in the scope of the fact that I was present on the location where that particular investigation takes place. Hence,

interviewing suspects of ongoing investigations was definitely a line I would not cross.

A last point to mention in the context of my research is whether files were analyzed which involved the same respondents that I was interviewing. I explicitly excluded these files from the research. First of all, it would not feel righteous towards the respondents if I would analyze these files and not inform them about it. And, if I *would* inform them, it could work counterproductive for establishing a relation of trust. In addition, reading these files could color or influence my opinion and impression about the respondent and also affect the way I would interpret the given answers, which I sought to avoid.

1.9. Reading guide

This dissertation is founded on six articles, which are integrated in six chapters. The current chapter is the first, more global introductory chapter. It is partly based on the first and the last publication conducted in the scope of this PhD research. The chapter provides the background, aim, focus and relevance of the research, but also offers a more global discussion of the cornerstones of actor-network theory in order to place the subsequent empirical chapters into a broader (theoretical) context. As announced, in chapter 2-5 ANT is explored also empirically in the context of high-tech cyber offending, offenders and victims. These chapters are written as and published (or submitted for publication) as journal articles. They are placed here in the dissertation in the way they

have been or (most likely) will be published. [20] Since it concerns articles, some overlap and repetition was unavoidable. For instance, an outline of ANT's conceptual framework had to be given in each single study and the botnet-analysis appears in chapter 2 and (to a smaller extent) in chapter 5 as well. Nevertheless, each chapter has quite a different point of departure, focus and application of ANT, as discussed below.

1.9.1. The botnet as a hybrid criminal actor-network (chapter 2)

Chapter 2 is the first chapter in the range of case studies, in which the ANT lens was explored. This study departs from the notion that criminology's anthropocentric theoretical repertoire is challenged in the digital age with the emergence of crimes that have a rather automated and distributed character. Botnets, networks of infected computers controlled by a botherder, illustrate this development fairly well. The central question in this study is whether we can understand the nature of botnets if we stick to the criminological notion that human agency is the main force behind it. It considers ANT and its concept of technical mediation as an alternative approach, since it offers a more hybrid and distributed understanding of agency and also assigns a more active role to technology in the course of action. In the empirical part, where the analysis of one botnet takes place, the study maps the involved human and non-human actors that (actively) participate in the formation, creation, use, continuation and ending of the botnet. The final discussion

[20] Since I wrote some of these articles with co-authors, I use the personal pronouns 'we' and 'us' in chapter 2, 3 & 5.

focuses on the question whether ANT enables us to grasp the composition and dynamics of botnets more profoundly than conventional approaches such as the routine-activity theory and the rational choice perspective. The study eventually launches the concept of 'cyborg crime', a concept, which is further explored in the subsequent case studies.

1.9.2. The other 'others' (chapter 3)

As mentioned before, this chapter was originally a 'spin-off' study of the other (ANT-based) hacker study (chapter 4). It looks at the hacker phenomenon from the (traditional) perspective of labeling theory. The study explores the role that (criminal) labeling plays in the lives of different hackers and examines how it affects their self-image. More specifically, the study seeks to shed light on how hackers believe society considers them, how they view themselves and how they conceive themselves in relation to other 'others' inside and outside the hacker community. The study also explores whether the assumptions of the labeling approach apply to hackers as a group of 'digital others' and considers whether the theory requires an update in the digital age. Eventually the study also establishes a connection with the ANT lens concerning its notion of group making and anti-group positioning. Yet, the lens of ANT plays a much more central role in the next study presented in the book.

1.9.3. The cyborgian deviant (chapter 4)

Chapter 4 like, chapter 3, takes a glance at the figure most commonly associated with 'cybercrime': the hacker. The point of departure of this case study is that hackers – whether they are engaged with technology in a deviant or non-deviant manner - require an approach that puts their relationship with technology more in the frontline of the analysis. Accordingly, ANT is presented as an alternative framework for grasping the hacker phenomenon and the involved hacker-technology relationship. The central question in the article 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? Based on (the same) ten hacker interviews, the study presents the different ways in which different hackers interact with, through and against technology and what this relationship means to them. The final discussion of this article addresses the question whether or not ANT can make a valuable contribution to the conceptual understanding of hackers and which aspects or dimensions it is better able to grasp than a conventional human and dualistic lens. Concerning the latter, also a comparison can be drawn with the previous chapter, which applies a more conventional lens on the same data.

1.9.4. The hybrid victim (chapter 5)

Chapter 5 takes a glance at the high-tech cyber victim. It leaves from the presumption that current digital developments bring new theoretical challenges for the criminological conceptualization and study of victims

and victimization. This study adopts a so-called problem-driven approach, by actually starting off with presenting the empirical cases. By describing how the victimization process in the case ransomware, botnets and high-tech virtual theft takes shape, the study critically examines the notions of criminological frameworks commonly used to study victimization. It identifies limitations and blind spots, which in turn might be countered by ANT's conceptual framework. In reference to the earlier cases, the added value of ANT is explored, resulting in an alternative conceptualization of the high-tech cyber victim.

1.9.5. Conclusion (chapter 6)

Chapter 6 is the concluding chapter, which is partly based on the last article published in the scope of the PhD research. This chapter starts with a general overview of the background and focus of this dissertation: how did the journey start? It then reflects upon the overall theoretical and empirical findings from the case studies. Based on these findings, it presents the four main dimensions of the cyborg crime perspective. The chapter will then elaborate more on how agency is perceived within cyborg crime perspective and will draw attention to some of the wider implications of the cyborg crime perspective, e.g. in relation to policy. The last part of the conclusion covers an assessment of the opportunities and possible pitfalls of engaging with ANT for (cyber)criminologists. The final section of the chapter provides some suggestions for future research.

Chapter 2

From Cybercrime to Cyborg crime: botnets as hybrid criminal actor-networks*

* This chapter has been published as: Wagen, van der W. & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *British Journal of Criminology*, *55*(3), 578-595.

Abstract

Botnets, networks of infected computers controlled by a commander, increasingly play a role in a broad range of cybercrimes. Although often studied from technological perspectives, a criminological perspective could elucidate the organizational structure of botnets, and how to counteract them. Botnets, however, pose new challenges for the rather anthropocentric theoretical repertoire of criminology, as they are neither fully human nor completely machine driven. We use actor-network theory (ANT) to provide a symmetrical perspective on human and non-human agency in hybrid cybercriminal networks and analyze a botnet case from this perspective. We conclude that an ANT lens is particularly suitable for shedding light on the hybrid and intertwined offending, victimization and defending processes, leading to the new concept of "cyborg crime".

Keywords: botnets**,** cybercrime**,** cyborg crime**,** actor-network theory**,** agency**,** technical mediation

2.1. Introduction

"The rise of the machines has begun. The future implications of botnets will stretch into almost all areas of our technological society. Typically we feel that we have power over the computers and that we rule them, the future will show us however that this is not the case. A virtual army is amassing that will carry more destruction power than any man made army. If we do not prepare, we are truly at the age where the machines will rise" (Cole, Mellor & Noyes, 2007: 13)

As predicted in 2007, crimes have become increasingly automated and robotic in nature. Nowadays, one single individual can remotely and with just a few mouse clicks commit large-scale sophisticated crimes and target millions of victims at the same time (Benschop, 2013; Wall, 2007; Yar, 2005a). Perhaps the best-known crime phenomenon that resembles this development is a so-called botnet, a "collection of infected computers connected to the Internet and controlled by a botnet commander, usually denoted as botherders, and utilized to commit a wide variety of cybercrimes" (De Graaf, Shosha & Gladyshev, 2013: 303) including spam, distributed denial-of-service (DDoS) attacks, information stealing, the mining and stealing of bitcoins and click fraud (Wagenaar, 2012). Besides being a tool or *force multiplier* for crime, the creation of the botnet itself is the result of different criminal activities, such as the hacking of computer systems and the spread of malicious software. Law enforcement agencies encounter major technological and legal difficulties in tackling botnets, since it is extremely difficult to trace

the source of the attack as well as the identity of the attacker (Benschop, 2013). Their takedown requires measures that are simultaneously directed to the human and technological components of the network (Schless & Vranken, 2013).

Due to their predominant technological nature, botnets have mostly been studied in the field of computer science. These studies focus, e.g., on the characteristics, behavior and detection of botnets (Silva *et al*., 2012). Criminological studies that specifically focus on botnets are, as far as we know, non-existent. An explanation for this could be a certain reluctance in criminology for the more advanced high-tech forms of cybercrime and the investigation of computer data (Maimon *et al*., 2013) or, simply the notion that botnets lend themselves better to be studied by computer scientists. Viewing botnets from a criminological perspective could however be very valuable. Firstly, from a more theoretical point of view, it would be fertile to gain a better understanding of crimes that include a large number of technological nodes and (partly) take place in an automatic fashion. Secondly, criminological knowledge and understanding of botnets becomes increasingly relevant due to their interconnection with cybercrimes already analyzed by criminologists (e.g. banking or identity fraud). Thirdly, a criminological analysis of botnets could contribute to further insights for counteracting these crimes.

However, the technological and robotic nature of botnets poses several challenges for criminologists and their theoretical repertoire. The fact

that technological nodes play such a prominent role in the formation and resilience of botnets, and partly operate autonomously, suggests that criminologists are obliged to include a significant technological component in the analysis of these crimes (Brown, 2006; Hinduja, 2012). It also implies that we should consider the role of machine or technology-driven agency in a crime context, an issue that has already been widely discussed outside criminology (e.g. Knappett & Malafouris, 2008; Sørensen & Ziemke, 2007). Although digital technologies are included in cybercrime studies, they are either treated as instruments, facilitators or targets for crime – or as a background or environment for criminal social interaction. In other words, the human dimension is in the end still prioritized in the analysis of cybercrime and the role of technology is mainly understood in instrumental or functionalistic terms.

In this article, we argue that we cannot understand the nature of crimes such as botnets fully if we stick to the anthropocentric notion in criminology that human agency is the main force behind it. We therefore take a different approach in this study. Rather than considering a botnet as a technological tool, an individual (opportunistic) crime *or* an asset on the criminal market, we treat a botnet as a *hybrid criminal network*, a crime that results from human/technology mutual cooperation and interaction. In this context, we explore and apply insights from actor-network theory (Latour, 2005; Law, 1992), a social constructionist approach that contests the common assumption of agency being an exclusively human property. Actor-network theory (hereafter ANT) is not a theory with causal assumptions that can be 'tested' empirically, but

rather a sensitizing approach that provides a lens for studying social phenomena (Law, 2004; Latour, 2005). Its specific attention for the active involvement of non-humans in the course of action (Latour, 2005; Mol, 2010) makes the approach a very good fit for our study.

Our primary goal of the article is then to examine theoretically and empirically, by applying this ANT lens, in what way technological actors can take an active role in the formation and organizational structure of botnets as hybrid criminal networks. Is a botnet mainly human- or machine-driven or does it rely on a complex blend of both? Our secondary goal is to explore ANT and its added value for the criminological analysis of botnets. Does the ANT lens provide us with insights we were not able to gather with a more conventional criminological lens such as routine activity theory or rational choice theory? Although we are aware of the fact that ANT also has its limitations, we finally conclude that the theory provides a lens that captures the hybrid or 'cyborg' dimension of botnets more thoroughly.

The article first briefly provides a general introduction into botnets, and then elaborates on the question why existing conceptualizations or approaches might be not fully satisfactory. Hereafter, ANT will be presented as an alternative approach for analyzing botnets where we particularly focus on ANT's view regarding non-humans. The article proceeds with an ANT analysis of a Dutch botnet case from 2010 where we focus on the creation of the botnet, the victimization process, the use of the botnet as well as its takedown. The last part of the article discusses

the added value of ANT for botnets and cybercrime in general and introduces the concept of cyborg crime.

2.2. Botnets: some basic features

The term botnet is an agglomeration of the word 'robot' and 'network'. A botnet is *robotic* in the sense that it "consists of a group of devices infected with malware to perform the actual work" (Wagenaar, 2012: 6). It is *networked* in the sense that it comprises a network of infected computers. Botnets are basically composed of three main components. The first component is the botherder, one or more individuals who build and control the botnet. The second element is the architecture or infrastructure of the botnet, which can be considered as a control mechanism or communication channel between the botherder and the bots. The third element is the network of compromised computers, also termed bots, zombie computers or victim machines. Estimates suggest that between 16-25% of computers connected to the Internet are actually part of a botnet (Silva *et al.*, 2012*).* The size of a botnet can vary from a few hundred up to millions of infected computers. The size is however not fixed: like human networks they are in a constant state of flux and have several evolutionary stages: birth, growth, contraction and death (Paxton, Ahn & Shehab, 2011). Looking more crime specific, we can distinguish four main stages or processes through which a botnet goes.

The first process is the building of an underlying infrastructure for the botnet. This infrastructure can be either centralized, decentralized (peer-to-peer) or a combination of both (hybrid). In a centralized

command & control infrastructure[21] a botherder can give commands to a large number of bots simultaneously, while a decentralized infrastructure relies on the self-propagation of commands. The second process, which is closely intertwined with the previous one, is the victimization process: to install and run a piece of malware on the target's device, preferably in a way that it stays unnoticed. This can be accomplished by different methods, including drive-by downloads, the (automatic) exploitation of systems, placing malware on a USB flash drive or sending out emails with malicious attachments (Wagenaar, 2012). The third process is the use of the botnet, which principally entails that the botherder will offer it as a "fee-based service for installing malware to third-parties customers who could use infected machines (bots) to commit various cybercriminal activities" (De Graaf *et al*., 2013: 303). Their broad use and capabilities make them desirable assets on the online criminal market (Mielke & Chen, 2008). Yet, in order to remain in business, botherders have to make sure that that they keep a high level of *resilience* (keeping the botnet online as long as possible as well as prevent its takedown), *stealth* (to remain undetected) and *churn* (keeping its size stable by preventing that there are more bots joining than leaving). This is why they "constantly tweak, upgrade and reinvent their botnet architectures and corresponding botnet communication channels" (Wagenaar, 2012: 11). The fourth process, which can only take place if the botnet gets detected, is the takedown or dismantlement of the botnet, a process that can be complicated by several factors such as the

[21] Command & Control Servers (C&C servers) are "channels used by botmasters to communicate with each infected machine" (Bilge *et al.*, 2012: 1).

complexity of the botnet infrastructure and its geographical distributed nature (*Idem*).

2.3. Towards a criminological conceptualization of botnets

For (cyber)criminologists there would be principally three ways of looking at botnets. The first way would be to treat it as a form of individual crime or criminal activity in which a rational human perpetrator creates a tool for himself or for others. The technological components are then considered as means or tools for building the botnet or elements of the opportunity structure of the crime. This view lies in the core of the Rational Choice Theory, which takes offender's decision-making as the central focal point for the understanding of criminal behavior (Clarke & Cornish, 1986). The second way of looking at botnets has basically the same conceptualization as Rational Choice Theory yet a somewhat different focus. The routine-activity theory (Cohen & Felson, 1979) focuses on the convergence (in time and space) of the motivated (rational) offender, suitable or vulnerable target and the absence of capable guardianship, features that are believed to pre-exist in every single crime situation. Unlike rational choice theory, routine-activity theory specifically focuses on how opportunities for crime emerge rather than on the offender motivation or choices per se, yet the approaches are often used complementary. The third way of looking at botnets would be to treat the botnet as an asset on the online criminal market and study, for example by means of a Social Network Analysis,

the process of how different human actors cooperate, communicate, build trust and settle business deals. This approach has often been used for the analysis of criminal (carding) forums (e.g. Monsma *et al*., 2010*;* Soudijn & Zegers, 2012; Yip, Shadbolt & Webber, 2012).

Although these approaches could be employed for a botnet study, they strongly lean on the notion of human agency as the driving force behind criminal activities.[22] Even the first two, who particularly focus on how humans and non-humans come together (in time and space), have "limited resources for theorizing how this process transforms crime other than through structuring people's choices" (Demant & Dilkes Frayne, 2015: 16). We believe that this reliance or centralization of human agency (or human choice) might be not fully satisfactory for crimes that have a robotic and automatic character such as botnets. Firstly, in these crimes technological (software) agents, whether malicious or not, carry out a large part of the work. Although they act on behalf of humans and are programmed by humans to operate as smart or autonomous agents, they can behave or propagate themselves in unpredictable ways (O'Neil, 2006; Benschop, 2013). This indicates that there might be unintended outcomes in terms of scale, impact and continuation, which cannot exclusively be attributed to the (rational) human actor(s) behind it and his/her decision-making. Secondly, we assume that the robotic nature of these crimes has transformed, at least partly, the (inter)relationship between humans and technology in these

[22] Human agency is also an essential element within social network analysis. For instance, entrepreneurship and other skills are considered to be very important for the organization of the crimes (see e.g. Milward & Raab, 2006).

crimes. Their relationship might be considered as more cooperative rather than top-down or one-directional. Along with the fact that in cyberspace technological ties seem to be more important than human ties (Brenner, 2002), it can be argued that the organizational structure of these crimes more closely resembles a hybrid or human/technology partnership than a human or social one. For both of these dimensions ANT offers a suitable framework.

2.4. Actor-network theory in a nutshell

As mentioned in the introduction, ANT is a sensitizing approach that helps to draw attention to things, actors or processes that social scientists usually take for granted (they are 'black boxed') *or* to those which are usually considered as passive or not important in explaining the social (Latour, 2005; Mol, 2010). A substantial part of ANT is dedicated to the participating role of objects or technologies in the course of action. ANT claims that the role of the human actor(s) should not be prioritized when we analyze social phenomena, since humans can only exist, act and give meaning to their actions when they align with non-humans (Latour, 2005). Therefore, humans and non-humans deserve equal or symmetrical attention in the analyses and can only be understood in a relational manner (Law, 2004). It is also important to emphasize that for ANT, actorship or agency is not based on the *essence* of the involved entity (e.g. having the cognitive ability to make decisions and reflect on them) but stems from whether the entity makes a difference, modifies the course of action or mediates in a certain state of

affairs (Latour, 2005). "This is not to say that machines think like people do and decide how they will act, but their behavior or nature often has a comparable role" (Latour, 1992: 151). Consequently, ANT assumes that agency cannot only be assigned to humans; but also to non-humans, or more specifically, ANT assigns agency to a hybrid composition or collective of interacting humans and non-humans (Verbeek, 2005).

To underline this hybridity, Latour prefers to speak of *actants* rather than actors and agency, which also closely resembles the *cyborg* concept that unites both human and non-human elements.[23] The *actant* concept embodies the actor (and its agency), but simultaneously the network concept, which is why Latour places a hyphen between actor and network (see Latour, 2005; Verbeek, 2005). In our study we will use the terms *actor* and *actant* interchangeably. The network concept of ANT refers to the ordering process itself; how collectives of human and non-human actors (e)merge, stabilize (pertain durability) and transform (translate) over time. Instead of understanding a network as a system in which different levels, layers, and structures can be mapped, ANT perceives a network as a techno-social assemblage or actor-network, which transforms over time and has no fixed borders. The topology of the 'actor-network' is therefore rather flat, open and 'mass-rooted', which Latour calls *rhizomatic* (see Latour, 1996).

[23] Latour does not specifically use the term 'cyborg.' Yet, since he speaks of the mixing of humans and nonhumans together and of the agency of non-humans, the term cyborg fits in the ANT framework (Gough, 2004).

From a more methodological point of view, ANT takes interactions as the starting point rather than a specific unit of analysis such as the 'individual' or 'group' (Latour, 2005). An ANT study "starts with a playing field in which all entities are initially (only initially) equal and determinate" (Law, 2000: 4) and "if differences exist it is because they are generated in the relations that produce them. Not because they exist, as it were, in the order of things" (*Idem*). Hence, the aim of an ANT study is to (re)trace connections or associations between different types of actors and to detect how the interacting actors perform and act, form groups, establish stability and change over time (Latour, 2005).

2.5. Non-humans as actors: the concept of technical mediation

In order to clarify how and why non-humans can be actors, Latour (1994) developed four meanings of technical mediation, which are interrelated and complementary rather than distinctive. We now elaborate on them and hereafter discuss which empirical questions can be derived from them for our case study.

2.5.1. Composition

ANT argues that human actors can only act, accomplish things and exist when they align with non-human actors. Their alignment produces the action and the result, not solely the human actor (Verbeek, 2005; Latour, 1994). Latour terms this first meaning of technical mediation *composition* or *complexity of actorship*, by which he seeks to shift the

attention from the human actor to the *network* he or she relies on (De Laet & Mol, 2000). The (rather simple) example provided by Latour is a situation in which a hotel manager wants to achieve that hotel guests return their key upon departure and do not omit to do that (follow the *anti-program*). By combining a verbal or written message with the attachment of a heavy object to the key, the manager is able to accomplish his/her program of action or goal (Latour, 1994; Verbeek, 2005). Complexity of actorship does however not solely refer to a situation in which a human actor is able to accomplish his goals, thanks to the mobilization and use of some non-human actors. In that sense, ANT would sound rather instrumental or *managerial* (De Laet & Mol, 2000). The core idea of composition is that there are different scenarios possible. Sometimes, human actors are acting strategically by enrolling and controlling the actors around them to reach a certain goal. Other times, human actors are guided by the actors around them, which implies that the credits and responsibilities should go to the network of all involved actors that enabled *and* gave shape to the actions and the result of those actions, including the non-human actors (Mol, 2010).

2.5.2. Delegation

Latour's non-instrumental view becomes clearer when we look at the meaning of delegation. Delegation refers to the idea that we can delegate certain duties, tasks or roles to non-humans, which can facilitate or constrain human action, shape their decision-making and influence the effects their actions have (Latour, 1992). For example, an electric sensor in the seat belt of a car forces drivers to use the seatbelt and behave

according to the rules (Latour, 1992). Objects and technologies are not only able to exert influence as signs or carriers of meaning (as symbols), but also as material things (Latour, 2005). While a traffic sign as a symbol urges someone to stop, a ramp will slow drivers down in order not to damage the car, which in turn enforces that they will drive safer and will not hit anybody (Verbeek, 2005). Delegation does however not mean that non-humans are merely human replacements, extensions or practical tools, as the term might suggest. Firstly, ANT assumes that non-humans do not have a functionality that is fixed or static since their *script* or *affordance* - the behavior or usage they invite (which is prescribed by the designer) - merges with the human users (see also the meaning of translation) (Akrich, 1992; Latour, 1992). Secondly, for ANT, what objects do, provoke or produce is not fully predictable. For example, a designer of an object cannot automatically expect that its users will follow (subscribe to) the 'built-in prescriptions' of the object. Users may refuse to use it or use it in a completely different way (Verbeek, 2005). Thirdly, humans are not able to fully master or control technologies and what they eventually will produce, since that would imply "that techniques are nothing more than pliable and diligent slaves" (Latour, 1994: 31), an aspect that seems to matter even more in the virtual than in the physical world (Benschop, 2013).

2.5.3. Reversible black-boxing

Reversible black-boxing refers to "a process that makes the joint production of actors and artifacts entirely opaque" (Latour, 1994, in Verbeek, 2005: 158). At first sight, something can look like an

intermediary or (simple) instrument, for example, a computer or projector, but if it breaks down, we remember its existence. The network of relationships between humans and non-humans becomes visible; before that, the separate elements were invisible parts of the *black box* of the object (*Idem*). Besides dealing with the often black-boxed hybrid composition of networks, reversible black-boxing touches upon the issue of causality. By thinking in terms of *mediators* or *mediation* rather than in terms of *intermediaries,* Latour claims that we might often conclude that linear or direct causality does not exist. He notes: "For intermediaries, there is no mystery since inputs predict outputs fairly well: nothing will be present in the effect that has not been in the cause…For mediators the situation is different: causes do not allow effects to be deduced as they are simply offering occasions, circumstances, and precedents. As a result, lot of surprising *aliens* may pop up in between" (Latour, 2005: 58-59). In other words, there might be a network between a cause and an effect, which we can only see if we seek to open the black box.

2.5.4. Translation

The fourth meaning of technical mediation deals more specifically with the issue of intentionality and how it can be (co)shaped or transformed by non-humans. According to ANT, human agents generally act or try to act according to a certain *program of action*, "the series of goals and steps and intentions that an agent can [have]" (Latour, 1994: 31). These can be disrupted for several reasons. When that happens agents have to make, what Latour (1994) calls, a *detour* or *deviation* from their original

program of action. For ANT, this detour is often mediated by non-humans. Latour (1994) speaks then of *translation* when human programs of actions merge with the functionalities of non-humans and result in a change or modification in both actors. Objects do however not have a deterministic influence for ANT since for different people a different action might come to mind when they enter a relationship with an object or technology. They are also not entirely neutral for ANT as they can invite certain behavior (based on their script). ANT therefore prefers to speak of a mutual or relational influence between humans and things. To clarify his view, Latour (1994) refers to the use of guns. Rather than saying 'guns kill people' or 'people kill people', ANT assumes that guns *might* change the people who have them in their hands and *might* thus provoke people to commit acts they ordinarily would not do (Latour, 1994; Verbeek, 2005).

Based on these four meanings of technical mediation we would like to formulate two main (broad) empirical questions that are central in each of these four meanings, which also form the leading thread for our botnet case analysis: 1) who and what performs the action and the final result and 2) who or what is in control or gives shape to these actions. By asking these questions we seek to maintain no a priori primacy of human over non-humans in our analysis as well as treat the non-human actors (if possible) as mediators rather than intermediaries or instruments.

2.6. Case study method

For this article we studied a large-scale police investigation from 2010, which was placed at our disposal by the Team High Tech Crime in the Netherlands (hereafter THTC). It concerns a botnet case in which THTC managed to take down the botnet and was able to trace and arrest the botherder. Although ANT ordinarily prescribes an ethnographical research method (see, Law 2004; Latour, 2005), it seemed that for this particular study, an analysis of police files was suitable. High tech crime police investigations are executed by digital detectives and therefore contain important information concerning the role of technological nodes in the crime process. These were very relevant for this study. The police files also included some chat conversations, emails and other communicational traffic between the botherder and his customers. We also attempted an interview with the botherder, but due to his release this could unfortunately not be realized. Nevertheless, we believe that this limitation has not been an extreme obstacle for our case study. Once more, our goal was to explore the utility of ANT for botnets and to see whether it provides a better understanding of its hybrid and robotic nature. This botnet case provided sufficient data for this purpose.

The analysis of the botnet case was not an easy task due to the technological complexity of the botnet. For this reason we conducted additional literature research. For example, documents on Bredolab (the malware used for this botnet) published by security companies have been studied, but also forensic analyses that were conducted in the

context of this particular police investigation (e.g. De Graaf *et al.*, 2013; Wagenaar, 2012) have been consulted. Furthermore, the police report itself brought some difficulties as the files did not provide a clear chronological picture of all the events. Findings during the police investigation often had to be corrected due to the fact that the investigation was hindered by the advanced and complex infrastructure of the botnet. By conducting an interview with one of the involved digital detectives many aspects could be clarified. Findings from this interview will also be discussed in the case analysis.

2.7. Short description of the case

The botnet in this police investigation came into the picture when a security employee, who conducted research on the spreading of Zeus[24] on the Internet, traced a server that was spreading malware. After further investigation a very complex infrastructure was found which was used for spreading and maintaining a botnet. The infrastructure was accommodated by one of the largest hosting providers in Europe. After this discovery, the Dutch police started its investigation in July 2010. The suspect that was supposed to be behind the botnet was (at that time) a 27-years-old male. As a botherder he was the administrator of the infrastructure of the botnet. He did not hire the servers himself, but through a so-called bulletproof hosting provider which operated as a reseller. A total of 281 IP-addresses on 144 servers were confiscated

[24] Zeus is one of the most well-known and threatful trojans: it is a spyware program, which is used to steal online data such as user names and passwords (www.kaspersky.com).

from this reseller. The police investigated the part that was supposed to belong to this botnet. It is estimated that since June 2009 at least 3 million computers worldwide have been infected through this infrastructure. The suspect set up a web shop and used chat servers (such as Jabber) to communicate with his customers. The money flows were processed through digital payment transactions such as prepaid credit cards and web money accounts. These customers used the botnet for different purposes such as the spreading of spam, banking fraud and DDoS attacks. The botherder himself was accused of the following crimes: possession and use of malware (botnet), hacking of websites (he managed to get access to the advertisement space of at least 148 websites), committing DDoS attacks and the (on order) spreading of spam. As he used the Virtual Private Network (VPN)-server[25] - which he utilized for the spreading and maintaining his botnet – also for private matters, it was possible to link the botherder to all the criminal offenses. In October 2010 the botnet was taken down. The botherder was arrested and sentenced to four years of imprisonment.

2.8. Case analysis

We will now analyze the botnet by looking at the aforementioned four processes within the crime process: building the technological infrastructure of the botnet, the victimization process, the use of the botnet and its takedown. Each process will firstly be described and then

[25] "A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet" (http://whatismyipaddress.com/vpn).

further analyzed from an ANT perspective by asking who/what acts and who is in control/shapes these actions.

2.8.1. (Building the) technological infrastructure of the botnet

In order to create and control the botnet, the program Bredolab[26] was used, a "complex downloading platform designed to facilitate (and to monitor) the spread of malware on a massive, large-scale rate" (De Graaf *et al.*, 2013: 303). Bredolab uses the principle of *server-side polymorphism,* which implies that the installed malware changes its method of packing and appearance and is therefore more difficult to detect for virus scanners. It is not clear to what extent the botherder in this case was involved in the creation and design of the Bredolab malware itself. The police report only reveals that he was selling bots, which were infected with it. The most advanced part of the botnet was its infrastructure, which consisted of six different servers to whom different tasks or programs of action were assigned: a malware management server, an FTP grabber server, a VPN server, a data base server, a Jabber chat server and various C&C servers to control the bots (see De Graaf *et al*., 2013 for a full (task) description of these servers). Between the bots and the C&C servers a central proxy server[27] was placed in order for the bots to be able to connect with these servers and at the same time hiding their location. The communication between the

[26] According to Wagenaar (2012: 23) "there is no such thing as *the* Bredolab botnet, as the malware that was used seems to keep resurfacing under different names. The name Bredolab is most often used to denote this specific botnet setup."
[27] A proxyserver is a "computer that functions as an intermediary between a web browser (such as Internet Explorer) and the Internet"(*www.windows.microsoft.com*)

bots and the C&C servers occurred in certain intervals and in an automatic fashion.[28] According to the detective, the most advanced element of this infrastructure was the database, also called the 'mothership' or the 'criminal bookkeeper.' The database consisted of several tables, each of them completing their own duty in the administrative process, such as counting the number of infections, monitoring the communication between the bots and the C&C servers and keeping track of the unique malware identification numbers, IP-addresses and serial number of the Windows C partition.

Although the infrastructure had a high level of sophistication, the police detective at the same time characterized the modus operandi of the botherder as being rather random and anticipating; his impression was that many choices derived from experimental and spontaneous behavior. He noted: "There was no structure. He tested out different things and anticipated on the things he encountered." The first example was that, after some time, an additional C&C server was placed at random in the infrastructure. This action was, according to the detective, not a logical step. The detective assumes that the botherder was not prepared for so many infections/bots. A second example is that, in a later stage, a restart was made with the botnet. A whole new installation of Bredolab was completed and the database was emptied. According to the detective it is most probable that the botnet at some point became contaminated with

[28] The bots established or *initiated* a connection with the C&C server to let it 'know' that they were ready to upload new malware. The bot reported (by means of a status report) whether the malware had been successfully installed. If the installation did not succeed, the malware was sent once again later.

malware. This may have led to the realization that *clean installs* (bots that are only infected with Bredolab) would be easier to sell than *installs* on which already different types of malware have been installed, as they have less value.

From an ANT point of view, we can argue that the construction or building of the technological infrastructure of the botnet resembles a network or *composition* of humans and non-humans, whose programs of action, interrelationship and task division gained further shape over time. Besides functioning as an underlying infrastructure for the rapid rise and growth of the botnet, the network had the capability to exclude external threats. For example, the virus scanners were kept outside of the network by the polymorphism of Bredolab, the VPN server functioned as a protection shield between the botherder and the network, and the (human) reseller enabled the botherder not to be directly linked with the malicious servers. Complexity of actorship manifests itself here thus not only in the sense that the infrastructure was responsible for a large part of the work, but also when it comes to a complex mutual interdependency between the botherder and his infrastructure. The strength and functionality of the infrastructure depended on the technological entities and their ability to operate in an autonomous and efficient manner as well as on the efforts and skills of the botherder. The ANT follow-up question is then whether we can view this process as being mainly human-directed.

Although we cannot deny that the botherder had an important role in setting up the infrastructure and was to a large extent in charge of this process, he was definitely not the only actor initiating, building and shaping the infrastructure. Firstly, it can be argued that the influence of technological entities already occurred in the initiation of the crime. For example, Bredolab did not only enable the creation of a botnet (as an instrument), but might also have mediated in the initiation of the creation of the botnet itself based on its functionality. As a ready at hand program that is so easily accessible or purchasable, it can further provoke or encourage the creation of botnets (like Latour's example of the gun). When such a program then arrives in the hands of a (highly) skilled person, as it happened in this case, its (malicious) functionality can be further enhanced or *translated*, in this case by setting up an advanced network of servers that operates the program. A similar reasoning can be applied to the technologies that enable to protect the network, such as the proxy servers and the VPN server. These technologies make the creation of a botnet less risky and at the same time enable trying out different things and exploring where it will all lead to, an aspect that was also observed in this case. Secondly, the case revealed that the technological entities sometimes fulfilled a mediating role in shaping and reshaping the infrastructure over time. Changes or detours had to be made since the network sometimes produced outcomes that were no longer desirable or foreseen (e.g. the botnet became too large or contaminated with malware). This aspect illustrates that the restraints were not only imposed by an 'external' environment (e.g. customers or law enforcement agencies), but were simultaneously produced by the

network itself, an aspect that is central in the meaning of delegation. It also reveals that the initial program of action 'to infect as many computers as possible' can overtime intersect or clash with other programs of action such as 'to keep the network smoothly running' and 'to remain undetected for law enforcement agencies.' From an ANT point of view, it is this complex merge or clash of human and non-human (programs of) actions or intentions, either inside or outside the network (as far as you can separate them), that produces adaptions and changes in the network over time as well as can generate a new order. The process seems to be thus more complex than a simple goal-means-end rhetoric.

2.8.2. The victimization process

In this botnet, the computers were infected by so-called *drive-by downloads*. In this method, vulnerabilities in the web browser are exploited by the use of *exploits*: software/code that abuses vulnerabilities in other software. It turned out to be possible to hack advertisement servers, to create an extra admin account and to change a piece of computer code. The reason why this particular strategy was chosen does not become clear in the police file. It was a method that was actually not most common for Bredolab infections, since they often took place by the use of email worms where users are encouraged to click on a malicious attachment (Tenebro, 2009). What we do know is that a certain programming flaw in advertising software was published in open sources. Hereafter, information was gathered regarding which websites

use this particular software. A ready at hand list existed of websites that use this software, which was purchased by the botherder. This list enabled to hack a large amount of websites in a short period of time, mostly websites that had a high number of daily visitors. After hacking the websites, Bredolab was implemented into its banners. Computers became infected with Bredolab as soon as its users clicked on these banners, yet only when their operating system was also vulnerable for it. The botherder most likely strongly relied on this method. An anti-virus company published the vulnerability in the software, which he was able to abuse. Hereafter the advertisement software was patched by the advertisement company. As a reaction, several DDoS attacks were launched against both companies, most likely in order to safeguard the method of infection.

From an ANT point of view, the victimization process also resembles a *composition* of different actants brought together in a network. In the drive-by download method, the system vulnerability together with its publication formed a coalition with the botherder to enable the first stage of the victimization process: hacking websites and using them in a way that is not intended by their owner or administrator. Also a list of vulnerable websites was added to the network. Besides enabling the botherder to hack a broad range of websites in a short time and generating a high exposure for potential victims, the list also more or less co-shaped the course of action and the employed strategy. Without the list, the whole process would have been much more cumbersome. The users themselves eventually also play an essential role in the actual

infection of their computer and thus the creation of the botnet. By clicking on the banners on the hacked websites, Bredolab was silently installed on their computer, which enabled that a program of actions could be assigned to the bots. A similar principle counts for the email worm method, which was not used in the case.

The victimization process also reveals how artifacts such as banners and attachments play an important role in the 'fooling' of users. They provoke users to click on them, not merely because of the meaning or message they carry, also due to their material construction. Yet unlike Latour's example of the heavy object attached to the hotel key, something more complex is happening. By 'just clicking on something', which suggests a rather routinized or innocent action, a whole new chain of actions and interaction is activated. The compromised computer becomes part of a larger network of (attacking) computers, which in turn enables a broad range of other crimes to happen, either against others either against themselves. However, the infection will eventually only succeed when their operating system also allows the malware to be installed. In that sense the operating system is an important mediator between an intended and a real infection. Accordingly, the victimization process is also something that is hard to control and predict, which is why it strongly relies on the principle: the more exposure to potential victims, the more chance of succeeding. The hacking of the websites, by contrast, was a more direct form of targeting (yet still a mediated one). Lastly, the case reveals that the victimization process (as a network) might be

threatened. The patching of the advertisement software had to be prevented by launching several DDoS attacks.

2.8.3. The use and control of the botnet

Once the botnet was operative, it became an asset on the criminal market. Customers who would like to use the botnet for their crimes (e.g. spam, banking fraud), could make an order in the online 'botnet shop' of the botherder based on a 'pay-per-install' principle or service. This entails that the customers could choose the number of bots they wanted to purchase, the countries where they were located and which malware they wanted to upload to the bots (based on the intended use) and the botherder took care of the rest. In other words, a certain number of bots was placed at the disposal of these users, yet the botherder preserved the control over the bots and the malware in the database. Other users did not have the same rights or authorization as the botherder himself. They could log into a dedicated C&C server to look at the (sub)botnet they had purchased. In this context it is worth mentioning that certain encoding and obfuscation techniques were used. For example: "The web hosting related scripts used to control and monitor the bots were all encoded with the Zend Guard encoder", which "can be used to encode and obfuscate PHP files, to make reading or changing the original source harder for researchers or customers of the botnet" (Wagenaar 2012). The botherder was however not strictly the person who only sold or outsourced the bots, since he also used the botnet for his own criminal activities. Firstly, he was (with others) involved in spreading spam for others (clients/customers). On a forum he posted the following

advertisement: “We are an ICQ spam service with a capacity of 800 million per day.” Hence the botherder used his own botnet for spam-related activities. Secondly, according to the detective, at some point, the botherder created his own (sub)botnet within his Bredolab-botnet, with the malware *FTP grabber*. With this malware he collected usernames and passwords of computer users.

From an ANT point of view, the use of the botnet can be also considered as a composition or alignment of different human and non-human actants. In order to make money, the botherder had to add customers or users to the network. On the one hand they were integrated in the network in the sense that they had access to a dedicated C&C server. On the other hand they were kept outside of it by not allowing them full access to the network and its source code, which in turn was mediated by the encoding techniques. The process of selling or outsourcing the network was further mediated by other non-human actors such as web money accounts and jabber chat servers, which basically enabled that the botnet could rapidly become part of a larger network of users and their program of action, a process we did not examine in full detail. In other words, once the (sub)botnet has been purchased a new chain of actions and new actor networks are generated. From an ANT point of view we can also consider this process as a form of delegation since the botherder basically delegates part of the control of the botnet to the customers. He has control over the botnet infrastructure (including the malware in the database), but cannot foresee which outcome the botnet will eventually produce in terms of (new) victims and damage. This is not only out of his

control, but also not part of his program of action. Yet, although he is not directly involved in the crimes committed by these customers, it can be argued that the botnet or infrastructure he created can be regarded as an integral part of these other crimes as well as their initiation. He built a (malicious) tool that affords (based on its inscription) to make these crimes more lucrative, large scale and fast and also offers a certain level of protection for detection. Therefore, botnets might co-shape the intention of human actors who get access to them, not merely by *facilitating* but also *inviting* malicious activities. As the case reveals, even the botherder himself did not stick to the task of controlling the network and selling it, but started to use it for its own activities. In other words, it can be argued that a botnet is more than just a tool or facilitator. It can act as a mediator as well as a spin-off for other criminal activities, including for the botherder himself.

2.8.4. The investigation and takedown of the botnet

As mentioned before, the botnet came into the picture of law-enforcement agencies after the discovery of a server that was spreading malware. Before the botnet could be taken down it was crucial for law enforcement agencies to gain a clear picture of the technological infrastructure, its different modules or elements and how these modules mutually interacted. The forensic analysis was however not an easy task. For a long time it was not clear for law enforcement agencies which servers were involved in this particular botnet and how these servers communicated mutually. For example, a server which at first sight was not considered as important, seemed to take a much more prominent

place within the infrastructure and vice versa. According to the detective, the process was complicated by the complex layered structure of the infrastructure. It consisted of distributed control points and was partly encrypted. Consequently, only in a later stage a clear picture could be gained of the network as a whole and the exact role of each actor in the network. Once it was clear how the network operated and who/what was involved in its creation and operation, measures could be taken against the botnet.

In this process the police assumed that a takedown could only succeed when measures were taken that were directed at the technological infrastructure of the botnet, the botherder and the individual bots. First of all, the network could not be taken down by just switching off the servers since the botherder could set up new servers, which would automatically reconnect with the infected computers. Secondly, arresting the botherder would also not be sufficient to take down the botnet since the network could be taken over by another botherder and the infection of the bots would not be eliminated. Law enforcement agencies therefore had to make sure that, before arresting him, the botherder was no longer able to communicate with his network; the access had to be blocked. Thirdly, the infection of the computers had to be eliminated since the infection would remain even when the botherder was arrested as well if the servers would be offline. By gaining access to and control over the backend panel on one of the C&C servers, the police could only prevent the infection of new computers. In order to disinfect bots that were already infected with Bredolab, “NHTC developed a

program that [was] uploaded to all bots in the network and launched a standard browser on the victims' computers to allow infected users to read a press warning message. This warning message has been viewed over 300,000 times. BredoLab botnet was let active for a few days in order to reach as much victims as possible. After that, the network connections to all servers were terminated" (De Graaf *et al*., 2013: 307).

In ANT terms, the investigation and takedown procedure most clearly resembles Latour's concept of reversible black-boxing since law enforcement agencies had to understand (unravel) the role of each single element taking part in the botnets and its complex interconnection with other elements. They were not able to take down the botnet as a criminal network by focusing either on the human elements (the botherder) either on the technological elements (the servers). By removing only one of the elements or actors, the botnet would 'reorganize' itself. In that sense, it can be argued that a botnet represents a hybrid (cyborg) entity, which can only be understood and taken down when the human and non-human elements are dismantled in association, an aspect which is also central in ANT's meaning of complexity of actorship. Of course it can be argued that combatting crime in the physical world might also require more than just arresting the perpetrator, yet these crimes do not have such a high number of technological and automatic agents involved that can stay active for quite a while without human intervention. Lastly, the takedown process provides an interesting example of Latour's meaning of translation. From an ANT perspective, Bredolab enabled the police to

use its functionality for their own program of action (ending the infection).

2.9. Discussion

Our results support Latour's argument that we cannot understand phenomena by neglecting the complex intermingling between human and non-human actors. The creation as well as maintenance and use of the botnet consisted of a complex chain or heterogeneous network of actors which was built, rebuilt and simultaneously had self-organizing and automatic features. Even though the botherder seems at first sight a criminal mastermind who was able to create a large-scale sophisticated infrastructure and enroll millions of infected computers in his network, he could only accomplish this result thanks to the contribution and participation of myriad of other actors and their interrelation. Sometimes these actors were designed or built to contribute to the creation and maintenance of the botnet (e.g. the network of servers), in other cases, they had to be fooled (the users) and in other cases they already existed (e.g. Bredolab, the list of websites with flawed software). The botnet was simultaneously part of a larger actor-network of users and threatened by the anti-program of law enforcement agencies, operating systems, anti-virus software and companies, and sometimes even 'threatened' by its own success.

Our case study also shows that agency often has a networked and hybrid character. Firstly, it can be argued that non-humans can already play a role in the initiation of crimes. While Bredolab co-shaped the initiation

of the botnet, the created botnet in turn invited new crimes, partly due to its malicious prescription or affordance. Secondly, the case study reveals that non-humans played an important role in the victimization process. While artifacts such as banners mediated in the fooling process, the operating system either allowed or blocked the actual victimization. Thirdly, our findings support Latour's notion that humans are not able to fully master or control technologies. Although the botherder was able to manage the botnet in an efficient manner, he could not always foresee what the interacting components of the network would eventually produce. In view of these findings, the cyborg figure provides a useful metaphor for resembling crimes such as botnets, not only when it comes to the hybrid composition of these networks (who/what acts) but also regarding who and what gives shape to the criminal actions.

The most important question is now whether ANT has provided us with insights we were not able to gather with a more conventional criminological lens. We firstly believe that ANT enabled to draw attention to a broader range of actors who either intentionally or unintentionally participated in the creation and maintenance of botnets. Rather than just mapping them, we were able to illustrate that these actors (whether small or big, human or non-human) only became significant when they were part of a larger network of actors. Secondly, we believe that ANT enabled us to more thoroughly describe how the offending, victimization and the defending process are intertwined. Rather than viewing offenders, victims and defense as pre-existing and somewhat separate elements (as in routine activity theory), ANT is able

to treat these elements as networks by themselves that have no fixed borders or essence and are constantly surrounded and shaped by actors that either support or fight them. Thirdly, ANT has added value when it comes to describing how non-human actors can participate in the crime as mediators. As ANT does not presume the primacy of human over non-humans and does not view their relationship as instrumental, it is better able to shed light on how other actors besides the botherder co-shape the criminal action over time and the final outcome. Indeed, a rational choice approach would also recognize that the botherder sometimes has to make changes in his original plan or strategy, e.g., because the tools he uses do not bring the pursued result. The main difference is that ANT does not *a priori* conceptualize the offender as a (bounded) rational (or irrational) actor and does not place the offender's choices and actions on the foreground. An ANT approach is therefore better able to explain the random, unintended and uncontrollable aspects of the crime process.

Accordingly, we believe that ANT and its cyborg lens touches upon a dimension that is present in many forms of cybercrime and thus can also open up new ways of studying and conceptualizing other forms of cybercrime. We suggest the term *cyborg crime* as a general description of crimes in which the technological agency has become so important that ANT, with its networked and hybrid agency conception, reveals aspects of the complexity that traditional approaches may overlook. While we, in this study, applied the cyborg lens to the understanding of the composition, structure and formation of botnets (as hybrid criminal networks), the lens could also be applied in other contexts and by using

other methods. For example, the lens could be used to study how non-humans co-shape the intentions, perceptions and actions of online offenders (and victims). If used this way the emphasis would lie more on the level of crime motivation and experience, which requires a more ethnographic approach. Of course, the full implications, utility and reach of the cyborg crime perspective requires additional research. For example, forms of technical mediation that are specific to the cyber domain may emerge from cross-case analyses, as well as from studying certain aspects in more detail, such as the particular types of delegation in which users are fooled into doing something for the attacker (basically accepting their computer to become infected). In addition, the technological infrastructure is subject to continuous change, and developments in, e.g. cloud computing may alter the botnet battlefield, as they also allow for (legally) renting computing infrastructure as a service. Studies into such changes, their relation with criminal activities and the associated role of actants could enhance the ANT perspective. Finally, the defense against cyborg crime will most likely need to have a cyborg structure itself, and the same lens could therefore be applied to study the hybrid structure of networks dealing with counteracting these crimes.

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.

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.

Chapter 5

The Hybrid Victim: Re-conceptualizing High-Tech Cyber Victimization Through Actor-Network Theory*

* Van der Wagen, W. & Pieters, W. (2018/under review). The hybrid victim: re-conceptualizing high-tech cyber victimization through actor-network theory.

Abstract

Victims are often conceptualized as single, human and static entities with certain risk factors that make them more vulnerable and attractive for offenders. This framework is challenged by emerging forms of high-tech cybercrime, such as ransomware, botnets and virtual theft, where the victim constitutes a composite of human, technical and virtual entities. This study critically assesses the current theorization of the cyber victim and offers an alternative approach. Drawing on actor-network theory and three empirical case studies, it theorizes the cyber victim as a hybrid actor- network consisting of different entities targeted by the offender(s). The proposed concepts of victim composition, translation and delegation enable to gain a more profound understanding of the hybrid and complex process of becoming a high-tech cyber victim.

Keywords: cybercrime**,** cyber victimization**,** actor-network theory, botnet, ransom ware, virtual theft

5.1. Introduction

While computer viruses have existed already for quite some time, today's 'digital demons' seem to take it even further. Nowadays our computers and devices can get infected with all kinds of advanced malicious software (malware[43]), enabling an offender to take over computers and use them as 'bots' or 'slaves' in a cyber-attack, or remotely taking a computer 'hostage' by means of 'ransomware'. In the latter case, the computer or computer files are locked or encrypted, denying the victim access until the ransom has been paid (Gazet, 2010). Malware can be used also to steal personal credentials or to make fraudulent bank transactions, e.g. by luring computer users to fake websites, a deceptive technique called 'phishing' (see, for example, Jansen & Leukfeldt, 2016; Hutchings & Hayes, 2008). In other words, our offline, digitalized and virtual lives can be targeted and harmed in multiple new, different and sophisticated ways.

These more technical forms of criminal victimization differ from traditional victimization in various manners. For instance, the interaction between the offender and victim is much more indirect (Reyns, 2011) and the offensive actions are often directed towards (multiple) vulnerable technical devices rather than towards humans alone. This poses the question whether victimologists and criminologists

[43] Malware can be considered as "an umbrella term used to encapsulate the range of destructive programs that can be used to harm computer systems, gain access to sensitive information, or engage in different forms of cybercrime" (Holt *et al*., 2015: 80).

are confronted with more hybrid kinds of victims than they are familiar with, and whether existing theories and concepts provide sufficient analytical power in this context.

This article critically assesses the current criminological theorization of the 'cyber victim' in light of new emerging forms of high-tech cyber victimization and provides an alternative conceptualization. In this context we adopt a problem-driven approach. Based on the analysis of three empirical cases of cyber victimization, involving respectively ransomware, botnets and virtual theft, we demonstrate that existing approaches commonly used in cybercriminology, the lifestyle routine activity approach in particular, are too anthropocentric, reductionist and dualistic in nature for a type of victimization in which there are no clear boundaries between the human and the technical, the actual and the fictional and the offending and the victimized (see also Brown, 2006; Aas, 2007; Van der Wagen, 2018 *forthcoming*).

We suggest an alternative conceptualization of the cyber victim through exploring the theoretical potential of Actor-Network Theory (ANT; Latour, 2005). In this context we build on the framework proposed by Van der Wagen and Pieters (2015) and Van der Wagen (2018 *forthcoming*) in the context of offending, but extend the framework to victims and victimization. ANT is a critical and constructivist approach that provides a conceptual framework in which entities, actors and actions are understood in a networked, heterogeneous and complex fashion (Latour, 2005; Verbeek, 2006). ANT does not differentiate a

priori between entities in terms of their *essence*, for example human versus non-human or victim versus offender. Rather it is interested in what different entities (as a network) do and how they contribute to certain actions or results, for example victimization (Law, 1992; Latour, 2005; Van der Wagen & Pieters, 2015). Drawing on this perspective, we propose to conceptualize the cyber victim as a heterogeneous network consisting of interacting human, technical and/or virtual entities that in a relational manner has to be targeted, deceived and/or controlled by the offender(s) – the latter also being an actor-network (see Van der Wagen & Pieters, 2015). This alternative framework consists of three interrelated concepts: 'victim composition', 'victim translation' and 'victim delegation', the combination of which enables a more nuanced understanding of the hybrid and complex process of becoming a high-tech cyber victim.

The first section of this article takes a glance at how the high-tech cyber victim is currently theorized in existing cybercriminological research. Hereafter we present the three empirical cases and point out different conceptual limitations of existing approaches in capturing the features of these forms of cyber victimization. The article then discusses ANT's conceptual framework and assesses its potential in relation to the cases, resulting in an alternative conceptualization of the high-tech cyber victim. In the final discussion we will touch upon the wider implications of the proposed hybrid victim approach and provide suggestions for further research.

5.2. The current theorization of the high-tech cyber victim

In recent years, cybercrime victimization has become an important and rapidly evolving field for criminology (see Holt and Bossler, 2014). Although it is a rather specific subfield, it deals with a wide variety of criminal victimization. Cybercrimes can be targeted against specific individuals (e.g. online harassment, stalking), groups of individuals (e.g. hate crimes), computer systems or networks (e.g. hacking), (large) populations of computer users (e.g. virus infections), virtual entities (e.g. cyber rape), critical infrastructures (e.g. cyber attacks against power plants) and so on. The current study concentrates on the theorization of forms of cybercrime that have a significant technical or 'high-tech' dimension, also referred to as 'computer-focused crime' (Maimon *et al*., 2015) or 'true cybercrime' (Wall, 2007). These crimes differ from the more 'low-tech' cybercrimes (e.g. cyber stalking) in the sense that digital technology is not only used as the means to commit crime, but is also a substantial target (Koops, 2011). These crimes have gained relatively little attention in criminology (see, for example, Bossler & Holt, 2009; 2011; Leukfeldt, 2015), while their technical nature might challenge existing theoretical frameworks more or differently than so-called computer-enabled crimes such as cyber stalking.

Criminological studies that have been conducted on high-tech cyber victimization are predominantly empirical tests of the life style approach (Hindelang, Gottfredson & Garofalo, 1978) and/or the routine activity theory (Cohen & Felson, 1979), theories that are also most influential in

traditional victim studies. The life style model supposes that certain behaviors (e.g. related to work, school and leisure) expose certain persons with certain demographic features to certain risky (crime-prone) situations (McNeeley, 2015). RAT on the other hand, focuses more on crime and victimization as an event (Pratt & Turanovic, 2015). It considers victimization as the result of the convergence in time and space of a motivated offender, a vulnerable or suitable target/victim and the absence of capable guardianship. It assumes that motivated offenders seek to find places where suitable targets are concentrated, but also places where they can find an absence of capable guardianship: humans or objects that can prevent crime from occurring (e.g. a fence, a surveillance camera or a police officer) (Yar, 2005a). Although these theories are distinct approaches, they lead to similar hypotheses and are often combined in one framework, also denoted as general opportunity theory or life style routine activity theory (see McNeeley, 2015 for an overview).

Following this approach, studies on (high-tech) cyber victimization seek to unravel which individual and situational factors put certain people at risk for cyber victimization. Yet, instead of offline activities, these studies concentrate primarily on people's *online* routine activities such as how much time they spend on the Internet and which websites they visit. Some scholars criticize such a segregated approach and argue that both offline and online activities should be assessed simultaneously in order to explain the transmission of risk in these domains (Van Wilsem, 2011). Others examined whether RAT, which was originally designed to explain

direct-contact offenses, can be still applied in the cyber domain (see e.g. Reyns, 2011). Yar (2005) for instance concludes that the three separate elements of RAT hold quite well in cyberspace, but the convergence of the elements in time and space is problematic due to the anti-spatial nature of cyberspace. Although such limitations are widely acknowledged, RAT remains to be the dominant perspective used to study (high-tech) cyber victimization, even in qualitative studies on cyber victimization (see e.g. Jansen & Leukfeldt, 2016). More recently, Gottfredson and Hirschi's (1990) theory on self-control is also used to study high-tech cyber victimization, which relates low self-control to the likelihood of becoming a victim. This perspective is often combined with a situational approach as well (see Bossler & Holt, 2010).

In short, criminological studies on high-tech cyber victimization generally apply an opportunity-based approach, hereby seeking to map the individual and structural features of the cyber-victim population. Although online and technical risk factors are also examined, these studies tend to conceptualize the victim in a similar vein as the victim of traditional crime: as a vulnerable (human) entity to whom certain risky characteristics apply that make them more visible, suitable and/or attractive for offenders. We question however whether such a framework provides an adequate and sufficient basis for the analysis of high-tech crime victimization as it has certain features and dynamics that we cannot or to a lesser extent observe in traditional forms of victimization.

5.3. Setting the empirical context: the victim of ransomware, botnets and virtual theft

In order to critically assess the dominant theories that are currently applied in criminology, we now take a closer look at three empirical cases of high-tech crime victimization, involving ransomware, botnets and virtual theft. By drawing on these cases and the features that can be abstracted from them, we seek to more concretely examine the applicability of current frameworks and to expose how and why they are contested. At the same time, the cases are used as the empirical basis for assessing ANT's analytical potential in relation to high-tech cyber victimization later in the article.

The reason for selecting these particular three cases is twofold. Firstly, the cases represent recent and underexplored types of high-tech cybercrime victimization and its characteristic general features, while each case also has distinguishing victimization elements, as discussed below. Secondly, we had the unique opportunity to get access to these cases through police investigations and offender interviews. The first two cases concern police investigations that were placed at our disposal by the Dutch High-Tech Crime Police Unit. Both investigations included

information on the victimization process.[44] The third case study is based on a face-to-face interview[45] with an offender who was engaged in virtual theft by hacking the computer system of his counter players. He explained in great detail how he conceived and targeted his victims, hereby providing insights in how this particular type of victimization takes shape.

In the following, we will first introduce the cases and then assess the analytical power of existing theories in analyzing the associated victims and victimization processes.

Case 1: Ransomware victimization

Ransomware can be defined as "a kind of malware which demands a payment in exchange for a stolen functionality" (Gazet, 2010: 77). Although ransomware emerged already in 1989 under the name 'PC Cyborg' (Overill, 1998), the concept of taking a computer system hostage has become extremely popular, threatening and sophisticated in recent years (see, for example, Trendmicro.com). The current case concerns one of the earlier manifestations of ransomware, also denoted as 'scareware',

[44] The ransomware case (2015) included information about the modus operandi and also contained a number of victim statements from individual computer users and companies whose website was used to distribute the malware. The botnet case (2010) contained mainly information on how the offender set up the botnet infrastructure and how the malware was spread (see Van der Wagen & Pieters, 2015 for a full case-description and analysis).
[45] This interview took place in 2015 and was conducted in the scope of a research on hackers (see Van der Wagen, 2018 *forthcoming*).

which is relatively easy to remove from the computer[46] and strongly depends on techniques of deception to make the computer user pay. At least 65000 computer users (only) in the Netherlands were infected with it.

The ransomware was mainly spread by means of infecting advertisements on pornographic and illegal downloading websites, but also through more regular websites such as newspaper and library websites. The targeted websites made use of an automated advertisement system such as banners and popups, based on a contract with an advertisement company. The offender(s) [47] purchased advertisement space and programmed the advertisements in such a manner that the ransomware could be downloaded when the computer users clicked on them. In this process computer users were actually silently re-directed to a server where a so-called 'exploit kit' was running, an advanced tool that automatically scans the vulnerability of the computer system and enables the installation of the ransomware. After its installation the computer displayed the following message: *"You are a suspect in a crime [e.g. distributing child pornography or illegally downloading content] and should pay a 100 euro fine [within 48 hours] in*

[46] The newer generations of ransomware, often referred to as 'cryptolocker', cannot be removed this way. Due to its sophistication it can force the victim to choose between payment or loss of the data. Only the offender has the key to decrypt the encrypted files, which he will (or will not) provide after payment.
[47] The police officers presumed that a professional criminal organization was behind the scheme, including malware writers, ransomware designers and botnet owners. They were however only able to arrest the offender who was responsible for infecting the Internet traffic with the malware, also referred to as 'traffic manager.'

order to avoid criminal charges as well as to regain access to your computer." The pop up message also included logos of the police and of the stores where the pay safe card could be bought. The users had to insert the code of the card in the field that was displayed on the blocked computer screen.

As we can read in the victim statements, those who paid the ransom sincerely believed that the displayed message was authentic. Most of the victims mentioned that the genuine-looking law enforcement imaginary, logos and text tricked them, along with the fact that the computer really appeared to be blocked. Only when the computer remained blocked after paying the ransom, most users realized that they were deceived, reported the incident to the police and visited a computer store for removal of the malware.

Case 2: Botnet victimization

A botnet can be defined as a network of 'victimized machines', 'zombie computers' or 'slaves', under the remote control of an offender (denoted as 'botherder'), facilitating a broad range of crimes, including banking malware, credit card theft and distributed denial-of-service (DDoS) attacks[48] (Wagenaar, 2012). While in the case of banking malware and credit card theft, the attack is directed at the bots within the network of infected machines; in the latter case the infected machines are used to

[48] A DDoS attack is "an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources" (http://www.digitalattackmap.com/understanding-ddos/)

attack machines or systems outside of the network (Schless & Vranken, 2013). The current case, which involved a botnet of at least three million computers, included both types of attacks.

In order to set up and control the botnet, the botherder first had to infect the computers with bot malware, in this case "Bredolab". He was aware of a specific vulnerability in advertising software and purchased a list of websites that used this particular software. He gained access to at least the advertisement space of 148 websites through which he was able to target a large number of computer users. As soon as Bredolab was successfully installed on the computers it basically functioned as a so called 'downloader', a program that enables the installation of additional malware, mostly on behalf of third parties who could make an order in the 'botnet shop' of the botherder (see also De Graaf, Shosha & Gladyshev, 2013). This additional malware was, for instance, a Trojan[49] that steals banking credentials from the compromised machines (Van der Wagen & Pieters, 2015).

The malware spread at unprecedented speed. Within a relatively short time multiple bots joined the network, even requiring that the botherder had to expand his infrastructure. However, the vulnerability the botherder was able to exploit was at some point (ready to be) patched or fixed by a security company. In order to prevent the patching of the software, he launched a DDoS attack on the company. Soon hereafter, law

[49] A trojan is type of malware, which appears in the capacity of something else (e.g. a file or attachment) and "requires some user interaction in order to execute the code" (Holt *et al*., 2015: 86)

enforcement agencies traced the botherder and dismantled the entire botnet (see for a full description Van der Wagen & Pieters, 2015).

Case 3: High-tech virtual theft victimization

Virtual theft refers to theft that takes place in the context of a virtual world or online game. As the stolen virtual goods can have actual material value, virtual theft is considered an illegal activity, an issue widely discussed by legal scholars (see, e.g., Strikwerda, 2012). The interviewed offender was active in a multiplayer game in which certain missions had to be accomplished for which he could earn valuable gears and outfits. The offender put forward that he was able to steal thousands of euros from his counter players, for which he employed two distinct methods.

In the first method he installed a remote access tool (RAT) on the computer of the counter player, a tool or Trojan that enables to take over someone's computer and webcam remotely. He was able to install the RAT by luring the counter players to a self-created (malicious) genuine looking website that was related to the game. He started a chat conversation with the counter players and then sent them the link of the fake website, e.g., by saying: "Here you can find the newest items of the game". Once the person clicked on the link, the RAT was silently installed. The offender sent the link of the fake website also to the friends of the victim in order to infect them with the malware as well. The next step was to observe the counter players through the webcam and to wait until

they left the computer, which gave him the opportunity to steal the most precious virtual goods from their account. After he succeeded, he removed the malware from the computer and deleted all the traces of his presence. The second method is rather different. The offender here in the capacity of virtual player (he had about 14 accounts) attacked his counter players during the game itself, while simultaneously launching a DDoS attack on their computer (IP address).[50] During this attack, the counter player was not able to defend him or herself as the system temporary crashed. After killing the player, he could take ('win') their virtual belongings.

5.4. Limitations of existing frameworks in analyzing high-tech crime

As mentioned earlier, one of the core assumptions within traditional frameworks is that certain individual and situational risk factors increase the likelihood of becoming a (cyber) victim. On the basis of the three cases, it seems that analyzing such factors can contribute to more knowledge about cyber victims. For instance, not updating the software, visiting certain websites and/or clicking on (malicious) advertisement banners, pictures or links, most likely increases the likelihood of becoming infected with malware. However, when we look more closely

[50] In order to accomplish the DDoS, the offender first had to figure out the IP address of the counter player, by means of an IP tracker. He sent a picture or file to them, in which the IP tracker was hidden, which installed when it was opened. He then used a botnet from someone else to launch the DDoS attack.

at the process in which the victim is targeted and becomes a victim, existing criminological frameworks seem to also encounter certain conceptual problems and have some critical blind spots.

Firstly, in the life style routine activity theory, risk and vulnerability are generally attributed or assigned to single entities. However, as we have seen in the cases, not one single homogeneous entity has to be targeted by the offender, but rather a chain or *network* of various human, technical and/or virtual elements, either chronologically or simultaneously. For instance in both the ransomware and botnet case, websites or advertisement companies have to be targeted first before any computer system can be infected and before any computer user and/or his personal data can be targeted. This not merely entails that offenders have to take different steps to victimize someone or something, which obviously applies to many traditional crimes as well. Our point is that it shows that computer users are partly victimized through the vulnerability of other entities, e.g. vulnerable advertisement software, vulnerable websites and/or other vulnerable computer users, entities with whom they consciously or unconsciously, directly or indirectly establish a connection. Such complexity makes a single and homogeneous conception of vulnerability and risk therefore problematic. At the same time these various entities also become victimized and not merely the eventual computer user. For instance, in the case of ransomware, website owners also considered themselves as victims and filed a complaint, while they at the same time contribute to the distribution of the malware (see third limitation). In this respect, the

question “who is entitled to be classified as a victim, by whom and under which circumstance” (Mythen & McGowan, 2018) also seems to be relevant in the context of high tech cybervictimization.

Secondly, it can be argued that existing frameworks are too anthropocentric when it comes to grasping who/what is ‘the victim’ in high-tech cyber victimization, an issue that has also been raised with regards to victims of environmental crime, such as animals, plants and ecosystems (see, for example, Hall, 2011; Halsey and White, 1998). Green criminologists plea for a broadening or extension of the victim concept, in order to give non-humans also the status of victim and take a critical stance towards the individual and human conception of victimhood in traditional frameworks. The emphasis on humans as victims has also been debated in the context of virtual criminality, which involves not merely entities that are non-human, but also those that are virtual and fictional. In the case of virtual rape for example not the human body is physically harmed, but rather the ‘virtual self’ is the one emotionally suffering, which in turn poses the question whether victimhood requires a conceptualization beyond the human body (Brown, 2006; Strikwerda, 2015).

In the context of high-tech cyber victimization, we do not argue for a broadening of the victim concept in the sense that technical or virtual entities should also have the status of victim. Instead we stipulate the rather hybrid nature of the victimized entity. As we have seen in the cases, the victim often constitutes a blend of humans and machines, of

people and information and/or of human, virtual and technical entities *and* is also targeted as such. An either human or non-human conception of victimhood would therefore not be satisfactory; an issue that also has been addressed by Whitson and Haggerty (2008) in their study on identity theft. They argue that 'the victim' of identity theft is nor merely human nor merely digital but a blend of both. The hybridity in high-tech crime victimization is functional but can also, like virtual criminality, have a subjective or experiential dimension. When our device, computer (or webcam) is hacked, invaded or taken hostage as in ransomware, the victim might experience that the boundaries between the human body and the object fade away, perhaps in a similar vein as with a domestic burglary. Concerning the latter, Kearon and Leach (2000) argue that a house cannot merely be considered as a property or space of the human (victim), but could also be regarded as an extension of the human self. The authors therefore argue for a more cyborgian understanding of how victims experience such burglaries. In any case, the boundaries between the human and the technical, the actual and the fictional, the offline and the online are rather blurry in high-tech cyber victimization. It is questionable whether traditional victim approaches in criminology can sufficiently grasp such blurriness since they still maintain binary oppositions (Brown, 2006; Franko Aas, 2007).

This brings us also to the rather dualistic nature of criminological frameworks. Opportunity theories and also criminology at large maintain strict divisions between what is human and what is technological (see also Brown, 2006; Aas, 2007), but also between who

is the victim and who is the offender (Van der Wagen & Pieters, 2015). Although much work has been done in victimology to study why offenders are more likely to become victims as well - also denoted as the 'offender-victim' overlap (see Jennings, Piquero & Reingle, 2012) - ontologically criminologists still consider the victim and the offender as two separate entities. As we can see in the cases, such distinction might vanish when digital technology is involved. In the case of botnets for example the victimized machines become part of a larger network of machines and are then used to attack others. A botnet can thus be simultaneously a victim or victimized network, an infrastructure or tool for other crimes and then operate in the capacity of an attacker. Also in the case of infected websites and in the use of already hacked accounts to spread the malware further we see this dynamics. This contagious nature of the victimization process also makes it more difficult to determine when an actual victimization virtually begins and ends, just like a biological virus. Life style routine activity theory tends to analyze and conceptualize victimization in terms of a concrete event, while victimization in the digital age can have a long lasting and unpredictable nature (see again Whitson & Haggerty, 2008).

Thirdly, life style routine activity theory is more engaged with assessing the suitability of the victim than the targeting process itself when it comes to explaining victimization. As we pointed out already, victimization is conceptualized in terms of *exposure* and *proximity*: when a motivated offender will encounter a suitable victim who/which lacks proper guardianship, the victimization is likely to occur. The cases

revealed that such a process is much more complex and interactive than opportunity theory suggests. First, the cases show that high-tech cyber victimization often takes place in a context of human, technical and virtual deception. Offenders make it hard for a user to distinguish a 'real' from a fraudulent or fake website and/or use a set of psychological tricks to deceive them (for example, by establishing trust and/or generating fear). As Cross (2013) points out, the deceptive context is a dimension that is often taken for granted in existing victim studies, while it is essential for grasping the complexity of how a vulnerability is generated and exploited. Second, we can observe in all three cases that, in the course of the victimization, victims have to complete an action for the offender (for example, clicking on a link). Without their contribution, the victimization will not succeed (Van der Wagen & Pieters, 2015). In this respect, high-tech crime is clearly different than a burglary, which is not particularly interactive (Rock, 2007), but does have similarities with fraud and deceit. Consequently, we cannot understand high tech cyber victimization as a process fully carried out and orchestrated by the offender either. As Demant & Dilkes-Frayne (2015) point out in their discussion of the limitations of situational crime prevention (SCP): we (criminologists) cannot understand how crime events unfold when we merely look at the (rational) choice making of offenders. They conceptualize crime events, in the footsteps of ANT, as a process that is co-shaped by multiple entities in the network and not merely by the offender. This angle is also one of the cornerstones of our approach to victimization (see later on).

This interactional nature of victimization automatically brings us to another theoretical aspect worth considering in the context of high-tech cyber victimization. The issue of how the victim plays a role and participates in the victimization process – aside from 'being vulnerable' or 'putting themselves in risky situations' - seems to be somewhat undertheorized or taken for granted in opportunity theory. The issue is however (considered to be) overemphasized in the traditional though controversial concept of 'victim precipitation,' which refers to the notion that victims actively contribute to their victimization (Von Hentig, 1940; 1948). This concept has always been associated with 'victim blaming' rather than merely being a neutral concept for 'just' analyzing the interaction between offenders and victims (see Rock, 2007). Based on what we have seen in the cases, it can be argued that victim contribution is a dimension that also needs further theoretical consideration if we fully want to grasp how high-tech cyber victimization takes shape as an interactive process. As we will argue later, the victim is one node among others that plays a role in the realization of high-tech cyber victimization.

5.5. The lens of actor-Network theory

The limitations outlined above - the rather anthropocentric, dualistic and reductionist nature of existing approaches used to study (high-tech) cyber victimization - led us to the constructivist framework of actor-network theory. ANT can be situated in science and technology studies and is commonly connected with the work of Callon (1986), Law (1992;

2004), Mol (2010) and Latour (1992; 2005). As its founders emphasize, ANT is not a theory in the traditional sense of the word, but rather a critical framework or lens that provides a list of sensitizing terms (Mol, 2010). ANT criticizes traditional social scientists (e.g. Giddens, Durkheim, Habermas, etc) - which Latour refers to as 'the sociologists of the social' - for treating 'the social' as a distinct substance (next to technical, biological and economic ones) and for presenting the social as some kind of stable force or cause (see Latour, 2005). Alternatively, Latour proposes to treat the 'social' or any 'thing' as a network or collective of various non-social (human and non-human) elements. This approach of the social he terms the 'sociology of associations.'

ANT also criticizes traditional sociology for considering 'the social' merely as the domain of interpersonal relations. It calls for a 'material turn' or a 'turn to things' (see also Preda, 1999), which argues that non-human entities should be viewed and studied as *active* participants within the social world. By arguing that human and non-human entities deserve symmetrical analytical attention (at least initially), ANT distances itself from anthropocentric or phenomenological approaches, which are mainly centered on humans or representations of humans. ANT also disassociates itself from the other meaning commonly associated with constructivism: the claim that social reality is constructed. Latour (2005) clarifies ANT's link with constructivism, by referring to buildings that are still 'under construction'. If the researcher would visit the scene (more than once), he or she would be able to observe all the human and non-human elements that co-shape or

constitute the building. These elements and their interrelation will (partly) vanish as soon as the building is completed. ANT's task is to study and make visible the process of how these elements turn (or how they are turned or have been turned) into more stable units. This line of reasoning ANT applies to everything, including the manufacturing of scientific facts (Latour, 1987; Latour & Woolgar, 1986). Latour's position can therefore be best understood as 'anti-blackboxing'. ANT does not aim and claim to be (better) able to capture reality, but to offer a lens which is particularly sensitive for processes (or actors) that are either hidden, blackboxed, taken for granted or treated in a mundane or passive manner (Mol, 2010).

We will now provide a brief overview of ANT's conceptual framework, which further specifies the above description of the ANT lens. Thereafter we will assess ANT's theoretical potential for analyzing high-tech cyber victimization.

One of the core concepts of ANT's framework, which also reflects ANT's criticism on the sociology of the social, is the metaphor of *heterogeneous network*. This concept reflects the notion that many terms we are familiar with (e.g. society, organization, machines, power, crime, offender, victim) are networks or *network effects* rather than single point actors or entities (Law, 1992; Callon 1986). ANT considers it as its task to deconstruct the (network of) separate elements of the actor, a practice also referred to as *reversible blackboxing*. Important to stress is that ANT's conceptualization of the network is not the same as the term is

commonly used, also in criminology. Firstly, as the word *heterogeneous* already implies, the actor-network not merely includes humans, but also comprises non-humans such as texts, machines, architectures, tools and so on (Law, 2004; Latour, 2005). ANT does not a priori make a distinction between what is human, technical, cultural or political; everyone and everything is treated as a hybrid collective of multiple interacting elements and should be studied as such (Latour 1993; Verbeek 2006). Secondly, the actor-network represents a network with a *complex* nature or topology. Unlike technical networks, which are strategically organized and its nodes intensely connected, the actor-network has a more open, complex, thread-like or 'rhizomatic' character, which cannot be captured in orderly terms such as levels, structures, layers or systems (Latour, 1996; Van der Wagen & Pieters, 2015).

ANT also points out that we should look at *actions* in a networked and heterogeneous fashion. It speaks of *actants* instead of actors, to pinpoint that humans and non-humans do not act separately but always in the capacity of 'hybrids' (Brown, 2006; Latour, 2005; Van der Wagen, 2018 *forthcoming*). For instance, when we drive, we act as 'human-car hybrids' (Dant, 2004) and when we shoot we act as a 'man-gun hybrid' (Bourne, 2012). ANT presumes that the abilities and strength of both humans and non-humans are often combined (in a network) when certain actions are carried out. In ANT terms, the human's *program of action* and the non-human functionality merge into a 'translated' program of action, a process also termed *translation* (Latour, 1992; 1994). The same principle of hybridity we can find in Latour's concept of *complexity of actorship* or

composition, which also seems to add a more organizational or strategic dimension. The classical example that is provided in this context is a hotel manager who wants to prevent that the guests forget to return their key. In order to achieve the program of action (getting the key back) and to prevent or 'defeat' the *anti-program* (not bringing the key back), the manager will add oral notices, written notices and finally metal weights to the key (Akrich & Latour, 1992; Latour, 1992). To make a connection with the earlier concept of heterogeneous networks, thinking in terms of programs of actions and anti-programs also provides a way to study the ordering of (actor) networks.

A related concept is ANT's notion of delegation. In order to complete a certain program of action, actions can be also *delegated* to humans or non-humans, which in turn results in a *distribution of competences* (Latour, 1992: 158). In the given example the metal weights attached to the key could be perceived as non-human delegates as they are assigned a role, which co-enables the program of action. ANT's concept of delegation does however not merely refer to the outsourcing or automation of a certain task. It also emphasizes that, when we delegate a task, we cannot fully predict its outcomes and effects. It might for instance generate certain unforeseen events, interactions or usages, which were not intended by the designer of the (delegated) object (see further Verbeek, 2006; Latour, 1992; 1994).

5.6. Conceptualizing high-tech cyber victimization through ANT

From the above description, it follows that ANT is a lens that requires viewing actors and actions in a more networked, hybrid and complex manner, a principle that is resembled in each single ANT concept. Drawing on this perspective, we propose to conceptualize the high-tech cyber victim as a heterogeneous network of various interacting elements that have to be targeted, deceived and/or controlled by the offender, being also an actor-network (Van der Wagen & Pieters, 2015). This analytical framework includes three main interrelated concepts: *victim composition*, *victim translation* and *victim delegation*, which we now will discuss in more detail with references to the earlier discussed cases and their features.

Victim composition

As pointed out before, there is often no single victim or target involved in high-tech cybercrime, but rather a chain or network of (multiple) targets/victims (human, technical and virtual) whose vulnerability has to be targeted, either sequentially or relationally. Traditional opportunistic frameworks, which have a tendency to attribute risk or vulnerability to a single point actor, therefore seem to have limited explanatory power in this context. ANT's concept of *composition* offers a valuable alternative, as it perceives notions such as risk and vulnerability as something distributed, relational and emergent. From this angle one

asks and analyzes how various entities generate this vulnerability rather than (pre-) assigning vulnerability to the eventual victim/target, e.g. the computer user. Non-human entities such as websites and software are then also considered as an integrative part of the victimized network rather than being merely considered as guardians or protecting agents, which excludes them from the targeted network. This also entails that we should not a priori make demarcations between a human and a technical vulnerability, but to look at how a vulnerability is generated by a hybrid network of both.[51]

As we have seen in the cases, the technical vulnerability is always essential to target a computer user, yet is often still not exploitable without a human vulnerability and/or a human action such as one 'wrong' click (see also concept of delegation). At the same time, the victim is targeted as a hybrid entity, being neither entirely human nor exclusively technical or virtual. In the case of ransomware, the victim is targeted as a human and a machine, one enabling the targeting of the other and also in the hybrid sense that computers are not merely tools, but devices that people are attached to and depend on. In the case of botnets the victim is either a hybrid of human and machine, a hybrid of human and information and/or a hybrid of victim and attacker. In the case of virtual theft, the victim is a virtual player who is attacked in the

[51] In this respect we can also draw parallel with the ANT based approach presented by Masys (2014) who uses ANT to reveal that system vulnerabilities (in the scope of critical infrastructures) emerge within a hybrid and interdependent collective of human, physical and informational domains (see also the study of Mähring, Holmström & Monteolegre, 2004).

setting of a fictional game, but also as a 'real' person behind the avatar and webcam, possessing virtual goods with 'real value'. Even the offender himself operated in both the capacity of virtual and real agent blurring the distinction between the fictional and the actual. The concept of victim composition can thus unravel the hybrid nature of the victim as an entity and target, functionally and perhaps also in a more subjective manner.

Victim delegation

As we could observe in the cases, various human and technical entities are mobilized, designed, rented and/or purchased by the offender(s) to initiate, carry out and realize the victimization. Traditional approaches used in victim studies do not draw much attention to the offending process itself in the analysis of the victim. The concept of *victim delegation* can shed light on the process in which the offender assigns a task, role or action to various human entities (computer users and website owners) or non-human entities (compromised machines and exploit kits). It enables to study which part of the victimization process is carried out by which actor, while being at the same time sensitive for the option that the role of the entity in this process can change or 'translate' over time, (see further the concept of victim translation). Unlike the traditional concept of victim precipitation, victim delegation does not have the undertone of victim blaming and again, it also includes the contribution of non-human entities. Victim delegation should however not be perceived as an exclusively functional process where tasks are delegated to others than the offender. Delegating an action also

implies that various new (malicious) events and interactions (for example, generating more infections) can be set in motion, a process that is not fully controllable and predictable and might continue much longer than anticipated (see also Van der Wagen & Pieters, 2015). This brings us to the concept of victim translation.

Victim translation

As mentioned before, traditional approaches tend to treat the suitable target as a pre-existing and rather static entity exposed to a motivated (strategic) offender. It can be argued that such a view blackboxes the interactive nature and dynamics of the victimization process. From the ANT angle, victimization is considered as an interactive and generative process in which the victim as a network has to be created, programmed, controlled and exploited by the offender. ANT's concept of translation – which stipulates the transformative nature of events, actors and situations - could be useful to look at victimization in a more interactive and fluid way. Target suitability is then not considered as something pre-existing but as being partly determined and generated *during* the victimization process. At the same time the victim or victimized network is presumed to be subject to change throughout this process and is not treated as entirely passive or non-resistant. As we have seen in the three cases, offenders add (over time) various entities (e.g. new visual tricks) in their network to accomplish their program of actions (e.g. installing malware, steal virtual goods), but also have to defeat the anti-programs they encounter throughout this process. For instance, they have to

prevent the patching of the software by the security company (as we have seen in the botnet case), prevent that computer users refuse to pay the ransom and prevent that the computer user or virus scanner detects the malware. In addition, victim translation emphasizes that entities and the role that they play might change (or translate) when they encounter other entities. As we have seen in the cases, in high-tech crime there is often no clear distinction between who/what is the tool, the victim or attacker, most exemplary in the case of botnets where victimized machines are used in a cyber attack. This blurriness might be hard to capture by traditional approaches. Last, victim translation is a suitable concept for shedding light on the fluidity and contagious nature of the victimization process. As we have seen, the victim can be the 'final destination,' but at the same time the beginning of a new chain of infections. In short, victim translation like victim delegation, places more emphasis on the victimization as a (complex) process or event rather than on the victimized entity itself.

5.8. Conclusion and discussion: towards a hybrid victim theory

In this article we have aimed at outlining some major limitations of the current theorization of the cyber victim – the lifestyle routine activity framework in particular – and suggested an alternative conceptualization based on actor-network theory. We are not the first ones addressing ANT's theoretical potential with regards to (cyber)

crime (see, e.g., Brown, 2006; Hinduja, 2011; Smith *et al*., 2017). ANT's hybrid approach is considered to be a suitable approach for grasping the blurry boundaries between the human and the technical, the real and the virtual and so on, typical for the digital age we live in and for the new crime phenomena that are emerging. Concrete criminological studies applying or operationalizing ANT concepts empirically are also appearing more frequently (e.g. Demant & Dilkes-Frayne, 2015; Van der Wagen & Pieters, 2015). Applying ANT in various case studies is important since theoretical progress can benefit significantly from empirical research. This study also took up the challenge by examining if and how ANT's concepts can contribute to the analysis of the *victim* of high-tech crime.

By assessing the ANT lens in the context of three high-tech crime cases, we formulated three ANT-based victim concepts, a framework we would like to denote as 'hybrid victim theory.' The concept of *victim composition* resembles the notion that we should look at the (vulnerable) victim as a hybrid and distributed network composed of human, technical and/or virtual entities. It conceives vulnerability as a distributed and emergent feature rather than as a singular and static property. The concept of *victim delegation* is specifically concerned with the distribution of tasks and roles in the victimization process and how these roles can change over time. The concept of *victim translation* is closely related to the other concepts, but highlights the interactional, fluid and transformative nature of the victimization process. It does not view victimization as a concrete event, but as a complex interplay between (human and non-

human) programs of actions and anti-programs, hereby also including the offending process in the analysis of victimization. All three concepts emphasize the blurry boundaries between humans and non-humans, tools and guardians and offenders and victims. The concepts can be employed individually, but can also be used in an integrative or complementary fashion, forming one analytical framework for studying the hybrid and complex process of becoming a high-tech cyber victim.

The remaining question is whether a hybrid victim approach also has some wider implications. Does the approach, for example, offer new leads for prevention? How does it approach issues such as responsibility? It can be argued that hybrid victim theory might inform novel ways of thinking about crime prevention, or, at least add a dimension to current approaches within situational crime prevention (see also Demant & Dilkes-Frayne, 2015). For example, since it looks at how vulnerabilities are distributed among various human and non-human nodes in the victim network, it will also propose the set-up of a distributed network of (interconnected) anti-programs to defeat and or to prevent cyber victimization. Resilience is then also perceived as something that only can be effective when networks are built. Various parties, both public and private, should contribute to such strategy rather than operate as individual nodes. Of course, to some extent this is already done in practice, also when it comes to tackling malware-related crimes such as botnets (see e.g. Dupont, 2017). ANT could be insightful for developing such initiatives further since it draws attention to how different parties as an interdependent (hybrid) network can make a

difference. From the ANT angle even a small contribution could make a major difference, when the actor/actions is part of network.

Measures could be also directed at (preventing) particular (inter)actions that play a role in enabling high-tech cyber victimization. Since hybrid victim theory draws explicit attention to how non-human entities co-shape actions, the approach inspires e.g. to think about how technology can be designed in manners that encourages 'responsible' behavior (see also Verbeek, 2014), something that could also be applied with reference to potential victims. For example, stimulating computer users to frequently change their password, not to click on every link or attachment they encounter or to update their software, should not only be done verbally, e.g. by means of awareness campaigns; this can also be encouraged or even enforced technically. Different forms of (in-built) 'technical assistance' could (consciously or unconsciously) direct users in their behavior and hereby make them better equipped ('resilient') to combat and defend themselves against various cyber risks, including malware-based infections. Such measures, of course, also already exist, but could be further prioritized and developed.

From the hybrid victim approach, it would be also crucial to provide more assistance to computer users that have *already* been infected, since this can prevent that the malware will spread further or that victims become infected with additional malware. Dupont (2017: 109), in this context, gives the example of anti-virus companies offering victims "free downloadable applications that automate the disinfection process and

prevent mistakes." In light of the contagious nature of malware, such measures could indeed be very effective.

Towards the issue of responsibility, the hybrid victim approach would also adopt a more hybrid and networked view. It considers victimization as the product and (then also) the responsibility of various actors and parties who play a role in generating the victimization. Fixing vulnerabilities and becoming more resilient should then be perceived as a collaborative duty. In this respect we agree with Masys (2015) who puts forward that: "resilience does not reside purely in cyber security patches and technical solutions but requires a more comprehensive and collaborative approach that embraces the social, organizational, economic, political and technical domains" (p. 143).

This study only marks the beginning of criminology's engagement and theorization of high-tech crime victimization, based on a study of ransomware, botnets and virtual theft. Valuable research could still be done in terms of additional case studies, extensions of the new conceptual framework, and assessing the implications for quantitative research in the cyber domain. At the same time our study provokes the question about criminology's future engagement and role in the analysis of high-tech crime and victimization. Since vulnerabilities are to a large extent technical in nature, criminologists should get either more technically proficient and/or more closely seek to cooperate with computer scientists.

Chapter 6

General conclusion and discussion*

* This chapter is partly based on: Van der Wagen, W. (2018). Het 'cyborg crime' - perspectief. Theoretische vernieuwing in het digitale tijdperk. *Tijdschrift over Cultuur en Criminaliteit*, (8) 1: 19-34.

6.1. Introduction: the departure of the journey

The question whether cybercrime is old wine in new bottles or a new or distinct form of crime requiring new theories, has been troubling criminologists for quite some time now and the debate will most likely not be settled in the near future. Although criminologists agree upon the fact that cybercrime differs from traditional crime, globally, technically, socially, psychologically and virtually, there is no consensus on whether it should be conceived as something fundamentally new, demanding theoretical renewal. This dissertation also entangled itself into this conversation and took the latter position that cybercrime, high-tech crime in particular, is rather distinct. It assessed the (a)typical features of cybercrime and examined which theoretical challenges derive from those features for criminology (research question 1). Yet, it also added an extra layer to the conversation. Whereas most (cyber)criminologists mainly assess to what extent traditional theories can account for cybercrime, the current research specifically attempted to extend the criminological theoretical repertoire. It departed from the notion that criminological frameworks are generally too instrumental, anthropocentric and dualistic in nature for a type of crime in which technology is so ubiquitous, where deviants constantly interact with, through and against technology and where the boundaries between the human and the technical, the actual and the fictional, the offender and the victim get increasingly blurry. In the footsteps of e.g. Brown (2006) and Franko Aas (2007; 2010) it was argued that current cyber developments demand criminologists to abandon the still prevailing

binary oppositions, to take a critical look at the concepts they quite often take for granted (e.g. agency, the offender and the victim) and to explore alternative theoretical angles.

This dissertation took up this challenge and called upon the constructivist framework of actor-network theory (ANT), which is particularly known for its claim that humans are not the only significant actors in the social world. ANT provides a way of thinking that treats (technical) things in a more active way and also promotes an anti-dualistic, less anthropocentric and more hybrid and complex way of grasping the phenomena that we study. The dissertation explored whether and how ANT can counter the theoretical challenges criminology is facing and can offer a valuable alternative or addition (research question 2).

These two overarching research questions have been explored in a set of different case studies: a study of a large botnet, two small-scale ethnographic studies on hacking and a study of three types of high-tech cyber victimization, respectively ransomware, botnets and virtual theft. The rationale behind conducting these case studies was first of all a theoretical one. The assumption was that the theoretical potential of ANT could be assessed most comprehensively by directly confronting its rather abstract framework with different empirical contexts. At the same time, the separate case studies were conducted for the purpose of gaining a nuanced understanding of the involved forms of high-tech offending, offenders and victims. Hence, the objective of this dissertation was to

make a theoretical and an empirical contribution to (cyber)criminology at the same time, eventually resulting in the new concept or perspective of 'cyborg crime.'

In this concluding chapter I will first summarize the main findings of each case study presented in this book, which provides answers to both research questions. Based on these findings, I will then distinguish four main ANT dimensions that I consider valuable for the criminological study of cybercrime. These four dimensions I denote as the cyborg crime perspective. The next section takes a closer look at how the cyborg crime perspective considers non-human agency in relation to human agency. The chapter continues by discussing some possible legal and policy implications. Hereafter, in a more general vein, I assess the opportunities and possible pitfalls for a (cyber)criminological engagement with ANT. At the end of the chapter suggestions for further research will be outlined.

6.2. Key findings from the case studies

In the following subsections I will summarize the main findings from the case studies. Where did the study depart from and what was the final outcome? I will focus on both the relevant empirical and theoretical findings, depending on the main focus of the study.

6.2.1. The botnet as a hybrid criminal actor-network (chapter 2)

The first case study in the dissertation involved the analysis of the phenomenon of botnets, a type of crime that is exemplary for the robotic features of high-tech cybercrime. The study departed from the notion that the automated and distributed nature of botnets might challenge the rather anthropocentric view of criminology, including the commonly used routine-activity theory (RAT) and the rational choice approach (RC). Alternatively, it called upon ANT's constructivist lens and conceptualized the botnet as a hybrid criminal actor-network, as a network that is not exclusive human-driven. ANT's four meanings of technical mediation (composition, translation, delegation and reversible blackboxing) were used as a framework to study a large botnet case empirically.

The first main finding of this study was that multiple human and non-human actors (small and large) play a role in the building of the infrastructure of the botnet, the victimization process, the use and control of the botnet and its takedown. Although the role of the botherder was important, viewing the botnet merely as a network created and managed by a human agent does not tell the full story. As we have seen, a wide variety of actors was involved in the 'success' of the botnet. These actors were either created, already existed or had to be fooled in order to get enrolled in the program of action of the botherder. Secondly, the role of technical entities appeared to be more than just functional. They could for instance invite a certain use and/or additional (criminal) actions, either committed by the botherder or his customers.

They were also active in the sense that they changed the course of action and brought unanticipated situations for the botherder. For example, the explosive growth of the botnet could not be pre-determined by the botherder, requiring changes in the infrastructure. The third main finding was that the continuation or 'survival' of the botnet depended on a complex intermingling or inter-existence of both human and non-human components. The botnet could only be switched off once the botherder, the technological infrastructure and the individual computer infections were stopped. If only one or two elements were removed from the network, the botnet could continue to exist.

The main theoretical conclusion of this study was that ANT has an added value in relation to RAT and/or RC in three main ways. First, ANT is able to map a larger and broader number of actors involved in shaping the botnet and to demonstrate that the involved entities (including the botherder) only get strength and significance in relation to the other entities involved. Next, ANT was able to reveal how the offending, victimization and defending process can be intertwined. While RAT treats these elements as somewhat pre-existing and segregated, ANT treats them in a networked and more dynamic fashion. Finally, it was argued that ANT's understanding of agency enables us to capture the active role of technology in shaping the crime process and final outcome more profoundly than RAT and RC, which ultimately consider human agency as the main force behind criminal events. The general conclusion was that ANT's networked and hybrid conception of agency can expose certain (complex) elements and dynamics of the criminal process more

profoundly than a traditional approach. The first contours of the cyborg crime perspective were drawn in this study.

While this first case study focused on the nature of the crime, the automatic and robotic features of cybercrime in particular, the second and third case study sought to shed light on the (a)typical cyber offender. They focused on the hacker, a deviant figure that is known for his (or her) specific (malicious) engagement with technology. As mentioned in chapter 1, the first study (chapter 3) mainly looked at hacking from a more conventional criminological lens (labeling theory) and the second study (chapter 4) assessed the phenomenon through the ANT lens. By placing them in this particular order in the book, the added value of ANT could be presented more comprehensively.

6.2.2. The other 'others' (chapter 3)

This chapter started off by stating that hacking is 'the' textbook case of crime being a socially constructed phenomenon. While in the sixties hackers were the heroes of cyberspace, since the nineties they have increasingly been conceived as stereotypical cybercriminals. In current times, the image of the hacker as a criminal is also present, but there is (at least in the Netherlands) also more reconciliation to observe towards ethical hackers. This study aimed to shed light on how hackers themselves view these developments, hereby exploring whether they reject and/or internalize the imposed label. More specifically the study explored how different hackers feel perceived by society at large, how they perceive themselves as 'others' and how they view themselves in

relation to 'others'. Theoretically, the study explored whether the labeling approach has explanatory power for this group of 'digital others' and whether it is ready for a digital upgrade.

The research findings showed that hackers experience that the outside world views them as mysterious, nerdy and somewhat dangerous others, but above all as criminal others, a label that they reject to the full. Instead the hackers define their otherness in non-criminal terms. They view themselves as hobbyists with a specific interest in technology and they also view hacking itself in terms of creativity and art, out of the box thinking and a certain state of mind. In addition, the respondents (also the black hat hackers) view themselves as helpers rather than criminals. Even if they do an illicit hack; helping, educating and confronting the 'victimized' company with their poor security is considered as a good thing. The interviewed hackers also hold specific views regarding how they perceive themselves in relation to others, including criminals. They disassociate themselves from 'real' criminals regarding intent, modus operandi and responsibility and from other hackers in terms of intent and character. In other words, hackers seem to successfully reject the criminal (negative) label that is imposed on them. The study, in accordance with the study of Turgeman-Goldschmidt (2008), also found that hackers are able to avoid the internalization of this label. Rather than a negative self-image, they perceive themselves as positive others. They have no shortcomings but something extra of which they are proud.

This latter finding is obviously quite contradictive with the assumption of the labeling approach that negative labeling leads to a negative image of the self or even a spoiled identity. The study suggested different explanations for this result. The first explanation was found in the hacker phenomenon itself. Hacking requires a very distinct skillset, involves a specific mindset and morale and also seems to be the domain of an exclusive group of (online) others. How the outside world views hackers and what they (are able to do) might be not so important. Instead, the (sub)group they identify themselves with is much more significant in shaping their sense of the self. The fact that they are able to drift across the online and the offline world simultaneously might enable that they can manage two identities at the same time. The latter can also reduce the negative implications of labeling and also neutralizes their engagement with harmful activities. Apart from adding a digital dimension to labeling theory, it was argued that the theory could be enriched, by drawing more attention to inner-group types of labeling. In this context, Latour's (2005) concept of the 'anti-group' was considered to be relevant. Being different is not only a matter of associating with like-minded others, but also a process of dissociating themselves from other groups (in this case criminals and other hackers in the community).

6.2.3. The cyborgian deviant (chapter 4)

The starting point of this study was that hackers – whether they are engaged in licit or illicit forms of hacking – require an approach that places the human-technology relationship more in the forefront of the

analysis. Although existing studies also look at this relationship, they view it in a rather anthropocentric, dualistic and hierarchical manner. It was argued that ANT, which adopts a more post-human or cyborgian view of agency, might enable to obtain a more nuanced understanding of this relationship, and subsequently also of the hacker phenomenon. On the basis of ten hacker interviews with both hackers involved in licit and illicit hacking activities, the study explored how hackers give meaning to themselves and their actions and how this was co-shaped by their (deviant) relationship and engagement with technology.

The results showed that hackers (whether black, gray or white) view themselves as non-criminal actors who have a very specific skillset and mindset, setting them apart from ordinary people and criminals alike. First of all they view themselves as talented and creative figures that have an inborn fascination for objects and technologies and their inner workings. They are 'reversible blackboxers' and 'out of the box thinkers' at the same time. The respondents also considered themselves as heroic moral philosophers who have their own specific believes regarding what is wrong and what is right. (Existing) boundaries of all kinds are unnatural for them. They want to break them, extend them or set their own ones. In various ways, the respondents also believed to possess extra sensory abilities in the sense that they can do, see and accomplish things that 'normal' people cannot. In that sense, they see themselves as somewhat superhuman or cyborgian – their body and mind is extended. While hackers can be considered as an atypical or unique deviant group,

the study also found some resemblance with other deviant and non-deviant groups, including robbers, gravity artists, athletics and gamers.

The second main finding of this study was that the interviewed hackers view their relationship with technology everything but instrumental. They described this relationship as cooperative, interactive, competitive, intimate and/or explorative. For example, the respondents put forward that they do not consider hacking merely as a solo-human performance. Apart from learning from other hackers, they depend on existing tools alias 'weaponry' and modify them to their own desire. This latter is comparable with Latour's gun-human hybrid, illustrative for the notion that (the functionality of) technologies co-enable and/or co-shape performances, skills and intentions too.

Theoretically, the study concluded that ANT's cyborg perspective added a new layer to existing concepts (e.g. mastery, thrill seeking, fun) that seek to capture the hacker essence since it more specifically aims to grasp how the interaction and engagement with technology co-shapes how hackers perform, act, think, do malicious things and so on. The case study hereby built forth on the cyborg crime concept developed in the botnet study – where agency was considered as something hybrid. Yet, it added a more subjective and experiential dimension to the cyborg crime perspective, which could only be explored and unraveled by means of in-depth interviews.

The theoretical conclusion of this study was that ANT was able to reveal certain aspects more profoundly than existing approaches because it looks at the various hybrid capacities in which a hacker acts and does not isolate meaning giving from the tools and technologies they engage with. In this context, the added value also becomes visible in relation to the labeling approach that was used in chapter 3. Both studies focused on how hackers view themselves and construct their identity, also in relation to others. We could see that an ANT-based cyborgian approach could reveal certain aspects even more sharply. It revealed more thoroughly that the manner in which hackers give meaning to their 'otherness,' cannot be understood in isolation from how they give meaning to their (deviant) relationship with technology. Another conclusion that was drawn in this study was that ANT, like the broader notion of Haraway's (1987) cyborg concept, enables to approach the hacker phenomenon in a less dualistic manner. It enabled to reveal that hacking as a practice and a type of transgression involves a complex interplay of both boundary breaking and boundary fixing, technically and morally as well. The overall conclusion was that ANT's 'more than a human approach' has theoretical potential for the study of hacking and other types of technocrime.

6.2.4. The hybrid victim (chapter 5)

After conducting different case studies on high-tech offenders, it seemed to be worthwhile exploring whether ANT could be a valuable lens for the study of the victim too. Therefore the last case study examined the process of becoming a high-tech cybervictim. This study was more

theoretical in content than the previous studies and it was also structured differently. It adopted a problem-driven approach by taking three empirical cases of cyber victimization (ransomware, botnets and high-tech virtual theft) as the point of departure. By describing these empirical cases and the features that can be abstracted from them, the study sought to expose the limitations and blind spots of existing theories in a more empirically grounded manner. It revealed that existing theories commonly used to explain cyber victimization, the lifestyle routine activity approach in particular, are too anthropocentric, reductionist and dualistic in nature for the analysis of the three cases. For instance, they view vulnerability as a single property, while the cases showed that vulnerability cannot be assigned to a single point actor. Victims are, e.g., partly targeted and victimized through the vulnerability of others (e.g. vulnerable websites) and thus have to be targeted technically first, before any 'human' vulnerability can be exploited. Hence, the human and technical vulnerability cannot be separated. The cases also showed that existing dualisms such as the human versus the non-human, the actual versus the fictional and the offender versus the victim are no longer productive in grasping both the victim as an entity and as a process. Accordingly, the study explored the theoretical potential of ANT in relation to the cases and whether and how ANT could counter some of the conceptual limitations of existing victim concepts.

The study eventually resulted in three alternative ANT-based victim concepts, denoted as 'hybrid victim theory'. The concept of *victim composition* resembles the notion that the (vulnerable) victim should be

viewed as a hybrid and distributed network that consists of human, technical and/or virtual entities that has to be targeted by the offender. In such view, vulnerability is treated in a distributed and emergent way and not considered as a property that can be assigned to a single point actor – whether it is a technical system or a person. The concept of *victim delegation* enables to assess how tasks and roles in the victimization process are distributed over time. The concept of *victim translation* enables to view victimization as a transformative, interactional and fluid process instead of a concrete event. It views the victimization as the result of a complex interaction between various programs of actions and anti-programs. All three concepts underscore the leaky boundaries between the offender, victim and defender, between human and machine, between tool and target and between the actual and the fictional. The study concluded that these concepts offer new leads for the analysis of high-tech crime victimization, but also invite to think differently about key issues and concepts in victim studies, including who/what makes victims vulnerable and resilient and how we can think about prevention strategies.

6.3. Arrival: The ANT-based cyborg crime perspective

As the findings from the case studies reveal, ANT has a different value for different research questions, themes and empirical contexts. Hence it would not make sense to "attempt to draw the findings of various studies together into an overarching explanatory framework" (Mol, 2010: 261). Yet, based on the different case studies that have been conducted in the

scope of this dissertation, I do think it is possible to highlight the main focal points of the ANT lens that are particularly valuable for the criminological analysis of high-tech crime. In this context I distinguish four main key dimensions, which I denote as the 'cyborg crime perspective':

1. Technologies should be treated as active entities, mediators or participants in high-tech crime offending;
2. The high-tech cyber offender-technology relationship is more than (just) functional;
3. High-tech cybercrime offenders are interacting with technologies, which they might not fully control;
4. High-tech cybercrime offending and victimization are hybrid products of human, technical and/or virtual (inter)actions.

In the following I will elaborate on these dimensions more extensively and discuss how they can have an added value for the criminological study of cybercrime. Important to stress is that they are complementary and not mutually exclusive.

Dimension 1: Technologies should be treated as active entities, mediators or participants in high-tech crime offending

The first dimension of the cyborg crime perspective concerns the view that we should look at objects or technologies in an active rather than a passive and neutral way. Their script prescribes a certain usage and can

invite a concrete type of behavior (e.g. a weapon invites shooting), resulting in a 'translated program of action' where human intentions and non-human functionalities become one. It can be argued that in the cyber domain - where deviant (human) actors continuously interact with technology (whether it concerns the writing of a malicious program, the control of a botnet or the launching of a DDoS attack) - such dimension can be valuable to shed light on the manner in which (potential) offenders gain access to and interact with the tools that they 'use.' As it was revealed in chapter 4, also hackers themselves do not consider the tools that they employ as passive and neutral. Hence, the cyborg crime perspective draws more explicit attention to the mutual interaction between (deviant) 'human' skills and intentions and the scripts[52] of the objects. It takes into consideration how particular technologies mediate in how and why certain crimes are carried out and it also looks at how technologies affect the moral decision-making of offenders.

Dimension 2: The high-tech cyber offender-technology relationship is more than (just) functional

The second dimension of the cyborg crime perspective involves the notion that the relationship between (deviant) humans and non-humans should be conceived as more multifaceted than just a 'user relationship'. The human-technology relationship might appear in various other, more non-functional ways as well, including a cooperative, competitive or

[52] See also the study of Silvast & Reunanen (2014) who use the script concept in the context of hacking.

intimate relationship. It can be argued that this second dimension can be particularly valuable for the understanding of deviant groups and practices in which the interaction with technology is on the foreground. Hacking is of course the most obvious example, yet the approach could be valuable for other forms of (high-tech) deviant behavior as well such as DDoS attacks. Perhaps different forms of cybercrime come along with different types of human-technology relationships (ranging from a more close relationship to a 'click and see what happens relationship'). In any case, the hybrid lens of the cyborg crime perspective keeps an eye open for a broader spectrum of human-technology relationship than a traditional criminological approach.

Dimension 3: High-tech cybercrime offenders are interacting with technologies, which they might not be able to fully control

The third dimension of the cyborg crime perspective concerns the notion that offenders might be interacting with objects and technologies that they might not be able to fully control. In the footsteps of ANT, the cyborg crime perspective presumes that offenders might not always be able to predict in advance what an object or technology may do, cause or disturb. This makes technologies not only more than instruments, but also not fully predictable and controllable. It can be argued that this aspect counts even stronger for digital objects and technologies than the objects Latour was actually referring to (e.g. an automated door). As Lehman *et al* (2018: 5) point out, when it comes to computer programs, "the outcome

cannot be predicted without actually running it."[53] This could also count for malicious programs. The script of certain tools might be quite fixed, e.g. the script of a DDoS tool will most likely be: "send a lot of traffic to a server in order to paralyze it." Yet, how much damage will be done is not predictable[54]. This definitely also counts for the spread of malware (see Skoudis & Zeltser, 2004). By assigning a more active role to technology and by treating them as mediators, we might be able to unravel certain crime dynamics in the digital world more profoundly, including the coincidences, transformations and translations that unfold in the course of criminal events. These might stay 'blackboxed' if we would consider technology as a passive and mundane entity and consider the human actor as the only agent (see also the fourth dimension). As Balzacq and Dun Cavelty (2016) point out in their ANT-based study of malware infections: Viewing malware as a mediator or actor "allows us to give malware transformative agency of its own, detached from the 'intent' of the person who wrote the code" (p. 183).[55] Especially in the cyber domain, technical entities cannot only play an active role, they can

[53] The authors provide in this context an overview of examples in which computer programs produced unanticipated (strange, surprising or creative) results. According to them digital or artificial organisms (like biological ones) can subvert human expectations and intentions. Usually we do not hear much about these occurrences since they are considered as 'errors' and therefore, as ANT would put it, are blackboxed.

[54] This was also an issue in the recent 'Wannacry' ransomware attacks (2017), which started most likely rather amateur, but had devastating consequences. See for a discussion on the matter:
https://www.vrt.be/vrtnws/nl/2017/05/16/_amper_65_000_dollarvergaardwaaromdecyberaanvaleenamateuristisch-1-2980227/)

[55] This quote again stipulates the fact that different actors carry out specific elements of the crime, while the first actor in the chain might not have any association with the latter one (Van der Wagen & Dimitrova, 2018).

eventually also lead a 'life' on their own, establishing new relationships with other human and technical entities. This clearly comes together with the first dimension, which stresses that technologies should be analyzed as (potential) actors or active participants in crime.

Dimension 4: High-tech offending and victimization are hybrid products of human, technical and/or virtual (inter) action

The fourth dimension of the cyborg crime perspective underscores that actions and outcomes, including criminal ones, should be studied in a more relational, networked and non-dualistic manner. Strongly connected with the previous point, it proclaims that we should not a priori assign all the credits to the human agent when analyzing (criminal or deviant) actions and their results, but to look at the composition of actors that carry it out and/or co-shape the event, process or situation. The underlying reason is that something might look like a single point actor (e.g. 'a botnet' or 'a victim') but when you look closer you see a network of multiple actors comprising the (blackboxed) actor. The cyborg crime perspective therefore views high-tech cybercrime as a hybrid product of (a network of) human, non-human and/or virtual (inter) action. As we have seen in chapter 5, which particularly explored ANT for the study of the high-tech cybervictim, this dimension also appeared to be valuable in the context of victimization. From the cyborg crime perspective, vulnerability is not (a priori) assigned to a single entity or actor, but attributed to an emergent network of multiple entities or actors: human, technical and/or virtual. In such a network it

is also blurry whether the entities are tools, instruments, humans, machines, guardians, offending or victimized entities.

6.4. Critical reflection on the results

Based on the four dimensions presented here, one might ask the question whether the empirical research was actually essential to come to the same results. Given that the empirical material was not substantial in terms of number of studied cases or respondents, this is a legitimate question to ask. One could even argue that ANT's theoretical potential can be assessed without doing any empirical research at all. I however consider the conducted empirical work in this dissertation essential for two main interconnected reasons. The first reason is that the empirical material served for achieving theoretical acuity and nuance. By merely assessing the potential value of ANT on the theoretical level, we can still not assess its utility and analytical abilities for the study of empirical material. By looking at specific (and different) cases through the ANT lens, it is e.g. possible to explore how a 'thing' can act as a mediator and why it actually matters. As mentioned in chapter 1 as well, case studies (particularly exemplary cases) enable to understand the limits of the theory and perhaps also discover new actors or dynamics for which the theory could be valuable. In chapter 4 for example, it turned out that ANT's hybrid view was also suitable for shedding light on how actors view themselves as hybrids or cyborgs. The hackers believed to have an extended body and mind.

The second reason why I consider the inclusion of the empirical material very essential is that it enabled to concretely compare the theoretical potential of ANT in relation to the potential of existing theories and concepts. As Mähring, Holmström and Monteolegre (2004), who used ANT in combination with escalation theory, also argue: applying different theoretical perspectives on a single case enables to "better understand the distinctive strengths of the perspectives involved" (p. 216). The latter, this dissertation also was able to illustrate by studying the hacker phenomenon through both a conventional (chapter 3) and the ANT lens (chapter 4). Which layer does ANT add and does such layer result in novel insights into that particular phenomenon? Moreover, such comparative approach makes you as a researcher also more critical and skeptical towards the application of ANT itself.

In the following I will look more closely at ANT's view of non-agency and the extent to which the cyborg crime perspective follows into its footsteps.

6.5. Taking a closer look at the agency of 'things'

As the four dimensions outlined above reveal, ANT's often-debated conceptualization of the agency of things is quite a central cornerstone within the cyborg crime perspective. Assigning agency to non-humans or technology inevitably raises the question how the ANT-based cyborg crime perspective views 'non-human agency' in relation to 'human

agency.' Does it place non-human agency on the same (ontological) footing as human agency, like ANT does? Yes it does, but this needs some clarification and nuance.

Important to stress (once more) that ANT does not give strict criteria of when an entity can be considered as an actor, at least the essence of the involved entity (being human or non-human) is not a criterion for considering an entity as an actor. It is also case dependent: "Every time a new case is considered it suggests different lessons about what "an actor" might be" (Mol, 2010: 257). For ANT someone or something can be 'labeled' as an actor when the entity makes a difference, changes a certain state of affairs or brings some surprises or disturbances. Whether an entity is human or non-human is not relevant from an analytical point of view, since it leads to the same changes or outcomes. ANT therefore considers agency (like anything else) as something relational and distributed as well. For Latour "no entity can be something 'in itself'. Only in relation to other entities can they become meaningful and relevant: only networks turn entities into actors" (Verbeek, 2014: 79). The follow up question is then how this understanding of agency relates to issues such as intentionality and morality. Does this view of agency make 'things' also moral beings?

Although ANT and the cyborg crime perspective alike, flatten the difference between humans and non-human actorship in analytical terms, as outlined above, it does however not argue that humans and non-humans are essentially and morally exactly the same. For instance it

is not argued that objects have a will on their own or have an intentionality or consciousness in the same manner that humans have. Things do not act by themselves (at least not yet), but might act differently than expected – which is why they have the ability to operate as actors (or mediators) in certain situations (see also Latour & Venn, 2002). At the same time, ANT argues that morality is not merely a 'human affair' either, since we cannot make a strict divide between human ends and technical means in the course of actions. It is the 'gun-human' hybrid that kills and not merely the human actor. In other words, ANT and other mediation approaches alike do not approach the issue of morality and intentionality from a "dualist paradigm that locates human beings and technological artefacts in two separate realms, humans being intentional and free, technologies being instrumental and mute" (Verbeek, 2014 : 75).

While ANT acknowledges the distinctiveness of human and non-human essence, it is not a focal point. It is exactly this aspect that is a source for misunderstanding and criticism alike. Indeed, the minor conceptual attention for 'the human' role in moral decision-making could be considered as a conceptual blind spot or 'black box' within ANT. As Krarup and Blok (2011) point out, Latour recognizes that morality is not solely constituted by the tools or objects alone, yet he has little to say about the human or subjective dimension that co-shapes moral decisions. These authors therefore argue that Latour's view is not symmetrical enough. The counterargument that can be given is that the added value of ANT lies exactly in its attention for the active and even

person-transformative abilities of non-humans. It fills an important blind spot of (most) approaches (also in criminology) that are located at the other (human-focused) extreme. Placing too much emphasis on the agency of non-humans on the other hand, might run the risk of applying a too strong sense of symmetry or head to other extreme. In any case, it is quite a challenge "to produce accounts that are robust enough to negate the twin charges of symmetrical absence and symmetrical absurdity" (McLean & Hassard, 2004: 494).

A related issue to address is whether the flattening of human and non-human agency and their collision (in the course of action), as proposed by ANT and the cyborg crime perspective, can go hand in hand with a more differentiated vision or conceptualization of agency at the same time. In this respect I agree with Kipnis (2015) and Verbeek (2014), who argue that we should not forget what is typical and unique about human agency, but also further assess what is typical about technological agency. For example, with regard to the latter, this dissertation revealed that technology has the ability to change the course of action, to produce unanticipated results in criminal events and to set in motion various new types of (deviant) interactions. To specifically understand the various ways in which the agency of technology can manifest itself in a crime setting or how technology can affect moral decision-making is a very essential issue for criminologists to consider in the scope of cyber-related research. Of course, a differentiated view might look like a return to a dualistic approach, which Latour specifically seeks to avoid. Yet, I

think that distinction and non-separation of human and non-human agency in the course of (inter)action can go hand in hand.

6.6. Possible legal and practical implications

Obviously, the flattening of human and non-human agency also brings up some legal and practical concerns. For instance, how does a hybrid view of agency, as proposed by the cyborg crime perspective affect the way we think about causality, responsibility and guilt? Should we increasingly criminalize the tools themselves?

Verbeek (2014) provides a clear answer to this question. He argues that a hybrid approach, as proposed by ANT and other philosophers of technology who adhere to a mediation approach, does not "reduce human morality, but adds to it; it shows dimensions that normally remain underexposed. Conceptualizing the moral significance of things does not undermine human responsibility by blaming cars for accidents but rather expands the ways in which we can design, implement, and use technologies in responsible ways " (p. 80).

Indeed, the cyborg crime perspective does not suggest that we should blame a computer virus for the damage that it causes. Even when a person intends to create a small rather innocent virus - but this virus eventually causes tremendous damage - he or she will most likely be held

accountable for this unforeseen damage as well.[56] Yet, what if the person did not create the tool him or herself, but bought the tool or just pushed some button and was not aware of the damage it could cause? And is it always possible with high-tech cybercrime to exactly determine who/what caused the damage (and which damage) and to map the chain of actors and actions that led to the eventual outcome? These are the issues the cyborg crime perspective wants to place more central. How the features and dynamics of high-tech cybercrime exactly challenge existing legal concepts and theories, e.g. those used in the scope of determining causality, has not been explored in this research, but would be definitely worth examining.

Another issue to consider in this context is related to future developments, particularly in relation to the rapid technological innovations in the field of robotics and artificial intelligence. It is actually not unthinkable that the agency of technology eventually becomes more 'human-like' (see e.g. Bostrom, 2014). Although it is not quite sure yet whether we will end up in a matrix-like world, where machines outsmart the human race, criminologists and legal scholars should not wait much longer with assessing and conceptualizing the nature, scope and boundaries of technical agency in a crime setting and also look ahead. Perhaps someday even the 'trans-human' deviant or criminal might appear on stage, demanding to expand the theoretical and legal frontiers even further.

[56] See, e.g., Kwakman (2007) on this matter.

Apart from possible legal implications, it is also worth considering whether the cyborg crime perspective has some practical implications. Let me briefly consider two implications for crime control and prevention deriving from the cyborg crime perspective.

Firstly, since the cyborg crime perspective stresses the mediating role of objects, tools, infrastructures and technologies in high-tech cybercrime, it would opt for an approach that takes this particular dimension into account when tackling cybercrime. The cyborg crime perspective would then imply a shift from an offender-oriented approach to a focus on those (other) entities that play an active or mediating role in generating the crime[57]. This could also be non-human actors. For example, offenders strongly rely on the infrastructures that they use in high-tech cybercrime. Those infrastructures are also crucial generators of the harm that is (eventually) inflicted. Measures targeting these infrastructures could then be effective for counteracting these crimes and could prevent or reduce further harm. Dupont (2017), in this context, highlights the essential role that Internet Service Providers could play. Since these actors can monitor Internet traffic and suspicious data flows, they can e.g. block or disturb the communication channels between botmasters and the infected computers.

[57] In this respect there is clear parallel to draw with a situational crime prevention, which also focuses on many more actors than the offender (see also Hutchings & Holt, 2017).

Furthermore, law enforcement agencies could make efforts in regard to limiting access to malicious tools. Law enforcement agencies could e.g. disturb or even target the market places where malicious tools, exploits, malware, etcetera are sold. This is a measure that has actually proven to be successful already.[58] Law enforcement agencies could also make efforts in relation to making tools or malware less effective. They could, e.g., actively exchange malware samples with security companies in order to develop anti-measures (anti-programs) already before new types of malware appear on the market (Van der Wagen & Dimitrova, 2018). In this respect, law enforcement agencies would become more closely involved in the arms race between malware writers and the security industry (see Iliopoulos, Szor & Adami, 2011). Perhaps, reasoning from the cyborg crime perspective, this is inevitable in light of the fact that various high-tech cybercrimes are not merely carried out by humans nor by machines, but by hybrid networks of both. This brings us to the second point.

Secondly, as it was outlined in chapter 2 and 5 already, counteracting cyborg crime also requires the formation of a hybrid network of different actors. No single actor can counteract cybercrime alone, but only a collective of various actors, public and private, human and non-human can form a powerful coalition that is truly prepared for combat. Of course, public-private cooperation in the scope of cybercrime is already

[58] In April (2018) the Dutch Police shut down one of the largest suppliers of tools that enable DDoS attacks, see e.g. https://www.businessinsider.nl/nederlandse-politie-ddos-webstresser/

a common practice. It is a strategy that is used in tackling various forms of crime (see e.g. Schuilenburg, 2015). The cyborg crime perspective could further nurture, co-shape and analyze such initiatives, e.g. by assessing how the interests, recourses and tools of the various actors can be (effectively) brought together in a network.

6.7. Opportunities and possible pitfalls of travelling with ANT

"With ANT you may go out and walk new roads. But beware: as you walk nobody will hold your hands, there are no assurances" (Mol, 2010: 261)

As became clear throughout this dissertation, ANT does not offer a strictly defined conceptual framework. It suggests directions rather than providing a detailed road map, which is why the theoretical journey undertaken in this dissertation was truly an exploration. There are of course certain ANT key dimensions that help you to navigate through the 'more than a human universe', as discussed extensively throughout this dissertation. Furthermore, as outlined in chapter 1, when you decide to take the ANT route: you should not stay on the usual tracks, take the small roads and also meet with the locals and make some report of their vision in your travel book.

Whether one agrees with the assumptions of ANT or not, it can be argued that a provocative perspective like ANT can be valuable in the scope of theoretical innovation in any case. ANT challenges not only to critically

look at existing (taken for granted) concepts, but also to ask new, less familiar and less obvious questions. As Kleemans, Weerman and Enhus (2007: 239) also claim: "Without asking the right questions about a certain phenomenon, the answers will always stay on the beaten track and the result will not produce much 'newness,' no matter how advanced the methods and how extensive the datasets are." It can be argued that the latter applies to most positivistic-orientated criminological research in the field of cybercrime, which is dominated by the routine-activity theory. What can be added here is that criminologists should also not restrict or limit themselves by only formulating questions that are (directly) relevant for policy (Staring & Van Swaaningen, 2016). Yet, this does not exclude the option that a theory-oriented research eventually might actually lead to new policy-related questions and research as well.[59]

The ANT-based 'cyborg crime' concept or perspective presented in this dissertation can therefore be considered as an attempt to break with the tendency to prioritize data (and policy) over theory and to develop and to explore new theoretical concepts. This dissertation could therefore inspire criminologists to consider and explore ANT and other

[59] In the aftermath of my PhD research I conducted together with criminologist Eli Dimitrova an additional research project named "Mission Cyborg: Towards a hybrid understanding of (counteracting) cybercriminal (actor-) networks", which was commissioned by the Team High Tech Crime of the Dutch National Police. In the research we explored, by analyzing private chat conversations, how cybercriminal (actor)-networks carry out high-tech crimes and organize themselves. The findings also served for providing new leads for interventions against these networks, including interventions specifically directed toward non-human or technical entities (see also section 6.6).

perspectives in the field of philosophy of technology. Although these perspectives are not preoccupied with the analysis of crime and deviant behavior nor do they focus on the cyber domain, they definitely offer valuable insights and concepts for the criminological theorization of the relationship between the human and the technical and provide leads to treat technology as mediators or agents. ANT in particular, provides also the means to dismantle the binary frameworks we (criminologists) are still burdened with.

Of course, there are also some critical questions or issues to address when it comes to engaging with ANT. The first question that can be asked is: does ANT truly bring you at different places that cannot be reached by travelling conventionally? In correspondence with what I outlined earlier in this chapter and throughout the case studies, I think that this dissertation has shown that ANT is definitely able to explore new paths, to add a new dimension to existing views or concepts and/or to put things into a different perspective. In particular its hybrid and symmetrical view of agency is considered valuable, since it enables to look at both the role of humans and non-humans in shaping deviant actions, (moral) decision-making and behavior. However, this does not entail that I consider ANT as a 'theory of everything' that can replace a large part of the existing theoretical repertoire of criminology. As chapter 4 clearly demonstrates, in order to shed light on the processes of labeling for example, labeling theory is still (also in the digital age) a very valuable approach to use. As I mentioned before, ANT concepts are also not preoccupied with understanding human nature and (deviant)

behavior, which is why various criminological concepts still matter, no matter how technical the crime is. Instead, I consider ANT (and the ensuing cyborg crime perspective) much more as a lens that is particularly suitable for shedding light on certain dimensions that are crucial in grasping high-tech crime offending and victimization, as outlined in section 6.3. It is complementary, enriching and likes to do some twisting as well. It also seeks to make interactions, relations and dynamics visible that are 'blackboxed' by existing, mainly positivist approaches.

A second question worth considering is whether it is realistic and desirable to fully follow ANT's tenets. Should we go 'all in'? In my believe to remain completely loyal to all of the valuable points ANT offers, is somewhat doubtful and perhaps even impossible. More specifically, I have some reservations concerning Latour's radical descriptivism, the shift from "theoretically interpreting human actions to obstinately 'following the actor' by tracking and mapping its multiple associations" (Krarup & Blok, 2011: 43). Describing phenomena in all their richness rather than seeking to capture them in large vague concepts, I also do appreciate. However, it can be debated whether ANT's claim to 'merely describe' is actually realizable since we are never able to observe (and thus to describe) the whole chain of associations that explain certain events or certain behavior. Our findings (or descriptions) are for example often shaped by some common sense explanations, which can also be found in Latour's own work (see Krarup & Blok, 2011).

Apart from the question whether mere description is possible, it is also questionable whether it is 'better' than doing some interpretation of what the actors are saying, to develop concepts and examine relationships between those concepts. It can be argued that the latter can actually result in a more nuanced understanding of phenomena, without necessarily losing the richness of the data. When we would merely describe, our research findings might also become somewhat loose as if they speak for themselves (Staring & Van Swaaningen, 2016). Matza (1969) brings up a rather different issue or tension when it comes to the descriptive practices of the criminologist. He argues, something Latour would most likely also agree upon, that in our study of deviant behavior we "have to stay committed "*to phenomena and their nature;* not to Science or any system of standards" (p.3). Yet, Matza also warns: "To take viewpoints at their [the deviant's] word may be misleading. We may be deceived into equating an idle and thus meaningless verbal affirmation with an abiding commitment [to naturalism]". In other words, the researcher cannot escape and perhaps should not escape completely from interpretative practices and should not take everything for granted what the actors are saying. In this respect I agree with Krarup and Blok (2011: 49) who argue that there is "neither pure explanation nor pure description, only various 'hybrids' in between."

The last question I would shortly like to consider is whether the ANT route can also lead to dead ends. In line with what was argued before, I think that an engagement with ANT can be a fruitful exercise in any case since it can offer new research directions and give a new impulse to

existing debates. Rather than dead ends, the researcher might get lost from time to time, at least speaking from my own experience. When engaging with ANT, staying close to the empirical world, is highly recommended for staying on the right track.

6.8. The journey continues: future research directions

With this dissertation, the journey has certainly not ended yet. As I put forward in the case studies, there is still more research to be done. Let me highlight a few options.

First of all, the cyborg crime perspective, as presented in this dissertation, could be further explored and enhanced, e.g. by conducting additional case studies and/or by applying it on a larger dataset. A larger number of in depth interviews with hackers would for example be able to validate some of the findings presented here and also to produce additional findings. Apart from more data, future research into the hacker phenomenon could draw more explicit attention to hacking as a practice, unraveling not only what hackers are thinking, but also producing a detailed account of what they are actually *doing* and to ideally follow them during that practice. In this context we can draw a curious parallel between the world of hackers and the world of social scientists, through the eyes of Latour and Woolgar (1986). Both hackers and social scientists like to portray their highly specialized world as a world apart and also play a role in maintaining that same mystique. More research in the internal workings of hacking as an activity could enhance

our criminological understanding of hacking as a practice and also enable us to more deeply penetrate this (still) somewhat mysterious world.

Second, the cyborg crime perspective could be used to conduct more research (e.g. interviews) on how victims become and experience high-tech cyber victimization. To what extent are victims aware of certain risks and how do they perceive their own risk of becoming a victim? Does being hacked generate the same feeling as a home burglary? How do victims experience a ransomware attack, having no access (perhaps never again) to all their files and photo's they are so attached to? The cyborg crime perspective could be also particularly suitable for research into virtual types of victimization such as cyber rape since it focuses on how the 'hybrid self' experiences harm.

Last, the cyborg crime perspective could be relevant to consider in the context of other cyber-related themes. An example is research into the role of bots and botnets in the spread of (fake) news. In the context of the Brexit and the American election campaigns for instance, bots (e.g. robotic twitter users) played a considerable role in shaping public opinion (see e.g. Kollanyi, Howard & Woolley, 2016). They were spreading tweets on a rapid scale, which were often retweeted by real human users and so on. From the cyborg crime perspective such a phenomenon would be interesting to analyze since it is no longer possible to separate human from non-human entities in the construction of knowledge and truth. Developments such as these at the same time stipulate an important point I would like to stress and conclude with:

ANT's pre-digital ideas concur very well, perhaps even better with the current digitalized world. That is why I predict that ANT and cybercriminology could be long lasting travel partners.

References

- Agee, J. (2009). Developing qualitative research questions: a reflective process. *International Journal of Qualitative Studies in Education*, *22*(4), 431-447.
- Akrich, M. (1992). The De-scription of Technological Objects. In W.E. Bijker & J. Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change* (pp. 205-224). Cambridge, MA: MIT Press.
- Akrich, M. & Latour, B. (1992). A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies. In W.E. Bijker & J. Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change* (pp. 259-264). Cambridge, MA: MIT Press.
- Balzacq, T. & Dunn Cavelty, M.D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176-198.
- Bauman, Z. (2000), *Liquid Modernity*. Cambridge: Polity.
- Baxter, P. & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The qualitative Report*, *13*(4), 544-559.
- Becker, H.S. (1963). *Outsiders. Studies in the Sociology of Deviance*. New York: The Free Press.
- Benschop, A. (2013). *Cyberoorlog. Slagveld Internet.* Utrecht: Ef & Ef Media.

- Bilge, L., Balzarotti, D. Robertson, W. K., Kirda, E. & Kruegel, C. (2012). Disclosure: detecting botnet command and control servers through large-scale netflow analysis. In *ACSAC* (pp. 129-138). ACM.
- Blankwater, E. (2011). *Hacking the field. An ethnographic and historical study of the Dutch hacker field*. Sociology Master's Thesis. University of Amsterdam.
- Blok, A. & Jensen, T.E. (2011). *Bruno Latour. Hybrid thoughts in a hybrid world.* London/New York: Routledge.
- Blumer, H. (1954). What is Wrong with Social Theory? *American Sociological Review, 19*(1), 3-10.
- Bossler, A.M. & Holt, T.J. (2009). On-Line Activities, Guardianship and Malware Infection: An examination of Routine Activity Theory. *International Journal of Cyber Criminology, 3*(1), 400-420.
- Bossler, A.M. & Holt, T.J. (2011). Malware Victimization: a Routine Activities Framework. In K. Jaishanker (Ed.), *Cybercriminology: Exploring Internet Crime and Criminal Behaviors* (pp. 317-346). CRC Press.
- Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies.* Oxford University Press.
- Bourne, M. (2012). Guns don't kill people, cyborgs do: a Latourian provocation for transformatory arms control and disarmament. *Global Change, Peace & Security*, *24*(1), 141-163.
- Brenner, S.W. (2002). Organized cybercrime. How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology, 4*(1), 1-50.

- Brenner, S. (2007). *Law in an Era of Smart Technology*. Oxford: Oxford University Press.
- Brown, S. (2006). The Criminology of Hybrids. Rethinking Crime and Law in Technosocial Networks. *Theoretical Criminology*, *1*(4), 223-244.
- Burden, K., & Palmer, C. (2003). Cyber crime - a new breed of criminal? *Computer Law and Security Report, 19*(2), 222–227.
- Cairncross, F. (2001). *The Death of Distance. How the Communications Revolution is Changing our Lives.* Boston: Harvard Business School Press.
- Callon, M. (1986). The sociology of an actor-network: The case of the electric vehicle. In M. Callon, J. Law & A. Rip (Eds.), *Mapping the dynamics of science and technology* (pp. 19-34). Basingstoke, UK: Macmillan Press.
- Callon, M. (1999). Actor-Network Theory – the market test. *The Sociological Review*, 47(1), 181-195.
- Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social and Legal Studies, 10*(2), 229-242.
- Casey, E. (2011). *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet.* San Diego/London: Elsevier Inc.
- Castells, M. (2001). *The Internet Galaxy: Reflections on the internet, business, and society*. Oxford: Oxford University Press.
- Castells, M. (2009). *Communication Power*. New York: Oxford University Press.

- Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis.* London: Sage Publications.
- Chandler, A. (1996). The Changing Definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24*(2), 229-251.
- Choo, K-K.R. (2008). Organized crime groups in cyberspace: a typology. *Trends in Organized Crime*, *11*, 270-295.
- Churchill, D. (2016). Security and Visions of the Criminal: Technology, Professional Criminality and Social Change in Victorian and Edwardian Britain. *British Journal of Criminology, 56*(5), 857-876.
- Clarke, R.V. & Cornish, D.B. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Springer-Verlag.
- Clynes, M.E., & Kline N.S. (1960). Cyborgs and Space. *Astronautics, 5*(9), 26-27.
- Cohen, L.E. & Felson, M. (1979). Social Change and Crime Rates Trends: A Routine Activity Approach, *American Sociological Review*, *44*(4), 588-608.
- Cole, A., Mellor, M. & Noyes, D. (2007). Botnets: The rise of the machines. In Proceedings on the 6th Annual Security Conference (pp. 1-14).
- Consoli, L. & Hoekstra, R. (2008). Inleiding. In I.L. Consolie & R. Hoekstra (Eds.), *Annalen van het Thijmgenootschap* (pp. 7-13). Nijmegen: Valkhof Pers.
- Cross, C. (2013). "Nobody's holding a gun to your head." Examining current discourses surrounding victims of online

fraud. In K. Richards & J. Tauri (Eds.), *Crime, Justice and Social Democracry: Proceedings of the 2nd International Conference* (pp. 25-32). Brisbane: Queensland University of Technology.

- Dant, T. (2004). The Driver-car. *Theory, Culture & Society*, *21*(4/5), 61-79.
- Deibert, R. & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *Papers from the British Criminology Conference*, *8*, 3-17.
- De Graaf, D., Shosha, A.F. & Gladyshev, P. (2013). Bredolab: shopping in the cybercrime underworld.' In M. Rogers & K.C. Seigfried-Spellar (Eds.), *Digital Forensics and Cybercrime* (pp. 302-313). 4th International Conference, ICDF2C 2012. Springer, available online at http://ulir.ul.ie/handle/10344/2896.
- Demant, J. & Dilkes Frayne, E. (2015). Situational Crime Prevention in Nightlife Spaces. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime studies. Explorations in Science and Technology* (pp. 5-19). London/New York: Ashgate.
- De Mul, J. (2002). *Cyberspace Odysee*. Kampen: Klement.
- De Laet, M. & Mol, A. (2000). The Zimbabwe Bush Pump: Mechanics of a Fluid Technology, *Social Studies of Science, 30*(2), 225–263.
- Deleuze, G. & Guatarri, F. (1987). *A Thousand Plateaus: Capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.
- Deseriis, M. (2017). Hacktivism: On the Use of Botnets in Cyberattacks. *Theory, Culture & Society*, *34*(4), 131-152.

- Dolwick, J.S. (2009). 'The Social' and Beyond: Introducing Actor-Network Theory. *J Mart Arch*, 4, 21-49.
- Douillet, A-C & Dumouline, L. (2015). Actor Network Theory and CCTV Development. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime studies. Explorations in Science and Technology* (pp. 21-35). London/New York: Ashgate.
- Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime Law & Social Change, 67*, 97-116.
- Feenan, D. (2002), Legal Issues in Acquiring Information about Illegal Behaviour Through Criminological Research. *British Journal of Criminology*, *42*(4), 762–81.
- Ferrell, J. (1996). *Crimes of Style: Urban Graffiti and the Politics of Criminality*. Boston: North-eastern University Press.
- Ferrell, J. (1997). Criminological Verstehen: Inside the immediacy of crime. *Justice Quarterly, 14*(1), 3-23.
- Finch, E. (2001), Issues of Confidentiality in Research into Criminal Activity: the Legal and Ethical Dilemma. *Mountbatten Journal of Legal Studies*, *1*(2), 34–50.
- Flyvbjerg, B. (2013). Case Study. In N.K. Denzin & Y.S. Lincoln (Eds.), *Strategies of Qualitative Inquiry* (pp. 169-203). Thousand Oaks: Sage.
- Forlano, L. & Jungnickel, K. (2015). Hacking Binaries/Hacking Hybrids: Understanding the Black/White Binary as a Socio-technical Practice. *Ada: A Journal of Gender, New Media and*

Technology, 6, available online at http://adanewmedia.org/2015/01/issue6-forlano-jungnickel/.

- Franko Aas, K. (2006). 'The body does not lie': Identity, risk and trust in technoculture. *Crime Media Culture*, *2*(2), 143-158.
- Franko Aas, K. (2007). Beyond 'The Desert of The Real': Crime Control in a Virtual(ised) Reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160-178). Collumpton: Willan Publishing.
- Franko Aas, K. (2010). Beyond 'The desert of the Real': Crime Control in a Virtual(sed) reality. In C. Greer (Ed.), *Crime and Media. A reader* (pp. 551-564). London/New York: Routledge.
- Franko Aas, K. (2015). Preface. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime studies. Explorations in Science and Technology* (pp. 9-13). London/New York: Ashgate.
- Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. London: Addison-Wesley.
- Gad, C. & Jensen, C.B. (2010). On the Consequences of Post-ANT. *Science, Technology & Human Values*, *35*(1), 55-80.
- Gaggi, S (2003). The Cyborg and the Net: Figures of the Technological Subject. *Bucknell Review: A Scholarly Journal of Letters, Arts and Sciences*, *46*(2), 125-139.
- Garfinkel, H. (1967). *Studies in Ethnomethodology*. Englewood Cliffs, NJ: Prentice-Hall Inc.
- Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in Computer Virology*, *6*(1), 77-90.
- Geertsema, H.G. (2006). Cyborg: Myth or Reality? *Zygon, 41*(2), 289-327.

- George, A.L, & Bennett, A. (2005). *Case studies and theory development in the social sciences*. Cambridge, MA: MIT Press.
- Gerring, J. (2004). What is a case study and what is it good for? *The American Political Science Review*, *98*(2), 341-354.
- Giese, L. (2008). How material are cyberbodies? Broadband Internet and embodied subjectivity. *Crime Media Culture*, *4*(3), 311-330.
- Glaser, B.G. & Strauss, A.L. (1967). *The discovery of Grounded Theory: strategies for qualitative research*. Chicago: Aldine Publishing Co.
- Goffman, E. (1959). *The presentation of self in everyday life.* London: Penguin Books.
- Goffman, E. (1963). *Stigma. Notes on the Management of Spoiled Identity.* Englewood Cliffs: Prentice-Hall.
- Goldschmidt, A. & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112-130.
- Goodman, M. (2010). *Future Crime. Inside the digital underground and the battle for our connected world*. London: Transworld Publishers.
- Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.
- Gottfredson, M. & Hirschi, T. (1990). *A general theory of crime*. Stanford CA: Stanford University Press.
- Gough, N. (2004). RhizomANTically Becoming-Cyborg. Performing posthuman pedagogies. *Educational Philosophy and Theory, 36*(3), 253-265.

- Graboski, P. (2001). Virtual criminality: old wine in new bottles? *Social & Legal Studies, 10*(2), 243-249.
- Guga, J. (2015). Cyborg Tales: The Reinvention of the Human in the Information Age. In J. Romportl, E. Zackova & J. Kelemen (Eds.), *Beyond Artificial Intelligence. Topics in Intelligent Engineering and Informatics* (pp. 45-62). Springer, Cham.
- Guinchard, A. (2010). Crime in virtual worlds: The limits of criminal law. *International Review of Law, Computers & Technology*, *24*(2), 175-182.
- Gunkel, D. (2001). *Hacking Cyberspace.* Boulder, CO: Westview Press.
- Halbert, D. (1997). Discourses of Danger and the computer hacker. *The Information Society, 13*(4), 361-374.
- Hall, M. (2011). Environmental Victims. Challenges for Criminology in the 21st Century. *Journal of Criminal Justice and Security*, 13(4), 345-371.
- Halsey, M. & White, R. (1998). Crime, Ecophilosophy and Environmental Harm. *Theoretical Criminology*, *2*(3), 371-391.
- Haggerty, K.D. & Ericson, R.V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622.
- Haraway, D.J. (1987). A Manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, *2*(4), 1-42.
- Haraway, D.J. (1991). *Simians, Cyborgs and Women: The reinvention of nature*. New York: Routlegde.

- Harman, G. (2009). *Prince of Networks: Bruno Latour and Metaphysics*. Melbourne: Re-pres & Graham Harman.
- Harvey, D. (1989). *The condition of postmodernity.* Oxford: Blackwell.
- Hayward, K. (2002). The vilification and pleisures of youthful transgression. In J. Muncie, G. Hughes & E. McLaughlin (Eds.), *Youth Justice: Critical Readings* (pp. 80-93). London: Sage.
- Hayward, K. (2012). Five Spaces of Criminology. *British Journal of Criminology*, *52*(3), 441-462.
- Hennink, M., Hutter, I. & Bailey, A. (2011). *Qualitative Research Methods*. London: Sage.
- Himanen, P. (2001). *The Hacker Ethic and the Spirits of the Information Age*. New York: Random House.
- Hindelang, M.J., Gottfredson, M.R. & Garofalo, J. (1978). *Victims of personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Cambridge, MA: Ballinger Publishing Co.
- Hinduja, S. (2012). The Heterogeneous Engineering of Music Piracy: Applying Actor-Network Theory to Internet-Based wrongdoing. *Policy and Internet, 4*(3-4), 229-248.
- Holt, T.J. (2010). Examining the role of Technology in the Formation of Deviant Subcultures. *Social Science Computer review*, *28*(4), 466-481.
- Holt, T.J. & Bossler, A.M. (2014). An Assessment of the current state of cybercrime scholarship. *Deviant behavior*, *35*(1), 20-40.
- Holt, T.J., Bossler A.M. & Seigfried-Spellar, K.C. (2015). *Cybercrime and digital forensics. An Introduction*. New york: Routledge.

- Holt, T.J. & Kilger, M. (2008). Techcrafters and Makecrafters: a comparions of two populations of hackers. WOMBAT *Workshop On Information Security Threats Data Collection and Sharing,* 67-78.
- Hutchings, A. & Hayes, H. (2009). Routine activity theory and phishing victimization: Who gets caught in the 'net'? *Current Issues in Criminal Justice 20*(3), 432-451.
- Hutchings, A. & Holt, T.J. (2016). The online stolen data market: disruption and intervention approach. *Global Crime*, *18*(1), 11-30.
- Ienca, M. (2015). Neuroprivacy, Neurosecurity and Brain-hacking: Emerging issues in Neural Engineering. *Bioethica Forum, 8*(2), 51-53.
- Ihde, D. (1990). *Technology and the Lifeworld*. Bloomington/Minneapolis: Indiana University Press.
- Iliopoulos, D., Szor, C. & Adami, P. (2011). *Darwin Inside the Machines. Malware Evolution and the Consequences for Computer Security*, available online at: arXiv:1111.2503v1
- Israel, M. (2004). Strictly Confidential? Integrity and Disclosure of Criminological and Socio-Legal Research. *British Journal of Criminology*, *5*(1), 715-740.
- Jaishankar, K. (Ed.). (2011). *Cyber criminology: Exploring Internet crimes and criminal behavior*. Boca Raton, FL: CRC Press.
- Jansen, J. & Leukfeldt, R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, *10*(1), 79-91.

- Jennings W.G., Piquero, A.R. & Reingle, J.M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and Violent Behavior*, *17*(1), 16-26.
- Jewkes, Y. & Yar, M. (Eds.) (2010). *The Handbook of Internet Crime*. Routledge.
- Jordan, T. & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, *46*(4), 757-780.
- Katz, J. (1988). *The Seductions of Crime: Moral and Sensual Attraction in Doing Evil*. New York: Basic Books.
- Kearon, T. & Leach, R. (2000). Invasion of the 'Body Snatchers': Burglary Reconsidered. *Theoretical Criminology*, *4*(4), 451-472.
- Kerstens, J. & Veenstra, S. (2015). Cyber Bullying in the Netherlands: A Criminological Perspective. *International Journal of Cybercriminology*, *9*(2), 144-161.
- Kilger, M. (2010). Social Dynamics and the Future of Technology-Driven Crime. In T.J. Holt & B. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 2015). Hershey, PA: IGI-Global.
- Kipnis, A.B. (2015). Agency between humanism and posthumanism. *Hau: Journal of Ethnographic Theory*, *5*(2), 43-58.
- Kitchin, R. & Dodge, M. (2011). *Code/Space: Software and Everyday Life*. Cambridge. MA: MIT Press.
- Kleemans, E., Weerman, F. & Enhus, E. (2007). Theoretische vernieuwing in de criminologie. *Tijdschrift voor Criminologie*, *49*(3), 239- 251.

- Knappett, C. & Malafouris, L. (2008). *Material Agency. Towards a Non-Anthropocentric Approach*. New York: Springer.
- Kollanyi, B., Howard, P.N. & Woolley, S.C. (2016). Bots and automation over Twitter during the U.S. Election. *Comprop Data memo. Available at: http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2016/11/Data-Memo-US-Election.pdf*
- Koops, B.J. (2010). The Internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.) *Transnational Criminology Manual*. Nijmegen: WLP, 735–754.
- Krarup, T.M. & Blok, A. (2011). Unfolding the social: quasi-actants, virtual theory, and the new empiricism of Bruno Latour. *The Sociological Review*, *59*(1), 42-63.
- Kwakman, N. (2007). De causaliteit in het strafrecht. Het vereiste van condition sine qua non als enige bruikbare criterium. *Nederlands Juristenblad* 827, *16*, 992-999.
- Latour, B. (1992). Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts. In W.E. Bijker & J. Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change* (pp. 225-258). Cambridge, MA: MIT Press.
- Latour, B, (1986). The powers of association. In J. Law (Ed.), *Power, Action and Belief. A New Sociology of Knowledge?* (pp. 264-280). London: Routledge and Kegan Paul.
- Latour, B. (1987). *Science in Action. How to follow scientists and engineers through society*. Cambridge: Harvard University Press.
- Latour, B. (1993). *We Have Never Been Modern.* Harvester Wheatsheaf.

- Latour, B. (1994). On technical mediation – Philosophy, Sociology, Genealogy. *Common Knowledge*, *3*(2), 29-64.
- Latour, B. (1996). On Actor Network Theory. A few clarifications. *Sociale Welt-Zeitschrift fur Sozialwissenschaftliche forschung und praxis*, *47*(4), 369-381.
- Latour, B. (1999). On recalling ANT. In J. Law and J. Hassard (Eds.), *Actor Network Theory and After* (pp. 15-25). Oxford: Blackwell.
- Latour, B. (2000). When things strike back: a possible contribution of 'science studies' to the social sciences. *British Journal of Sociology*, *51*(1), 107-123.
- Latour, B. (2004). On using ANT for studying information systems: a (somewhat) Socratic dialogue. In C. Avgerou, C. Ciborra & F. Land (Eds.), *The Social Study of Information and Communication Technology. Innovation, Actors and Contexts* (pp. 62-76). Oxford University Press.
- Latour, B. (2005). *Reassembling the Social. An introduction to Actor-Network-Theory*. New York: Oxford University Press.
- Latour, B. (2013). An Inquiry into Modes of Existence. An Anthropology of the Moderns. Harvard University Press.
- Latour, B. & Venn, C. (2002). Morality and Technology: The End of the Means. *Theory Culture Society*, *19*(5/6), 247-260.
- Latour, B. & Woolgar, S. (1986). *Laboratory Life. The Construction of Scientific Facts.* New Jersey: Princeton University Press.
- Law, J. (1992). Notes on the Theory of the Actor-Network: Ordering, Strategy and Heterogeneity. *Systems Practice, 5*(4): 379-393.

- Law, J. (1999). After Ant: Topology, naming and complexity. In J. Law & J. Hassard (Eds.), *Actor Network Theory and After* (pp. 1-14). Blackwell.
- Law, J. (2000). *Networks, Relations, Cyborgs: On the Social Study Of Technology. Centre for Science Studies and the Department of Sociology*, Lancaster University, available online at http://www.comp.lancaster.ac.uk/sociology/soc042jl.html.
- Law, J. (2004). *After method: Mess in Social Science Research*. Routledge.
- Law, J. & Hassard, J. (1999). (Eds.), *Actor Network Theory and After*. Blackwell.
- Lemert, E. (1967). *Human Deviance, Social Problems and Social Control.* Englewood Cliffs: Prentice_Hall.
- Lehman, J. *et al* (2018). *The Surprising Creativity of Digital Evolution: A Collective of Anecdotes from the Evolutionary Computation and Artificial Life Research Communities*, available online at: arXiv:1803.03453
- Leukfeldt, E.R. (2015). Comparing victims of phishing and malware attacks. Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering*, *4*(4), 26-32.
- Leukfeldt, E.R., Domenie, M.M.L & Stol, W.Ph. (2011). Cybercrime is van het volk. Onderzoeksconsequenties voor de beleidsvorming. *Secondant*, *25*(1), 42-45.
- Leukfeldt, E.R., Kleemans, E.R. & Stol, W.Ph. (2016). Cybercriminal Networks, Social Ties and Online Forums: Social Ties versus

Digital Ties Within Phishing and Malware Networks. *British Journal of Criminology*, *57*(3), 704-722.

- Leukfeldt, E.R. & Yar, M. (2016). Applying Routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.
- Levy, S. (1984). *Hackers heroes of the information age.* New York: Double Day.
- Leys, M., Zaitch, Z. & Decorte, T. (2016). De Gevalstudie. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve Methoden en Technieken in de Criminologie* (pp. 161-186). Leuven/Den Haag: Acco.
- Lindgren, S-A. (2005). Social Constructionism and Criminology. Traditions, Problems and Possibilities. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *6*(1), 4-22.
- Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal (Canadian Edition)*, *7*(1), 35-49.
- Lupton, D. (1999). Monsters in Metal Cocoons: 'Road Range' and Cyborg bodies. *Body & Society, 5*(1), 57-72.
- Lyng, S. (2004). Crime, Edgework and Corporeal Transaction. *Theoretical Criminology, 8*(3), 359-375.
- Mähring, M., Holmström, J., & Montealegre, R. (2004). Trojan Actor-Networks and Swift Translation: Bringing Actor-Network Theory to Project Escalation Studies. *Information Technology & People*, *17*(2), 210-238.

- Maimon, D. *et al*. (2015). On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology*, *55*(3), 615-634.
- Maimon, D., Kamerdze, A., Cukier, M. & Sobesto, B. (2013). Daily Trends and Origins of Computer-Focused Crimes against a Large University Network. An Application of the Routine-Activities and Lifestyle Perspective. *British Journal of Criminology*, *53*(2), 319-343.
- Mann, D. & Sutton, M. (1998). >>NETCRIME: More Change in the Organization of Thieving. *The British Journal of Criminology, 38*(2), 201-229.
- Martin, A. (2005). Agency in Inter-Action: Bruno Latour and Agency. *Journal of Archaeological Method and Theory*, *12*(4), 283-311.
- Masys A.J. (2014). Critical Infrastructure and Vulnerability: A Relational Analysis Through Actor Network Theory. In Masys A. (eds), *Networks and Network Analysis for Defence and Security* (pp. 265-280). Lecture Notes in Social Networks. Springer, Cham.
- Masys A.J. (2015). The Cyber-Ecosystem Enabling Resilience Through the Comprehensive Approach. In Masys A. (eds) *Disaster Management: Enabling Resilience. Lecture Notes in Social Networks* (pp. 143-154). Springer, Cham
- Matza, D. (1964). *Delinquency and Drift*. New York: John Wiley.

- Matza, D. (1969). *Becoming Deviant.* Englewood Cliffs: Prentice Hall.
- Mead, G.H. (1934). *Mind, Self and Society: From the Standpoint of a Social Behaviorist*. Chicago: Chicago University Press.
- McGuirre, M. (2008). *From hyperspace to hypercrime: Technologies and the geometries of deviance and control* (British Criminology Conference 8). Londen: British Society of Criminology.
- McLean, C. & Hassard, J. (2004). Symmetrical Absence/Symmetrical Absurdity: Critical Notes on the Production of Actor-Network Accounts*, Journal of Management Studies*, *41*(3), 493-519.
- McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice*, *31*(1), 30-52.
- Michalowski R.J. & Kramer, R.C. (2007). State-Corporate Crime and Criminological Inquiry. In H.N. Pontell & G. Geis (Eds.), *International Handbook of White-Collar and Corporate Crime* (pp. 200-219). Springer, Boston, MA.
- Mielke, C. J. & Chen, H. (2008). Botnet and the cybercriminal underground. In *International Conference on Intelligence and Security Informatics 2008* (pp. 206-211). IEEE.
- Milward, H.B. & Raab, J. (2006). Dark Networks as Organizational Problems. Elements of a Theory. *International Public Management Journal*, *9*(3), 333-360.

- Mol, A. (2010). Actor-Network Theory: sensitive terms and enduring tensions. *Kölner Zeitschrift für Soziologie und Sozialpsychologie, 50*(1), 253-269.
- Monsma, E., Buskens, V., Soudijn, M. & Nieuwbeerta, P. (2010). Partners in cybercrime: An online forum evaluated from a social network perspective. *ISCORE papers, 285*, 1-28.
- Moszkowicz, Y. (2009). Een kritische noot bij "Runescape" en "Habbo-hotel"-uitspraken: een illusie is geen goed. *Strafblad*, 495-503.
- Mythen, G & McGowan, W. (2018). Cultural victimology revisited. Synergies of risk, fear and resilience. In S. Walklate (Ed.), *Handbook of Victims and Victimology* (pp. 364-378). London/New York: Routledge.
- Nikitina, S. (2012). Hackers as Trickster of the Digital Age: Creativity in Hacker culture. *Journal of Popular Culture, 45(1)*, 133- 152.
- Nissen, J. (1998). Hackers: Masters of Modernity and Modern Technology. In J. Sefton-Green (Ed.), *Digital Diversions: Youth Culture in the Age of Multimedia* (pp. 149–171). London: UCL Press.
- Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media* Society, *6*(2), 195-217.
- O'Brien, M. (2005). What is Cultural about Cultural Criminology? *British Journal of Criminology*, *45*(5), 599-612.
- Odinot, G., Verhoeven, M.A., Pool, R.L.D & De Poot, C.J. (2016). Chapter II. Cyber-OC in the Netherlands. In G. Bulanova-Hristova

et al. (Eds.), *Cyber-OC-Scope and manifestations in selected EU member states* (pp. 15-99). Bundeskriminalamt Criminalistic Institute.

- O'Neil, M. (2006). Rebels for the system? Virus writers, general intellect, cyberpunk and criminal capitalism, *Continuum: Journal of Media & Cultural studies*, *20*(2), 225-241.
- Overill, R.E. (1998). Trends in Computer Crime. *Journal of Financial Crime*, *6*(2), 157-162.
- Paxton, N.C. Ahn, G-J. & Shehab, M. (2011). Master-Blaster: Identifying Influential Players in Botnet Transactions. In *The 35th Annual Computer Software and Applications Conference* (pp. 413-419). IEEE.
- Pease, K. (2001). Crime futures and foresight. Challenging criminal behavior in the information age. In D. Wall (Ed.), *Crime and the Internet* (pp. 18-28). London: Routlegde.
- Pinch, T. (2010). The Invisible Technologies of Goffman's Sociology From the Merry-go Round to the Internet, *Technology and Culture*, *51*(2), 409-424.
- Pratt, T.C. & Turanovic J.J. (2015). Lifestyle and Routine Activity Theories Revisited: The Importance of "Risk" to the Study of Victimization. *Victims & Offenders*, *11*(3), 335-354.
- Preda, A. (1999). The turn to things: Arguments for A Sociological Theory of Things. *The Sociological Quarterly*, *40*(2), 347-366.
- Reyns, B.W. (2013). Online routines and identity theft victimization further expanding routine activity theory beyond

direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238.

- Rock, P. (2007). Theoretical perspectives on victimization. In S. Walklate, *Handbook of Victims and Victimology* (pp. 37-61). Willan Publishing.
- Sandywell, B. (2010). On the globalization of crime: the Internet and new criminality. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 38-66). London/New York: Routledge.
- Schinkel, W. (2007). Sociological discourse of the relational: the cases of Bourdieu & Latour. *The Sociological Review*, *55*(4), 707-729.
- Schless, T. & Vranken, H. (2013). Counter Botnet Activities in the Netherlands. A study on organization and effectiveness. In *the 8th International Conference for Internet Technology and Secured Transactions* (pp. 437- 442). IEEE.
- Schuilenburg, M.B. (2015). *The Securization of Society: Crime, Risk and Social Order*. New York: New York University Press.
- Silva, S.S.C., Silva, R.M.P, Pinto, R.C.G. & Salles, R.M. (2012). Botnets: A Survey. *Computer Networks*, *30*, 378-403.
- Silvast, A. & Reunanen, M. (2014). Multiple Users, Diverse Users: Appropriation of Personal Computers by Demoscene Hackers. In G. Alberts & R. Oldenziel (Eds.), *Hacking Europe. From Computer Cultures to Demoscenes* (pp. 151-163). Springer.
- Skibell, R. (2002). The Myth of the Computer Hacker. *Information, Communication and Society*, *5*(3), 336-356.

- Skoudis, E. & Zeltser, L. (2004). Malware Fighting Malicious Code. New Jersey: Prentice Hall.
- Smith, G.J.D., Bennet Moses L & Chan, J. (2017). Challenges of doing criminological research in the big data area: towards a digital and data-driven approach. *British Journal of Criminology*, *57*, 259-274.
- Sørensen, M. H. & Ziemke, T. (2007). Agents Without Agency? *Cognitive Semiotics (special issue)*, 102–124.
- Soudijn, M.R.J. & Zegers, B.C.H.T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*(2-3), 111-129.
- Speer, D.L (2000). Redefining Borders. The Challenges of Cybercrime. *Crime Law & Social Change*, *34*(3), 259-273.
- Stake, R.E. (2008). Qualitative case studies. In N.K. Denzin & Y.S. Lincoln (Eds.), *Strategies of qualitative inquiry* (pp. 119-150). Thousand Oaks, CA: Sage.
- Staring, R. & Van Swaaningen, R. (2016). Kwalitatief onderzoek en criminologische theorie. Over de relatie tussen theorie, onderzoeksvragen en methode. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve Methoden en Technieken in de Criminologie* (pp. 33-80). Leuven/Den Haag: Acco.
- Steinmetz, K.F. (2014). The Greatest Crime Syndicate Since the Gambino's: A Hacker Critique of Government, Law, and Law Enforcement. *Deviant Behavior, 35*(3), 243-261.
- Steinmetz, K.F. (2015) Craft(y)ness. An Ethnographic Study of Hacking. *British Journal of Criminology*, *55*(1), 125-145.

- Steinmetz, K.F. & Gerber, J. (2015). "It Doesn't Have Be This Way": Hacker Perspectives on Privacy. *Social Justice, 41*(3), 29-51.
- Steinmetz, K.F. & Nobles, M.R. (2017). *Technocrime and Criminological Theory*. Routledge.
- Sterling, B. (1993). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Viking: London.
- Strikwerda, L. (2012). Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. *Ethics and Information Technology, 14*(2), 89-97.
- Strikwerda, L. (2015). Present and Future Instances of Virtual Rape in Light of Three Categories of Legal Philosophical Theories on Rape. *Philosophy & Technology*, *28*(4), 491-510.
- Stryker, C. (2012). *Hacking the future: Privacy, Identity and Anonymity on the web*. New York: Cole Stryker.
- Suarez, J.R.P. (2015). *We are Cyborgs: Developing a Theoretical Model for Understanding Criminal Behaviour on the Internet*. Dissertation, University of Huddersfield.
- Suler, J. (2004). The online disinhibition effect. *CyberPsychology and Behavior*, 7(3), 321-326.
- Tarde, G. (1999). *Monadologie et sociologie*, re-edition. Paris: Les empêcheurs de penser en rond.
- Taylor, P.A. (1999). *Hackers. Crime in the digital sublime.* London and New York: Routledge.
- Taylor, P.A. (2005). From Hackers to Hacktivists: Speed bumps on the Global Superhighway? *New Media Society, 7*(5), 625-646.

- Tenebro, G. (2009). The Bredolab Files. Symantec Corporation, available online at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_bredolab_files.pdf
- Thomas, D. (2005). Hacking the body: code, performance and corporeality. *New Media & Society*, *7*(5), 647-662.
- Thomas, D. & Loader, B. (2000). Introduction – Cybercrime: Law enforcement, security and surveillance in the information age. In D. Thomas & B. Loader (Eds.), *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge.
- Tombs, S. (2017). Mitigating and Responding to Corporate Violence: Beyond Crime and Criminology. In A. Amatrudo (Eds.), *Social Censure and Critical Criminology* (pp. 217-245). London: Palgrave Macmillan.
- Tropina, T. (2016). The nexus of information technologies and illicit financial flows. *ERA Forum*, DOI 10.1007/s12027-016-0435-2.
- Turgeman-Goldschmidt, O. (2005). Hacker's Accounts: Hacking as a Social Entertainment. *Social Science Computer Review, 23*(1), 8-23.
- Turgeman-Goldschmidt, O. (2008). Meanings that Hackers Assign to their Being a Hacker. *International Journal of Cyber Criminology, 2*(2), 382-396.

- Turkle, S. (1982). The Subjective Computer: A Study in the Psychology of Personal Computation. *Social Studies of Science, 12*, 173-205.
- Turkle, S. (1984). Hackers: Loving the Machine for Itself. In *The Second Self: Computers and the Human Spirit* (pp.196-238). New York: Simon & Schuster.
- Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. New York: Simon & Schuster.
- Turkle, S. (2005). *The Second Self: Computers and the Human Spirit*. Cambridge, MA: MIT press.
- Van Baar, A. & Huisman, W. (2012). The Oven Builders of The Holocaust. A Case Study of Corporate Complicity in International Crimes. *British Journal of Criminology*, *52,* 1033-1050.
- Van de Bunt, H. (2015). Ethische dilemma's bij criminologisch onderzoek. Tijdschrift over Cultuur en Criminaliteit, *5*(1), 55-69.
- Vandenberghe, F. (2002). Reconstructing Humants: A Humanist Critique of Actant-Network Theory, *Theory, Culture Society*, *19*(5/6), 51-67.
- Van de Port, M. (2001). G*eliquideerd: criminele afrekeningen in Nederland*. Amsterdam: Meulenhof.
- Van der Hulst, R.C. & Neve, R.J.M. (2008). *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie.* Den Haag: Wetenschappelijk Onderzoek-en Documentatiecentrum.
- Van der Wagen, W. (2018/*forthcoming*). The Cyborgian Deviant: An Assessment of the Hacker through Actor-Network Theory. *Journal of Qualitative Criminal Justice & Criminology*.

- Van der Wagen, W., M. Althoff & Van Swaaningen, R. (2016). De andere 'anderen'. Een exploratieve studie naar processen van labelling van, door en tussen hackers. *Tijdschrift over Cultuur & Criminaliteit, 6*(1), 27-41.
- Van der Wagen, W. & Dimitrova, E. (2018). *Mission Cyborg: Op naar een hybride kijk op (de bestrijding van) cybercriminele (actor)netwerken*. Driebergen: Dienst Landelijke Recherche, report.
- Van der Wagen, W. & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578-595.
- Van der Wagen, W. & Pieters, W (2018/under review). The hybrid victim: Re-conceptualizing high-tech cybervictimization through actor-network theory.
- Van Hardeveld, G.J., Webber, C & O'Hara, K. (2017). Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist*, *61*(11), 1244-1266.
- Van Erp. J., Stol, W. & Van Wilsem, J. (2013), Criminaliteit en criminologie in een gedigitaliseerde wereld. *Tijdschrift voor Criminologie, 55*(4), 327-341.
- Van Loon, J. (2002). *Risk and Technological Culture. Towards a sociology of virulence*. London and New York: Routledge Taylor and Francis Group.

- Van't Hof, C. (2015). *Helpende Hackers. Verantwoorde onthullingen in het digitale polderlandschap*. Rotterdam: Uitgeverij Tek Tok.
- Van Wilsem J.A. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2): 115-127.
- Veenstra, S., Zuursteen, R. & Stol, W.Ph. (2016). *Cybercrime among companies. Research into cybercrime victimisation among small and medium-sized enterprises and on-businesses in the Netherlands.* Eleven International Publishing.
- Verbeek P-P. (2005). *What Things Do: Philosophical Reflections on Technology, Agency and Design*. University Park: Pennsylvania State University Press.
- Verbeek, P-P (2008). De grens van de mens. Over de relatie tussen mens en techniek. In I.L. Consolie & R. Hoekstra (Eds.), *Annalen van het Thijmgenootschap* (pp. 14-36). Nijmegen: Valkhof Pers.
- Verbeek, P-P. (2014). Some Misunderstandings About the Moral Significance of Technology. In P. Kroes & P-P. Verbeek (Eds.), *The Moral Status of Technical Artefacts* (pp. 75-88). Dordrecht: Springer.
- Verschuren, P.J.M. (2003). Case study as a research strategy: some ambiguities and opportunities. *International Journal of Social Research Methodology*, *6*(2), 121-139.

- Vicini, A. & Brazal, A.M. (2015). Longing for Transcendence: Cyborgs and Trans- and Posthumans. *Theological Studies*, *76*(1), 148-165.
- Von Hentig, H. (1940). Remarks on the interaction of perpetrator and victim. *Journal of Criminal Law and Criminology, 31*(3), 303-309.
- Von Hentig, H. (1948). *The Criminal and His Victim*. Hamden, CT: Archon Books.
- Wall, D.S. (2007). *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press.
- Wall, D.S. (2008). Cybercrime and the Culture of Fear. Social Science Fiction(s) and the Production of Knowledge about Cybercrime. *Information, Communication & Society, 11*(6), 861-884.
- Wagenaar, P. (2012). *Detecting botnets using file system indicators*, Master Thesis*,* University of Twente, Enschede.
- Webber, C. & Vass, J. (2010). Crime, film and the cybernetic imagination. In Y. Jewkes & M. Yar (Eds.), *The Handbook of Internet Crime* (pp. 120-144). London/New York: Routledge.
- Wessells, A.T. (2007). Reassembling the Social: An Introduction to Actor-Network Theory by Bruno Latour (book review). *International Public Management Journal*, *10*(3), 351-356.
- Whitson, J.R. & Haggerty, K.D. (2008). Identity Theft and the care of the virtual self. *Economy and Society*, *37*(4), 572-594.

- Wouters, K., Loyens, K., Maesschalck, J. & De Schrijver, A. (2004). Morele dilemma's bij criminologisch onderzoek. *Panopticon: Tijdschrift voor Strafrecht, Criminologie en Forensisch Welzijnswerk*, *35*(4), 313-335.
- Wood, M. (1998). Agency and Organization: Toward a Cyborg-Consciousness. *Human Relations*, *51*(10), 1209-1226.
- Wood, M.A. (2017). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's technological unconscious. *Theoretical Criminology*, *21*(2), 168-185.
- Yar, M. (2005a). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.
- Yar, M. (2005b). Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal, 44*(4), 387-399.
- Yar, M. (2012). Sociological and Criminological Theories in the Information Era. In E.R. Leukfeldt & W.Ph Stol (Eds.), *Cyber Safety: An Introduction* (pp. 45-55). The Hague: Eleven International Publishing.
- Yar, M. (2013). *Cybercrime and society*. Thousand Oaks, CA: Sage.
- Yip, M., Shadbolt, N. & Webber, C. (2012). Structural analysis of online criminal social networks. In *International Conference on Intelligence and Security Informatics* (pp. 60–65). IEEE.

Nederlandse samenvatting (Dutch Summary)

Achtergrond, vraag- en doelstelling van het proefschrift

De vraag of cybercrime 'oude wijn in nieuwe zakken is' of dat het echt om een fundamenteel nieuw verschijnsel gaat dat om nieuwe theorieën vraagt, heeft tot dusver veel cybercriminologen beziggehouden. Dit proefschrift mengde zich ook in deze discussie door na te gaan of bestaande criminologische theorieën nog voldoende verklaringskracht hebben in het licht van de (a)typische kenmerken van hightech cybercrime, waaronder haar (deels) geautomatiseerde en gedistribueerde karakter. Het proefschrift vertrok vanuit de aanname dat bestaande raamwerken in de (cyber)criminologie (nog) te instrumenteel (substantivistisch), antropocentrisch en dualistisch zijn ingesteld om deze kenmerken te duiden en dat de criminologie daarom haar theoretische grenzen moet verleggen. Het proefschrift beoogde dit te doen door exploratief onderzoek te doen naar het theoretische (cyber)potentieel van de actor-netwerktheorie (ANT). Dit betreft een perspectief (of lens) die de mens-techniek relatie juist niet in uitsluitend instrumentele (of deterministische) termen duidt, die de mens niet als de enige significante actor in de sociale wereld beschouwt en die zich tegen dualistische of binaire denkkaders keert. Het perspectief zou daarmee mogelijk waardevolle handvatten kunnen bieden voor theoretische vernieuwing in de cybercriminologie.

Om de theoretische (meer)waarde van ANT te exploreren, zijn een viertal empirische casestudies uitgevoerd, namelijk een analyse van een botnet, twee kleinschalige etnografische studies naar hackers en een casestudie waarin drie soorten slachtofferschap zijn geanalyseerd (respectievelijk ransomware, botnets en virtuele diefstal). De achterliggende gedachte achter het doen van deze casestudies was dat het theoretische potentieel van ANT beter verkend, getoetst en verfijnd kon worden op basis van empirisch materiaal en dat zo ook de toevoegde waarde ten opzichte van bestaande theorieën beter inzichtelijk zou kunnen worden gemaakt. Het uiteindelijke doel van het onderzoek was om, op basis van deze casestudies een alternatief perspectief te ontwikkelen, wat uiteindelijk het 'cyborg crime' - perspectief is gaan heten.

De vier casestudies en haar bevindingen

Hieronder volgt een samenvatting van de verschillende casestudies die in het proefschrift aan de orde zijn geweest. Wat was het vertrekpunt van de casestudie en wat heeft de studie theoretisch en/of empirisch gezien opgeleverd?

Het botnet als hybride crimineel actor-netwerk (hoofdstuk 2)

De eerste casestudie in het proefschrift betrof de analyse van een botnet, een crimineel fenomeen dat exemplarisch is voor het gerobotiseerde karakter van cybercrime. De studie vertrok vanuit de gedachte dat bestaande criminologische theorieën, inclusief de routine-activiteitentheorie en de rationale keuzetheorie te antropocentrisch

lijken te zijn voor de analyse van vormen van hightech cybercrime die een geautomatiseerd en gedistribueerd karakter hebben zoals botnets. Om deze reden werd een beroep gedaan op de constructivistische lens van ANT en werd het botnet geconceptualiseerd als een hybride crimineel actor-netwerk dat niet uitsluitend wordt aangestuurd door de mens noch door de machine. De vier betekenissen van ANT's concept van technische mediatie ('composition', 'translation', 'delegation' en 'reversible blackboxing') werden gebruikt als conceptueel kader om een botnet-casus te bestuderen. In dit kader zijn politiedossiers geanalyseerd en is een interview met een bij het onderzoek betrokken rechercheur afgenomen.

Uit het onderzoek kwam ten eerste naar voren dat diverse menselijke en niet-menselijke actoren (groot en klein) een rol spelen in de opzet van de infrastructuur van het botnet, de besmetting van de computers, het gebruik en het beheer van het botnet en bij de ontmanteling van het botnet. Hoewel de rol van de botherder belangrijk was, zou het te beperkt zijn om het botnet slechts als een door de mens (botherder) aangestuurd netwerk te beschouwen. De studie liet namelijk zien dat er verschillende actoren direct of indirect (actief) betrokken waren bij het 'succes' van dit botnet. Deze actoren waren ofwel gecreëerd, bestonden al of moesten misleid worden om in het handelingsprogramma van de botherder te worden opgenomen. De studie liet ten tweede zien dat de rol van de betrokken technische entiteiten niet slechts functioneel en passief was. Ze konden bijvoorbeeld een bepaald gebruik of nieuwe (criminele) handelingen uitlokken (zowel bij de botherder of zijn

klanten) en brachten ook onverwachte situaties teweeg voor de botherder. Zo kon de explosieve groei van het botnet niet op voorhand voorspeld worden en moest de botherder aanpassingen maken in de infrastructuur. Ten derde kwam uit het onderzoek naar voren dat de continuering of 'overleving' van het botnet ook afhankelijk was van een complexe vermenging tussen zowel menselijke als niet-menselijke componenten. Zo kon het botnet pas ontmanteld worden zodra de botherder, de infrastructuur en de individuele infecties werden gestopt. Als slechts een of twee element uit het netwerk werden gehaald, kon het botnet blijven voortbestaan.

De studie concludeerde dat ANT in drie opzichten toegevoegde waarde had ten opzichte van bestaande perspectieven zoals de routine-activiteitentheorie (RAT) en de rationele keuze theorie (RC). Allereerst maakte ANT het mogelijk om een grotere en diversere groep actoren in kaart te brengen die een rol spelen bij het ontstaan en de ontwikkeling van een botnet. Het kon zo inzichtelijk maken dat de betrokken entiteiten (inclusief de botherder) pas kracht en betekenis krijgen in relatie tot andere entiteiten in het netwerk. Daarnaast kon de ANT lens ook goed laten zien hoe daderschap, slachtofferschap en preventie/toezicht met elkaar verweven kunnen zijn. Waar de RAT dit min of meer als drie aparte en vooraf bestaande statische elementen beschouwt, ziet ANT deze elementen als dynamisch en beschouwt hen als met elkaar vervlochten of gedeeltelijk overlappende netwerken. Tot slot werd gesteld dat ANT's visie van actorschap beter inzichtelijk kan maken hoe technologie actief het criminele proces en het resultaat daarvan kan

vormgeven, omdat zij de mens niet als de (enige) centrale kracht ziet achter (de uitvoering van) criminele activiteiten. De algehele conclusie van deze studie was dat ANT en haar hybride en 'genetwerkte' duiding van actorschap bepaalde (complexe) elementen en dynamieken van het criminele proces beter in kaart kan brengen dan een traditionele criminologische benadering. De eerste contouren van het 'cyborg crime' - perspectief waren getekend in deze studie.

Waar deze eerste casestudie zich vooral focuste op de aard van hightech cybercrime, het geautomatiseerde of gerobotiseerde karakter in het bijzonder, trachtten de opvolgende casestudies licht te werpen op de (a)typische cyberdader: de hacker. De eerste studie (hoofdstuk 3) benaderde het fenomeen vooral vanuit een meer conventionele criminologische lens (de labellingbenadering) en de tweede studie (hoofdstuk 4) maakte gebruik van de ANT lens. Zo kon de toegevoegde waarde ANT beter inzichtelijk worden gemaakt.

De andere 'anderen' (hoofdstuk 3)

Deze studie ving aan met de constatering dat hacking een schoolvoorbeeld is van de notie dat criminaliteit een sociale constructie is. Waar hackers in de jaren zestig nog beschouwd werden als helden of whizzkids; sinds de jaren negentig worden ze vooral geportretteerd als stereotypische cybercriminelen. Tegenwoordig, althans in Nederland, lijkt er echter tegelijkertijd sprake te zijn van enige toenadering tot zogenaamde 'ethische' hackers, hackers die zich vooral richten op het

vinden van beveiligingslekken en deze gedicht willen krijgen. Deze studie had als doel om te onderzoeken hoe hackers zelf tegen deze ontwikkelingen aankijken en om te exploreren of zij het label dat zij opgeplakt krijgen van zich afwerpen en/of internaliseren. Meer specifiek, wilde de studie achterhalen hoe hackers denken dat de buitenwereld hen ziet, hoe zij zichzelf zien en hoe zij zichzelf beschouwen ten opzichte van anderen. Voorts, in het verlengde hiervan, beoogde de studie de verklaringskracht van de labellingbenadering te exploreren voor hackers als 'digitale anderen,' om zo na te gaan of de theorie een digitale impuls nodig heeft. Naast interviewmateriaal werd ook nog een vijftal strafdossiers geanalyseerd waarbij hacking de centrale aanklacht was.

De onderzoeksbevindingen lieten zien dat hackers het gevoel hebben dat de buitenwereld hen ziet als mysterieuze, 'nerderige' en gevaarlijke anderen, maar bovenal als criminele anderen, een label die ze volledig afwijzen. In plaats daarvan definiëren de hackers hun 'anders zijn' vooral in niet-criminele termen. Ze typeren zichzelf als hobbyisten met een specifieke belangstelling voor technologie en beschouwen hacking in termen van creativiteit en kunst, 'out of the box' denken en een bepaalde 'state of mind.' Tevens zien respondenten (ook de black hat hackers) zichzelf veeleer als helpers dan als criminelen. Ook al doen ze een hack die illegaal is, ze stellen dat ze het slachtoffer - het bedrijf dat de beveiliging niet op orde heeft - juist helpen, onderwijzen en confronteren. De geïnterviewden positioneren zichzelf ook sterk ten opzichte van andere 'anderen'. Ze distantiëren zich van de 'echte'

cybercriminelen met betrekking tot hun intentie, modus operandi en verantwoordelijkheid en ten opzichte van andere hackers in termen van intentie en karakter. Hackers slagen er in ieder geval in om het opgeplakte label succesvol van zich af te werpen. De studie brengt tevens naar voren, in lijn met de bevindingen van Turgeman-Goldschmidt (2008), dat hackers in staat zijn om het label ook niet te internaliseren. In plaats van een negatief zelfbeeld, zien zij zichzelf vooral als positieve anderen. Zij hebben geen tekortkomingen, maar iets extra's waar zij trots op zijn.

Deze laatste bevinding rijmt dan ook niet met de assumpties van de labellingtheorie. Deze benadering gaat er namelijk van uit dat labelling leidt tot een negatiever zelfbeeld of zelfs tot een geschonden identiteit. De verklaring voor het feit dat dit bij hackers minder of niet speelt, werd vooral gezocht in de kenmerken van het hackerfenomeen zelf. Hacking vraagt om een specifieke skillset en ook hebben hackers een sterk eigen moraal waarin zij hun handelingen betekenis geven. Niet de buitenwereld, maar vooral andere hackers (de exclusieve groep waarmee ze zich associëren) zijn belangrijk bij de vorming van hun zelfbeeld. Ook de rol van de digitale wereld is mogelijk van belang. Het feit dat hackers kunnen driften tussen de online en offline wereld, zou er voor kunnen zorgen dat ze twee identiteiten tegelijkertijd kunnen managen. Dit laatste reduceert mogelijk niet alleen de negatieve implicaties van labelling, maar het neutraliseert ook hun betrokkenheid bij eventueel schadelijke activiteiten. Naast het toevoegen van een digitale dimensie aan de labelling benadering, werd gesteld dat de

theorie verrijkt zou kunnen worden door meer aandacht te besteden aan labelling binnen groepen. In deze context, leek Latours (2005) concept van de 'anti-groep' relevant. 'Anders zijn' is namelijk niet alleen een kwestie van associatie met soortgelijke anderen, maar juist ook een proces van zich distantiëren van andere binnen of buiten de eigen groep.

De cyborg-deviant (hoofdstuk 4)

Het startpunt van deze studie was dat hackers, of ze nu betrokken zijn bij legale of illegale hackerpraktijken, een benadering behoeven die de relatie tussen mens en technologie centraler stelt in de analyse. Hoewel bestaande studies ook wel naar deze relatie kijken, wordt hier op een vrij antropocentrische, dualistische en hiërarchische manier naar gekeken. Gesteld werd dat ANT, een perspectief die een meer 'post-menselijke' of 'cyborg' kijk hanteert ten aanzien van actorschap, in staat zou kunnen zijn om een genuanceerder begrip te kunnen krijgen van deze relatie. Op basis van tien interviews met zowel hackers, die betrokken waren legale als illegale hacks, verkende deze studie hoe hackers betekenis geven aan zichzelf en hun acties en hoe dit mede werd gevormd door hun (deviante) relatie met technologie.

De resultaten lieten zien dat hackers zichzelf zien als actoren met een hele specifieke 'skillset' en 'mindset', welke hen onderscheidt van 'normale' mensen en criminelen. Ten eerste zien ze zichzelf als getalenteerde en creatieve personen die een aangeboren fascinatie en affiniteit hebben met objecten en technologie. Ze typeren zichzelf zowel

als ‘reversible blackboxers’ als ‘out of the box denkers’. De respondenten zien zichzelf ook als helden of moraalridders die hun eigen specifieke ideeën hebben over goed en kwaad. (Bestaande) grenzen zijn onnatuurlijk voor hen. Ze willen deze (door)breken, verleggen of juist eigen grenzen stellen. Ze geloven ook over bepaalde zintuigelijke vaardigheden of krachten te beschikken waarmee ze bepaalde dingen kunnen zien, opmerken of doorgronden waar normale mensen blind voor zijn. In dat opzicht zien ze zichzelf ook in zeker zin als supermensen of cyborgs, want hun lichaam en geest heeft een extensie. Hoewel we hackers als een atypische of unieke deviante groep kunnen beschouwen vond de studie ook gelijkenissen met andere deviante en niet-deviante groepen, waaronder bankrovers, graffitispuiters, sporters en gamers.

Een tweede bevinding was dat de geïnterviewde hackers hun relatie met technologie niet slechts als instrumenteel of functioneel beschouwden. Zij beschreven deze relatie onder meer als coöperatief, competitief, intiem en exploratief. Zo zien de respondenten hacking bijvoorbeeld niet slechts als een menselijke solo-operatie, omdat ze ook een beroep moeten doen op bestaande technologische tools c.q. ‘wapenarsenaal’. Ze passen deze aan naar hun eigen voorkeur of handelingsprogramma. Hier zien we dan ook duidelijk Latours ‘wapen-mens hybride’ in terug, welke illustratief is voor de notie dat (de functionaliteit van) technologie menselijke capaciteiten, vaardigheden en intenties kan medevormgeven.

In theoretisch opzicht werd geconcludeerd dat ANT’s cyborg-perspectief een nieuwe dimensie toevoegt aan bestaande concepten (bijvoorbeeld

'meesterschap', 'spanning zoeken', 'plezier') die gebruikt worden om het hackerfenomeen te duiden, omdat het zich specifieker richt op hoe de interactie met technologie deviante handelingen, percepties en intenties mede vormgeeft. Hiermee bouwde de studie dus voort op het 'cyborg crime' concept zoals deze was geformuleerd in de eerdere botnetstudie. Het voegde echter een subjectieve dimensie hieraan toe, welke ook alleen te exploreren en te achterhalen was door middel van diepte-interviews. In het kader van de toegevoegde waarde van ANT ten opzichte van bestaande concepten, concludeerde de studie dat ANT bepaalde aspecten beter kon duiden omdat het naar de verschillende hybride hoedanigheden kijkt waarin een hacker handelt en beweegt en daarmee hun betekenisgeving niet loskoppelt van de tools en technologie waarmee zij in verbinding staan. In het kader van dit laatste werd dan ook de toegevoegde waarde zichtbaar van het cyborg-perspectief ten opzichte van de labellingbenadering, toegepast in het voorafgaande hoofdstuk.

Een andere belangrijke conclusie was dat de ANT lens, net als de bredere notie van Haraway's (1987) cyborg, het mogelijk maakt om het hackerfenomeen op een minder dualistische manier te benaderen. Zo was het mogelijk om te (laten) zien dat hacking als een praktijk en vorm van deviant gedrag, een complex samenspel is van zowel grenzen doorbreken als grenzen bepalen en verleggen, zowel technisch als moreel. De algehele conclusie was dat ANT's post-menselijke benadering zeker theoretisch potentieel heeft voor de studie van hacking en andere vorm van hightech cybercrime of deviant gedrag.

Het hybride slachtoffer (hoofdstuk 5)

De laatste casestudie in het proefschrift nam drie soorten hightech slachtofferschap onder de loep. Deze studie was relatief theoretischer dan de vorige studies en had ook een andere opbouw. Het hanteerde een probleemgestuurde benadering door drie empirische casussen van cyber-slachtofferschap (ransomware, botnets and high-tech virtuele diefstal) als startpunt te nemen. Door (a)typische kenmerken uit de casussen te abstraheren, beoogde de studie de beperkingen en blinde vlekken van bestaande benaderingen, die gebruikt worden om slachtofferschap te verklaren, bloot te leggen. Het liet zien dat benaderingen zoals de levensstijlbenadering en de routine-activiteitentheorie (RAT) te antropocentrisch, reductionistisch en dualistisch zijn voor de analyse van de casussen. Ze conceptualiseren kwetsbaarheid bijvoorbeeld vooral als een kenmerk dat toegeëigend kan worden aan een enkele entiteit (mens of object). De casussen laten echter zien dat kwetsbaarheid wordt gegenereerd door verschillende entiteiten samen. Zo worden computergebruikers vaak bereikt via de kwetsbaarheid van andere actoren waar ze mee in verbinding staan (bijvoorbeeld kwetsbare websites) en/of moeten ze eerst op een technische manier getarget worden voordat er een 'menselijke' kwetsbaarheid ter sprake komt. Met andere woorden: de menselijke kwetsbaarheid kan ook niet losgezien worden van de technische kwetsbaarheid. De casussen laten tevens (en wederom) zien dat het handhaven van bestaande dualismen zoals menselijk versus niet-menselijk, echt versus fictioneel, dader versus slachtoffer niet langer

productief is bij de duiding van het cyberslachtoffer(schap) als entiteit en als proces. Op basis van deze analyse, heeft de studie het theoretische potentieel van ANT onderzocht in relatie tot deze casussen en gekeken of ANT een alternatief zou kunnen bieden voor de conceptuele beperkingen van de eerder besproken theorieën.

Het onderzoek resulteerde uiteindelijk in drie alternatieve op ANT-gebaseerde concepten, aangeduid als de 'hybride slachtoffertheorie.' Het concept 'victim composition' weerspiegelt de notie dat het (kwetsbare) slachtoffer beschouwd moet worden als een hybride en gedistribueerd netwerk dat bestaat uit verschillende menselijke, technische en/of virtuele entiteiten die moeten worden 'getarget' door de dader. Vanuit dit perspectief wordt kwetsbaarheid geconceptualiseerd op een meer gedistribueerde en emergente manier en wordt het niet beschouwd als een kenmerk dat toegekend kan worden aan een enkele entiteit – of het nu een technisch systeem of een persoon betreft. Het concept 'victim delegation' vestigt de aandacht op hoe de taken en rollen verdeeld zijn in de totstandkoming van slachtofferschap over tijd. Het concept 'victim translation' stelt in staat om slachtofferschap als een meer veranderlijk, interactioneel en fluïde proces te analyseren in plaats van als een afgebakende concrete gebeurtenis ('event'). Het beschouwt slachtofferschap derhalve als het resultaat van een complexe interactie tussen verschillende handelingsprogramma's en anti-programma's. Alle drie concepten benadrukken dat de grenzen tussen dader en slachtoffer, mens en machine, instrument en doelwit en fictie en werkelijkheid vervagen of wegvallen. De studie concludeert dat de geformuleerde

concepten nieuwe aanknopingspunten kunnen bieden voor de analyse van hightech slachtofferschap, maar ook dat deze concepten er toe uitnodigen om anders (meer hybride) te denken over belangrijke facetten van slachtofferschap, waaronder wie/wat slachtoffers kwetsbaar en weerbaar maakt en hoe preventiemaatregelen vormgegeven zouden kunnen worden.

De vier dimensies van het 'cyborg crime' perspectief

Op basis van de casestudies zijn vervolgens vier dimensies van het 'cyborg crime' - perspectief onderscheiden die waardevol zouden kunnen zijn bij de analyse van hightech cybercrime. Ze staan niet los van elkaar, maar liggen in elkaars verlengde. Het betreft de volgende dimensies:

1. Technologieën moeten beschouwd worden als actieve entiteiten, bemiddelaars of participanten in hightech cybercrime;
2. De relatie tussen daders van hightech cybercrime daders en technologie is meer dan slechts functioneel;
3. Daders van hightech cybercrime interacteren met technologieën waar ze mogelijk niet de volledige controle over hebben;
4. Dader- en slachtoffers van hightech cybercrime zijn hybride producten van menselijke, technische en/of virtuele (inter)acties;

Gesteld werd dat deze dimensies vooral als een aanvulling en niet als vervanging dienen voor het bestaande theoretische repertoire van de

criminologie. Ze leggen vooral de nadruk op de wijze waarop technologie criminele handelingen, processen en intenties en de resultaten daarvan kan medevormen, dimensies die nog (te) onderbelicht zijn in de criminologie.

Het toekennen van actorschap aan technologie roept uiteraard ook diverse vragen op, waaronder de vraag hoe technologisch actorschap in relatie staat tot het actorschap van de mens. Het 'cyborg crime' - perspectief volgt ANT in zoverre dat het in de analyse (in eerste instantie) evenveel aandacht wil besteden aan hoe menselijke en niet-menselijke entiteiten een rol spelen in handelingen en benadrukt eveneens dat beide in essentie niet hetzelfde zijn. Het 'cyborg crime' - perspectief zou echter wel iets meer ruimte willen toelaten voor een gedifferentieerde opvatting van menselijk en technisch actorschap door nader te specificeren op welke verschillende manieren technologie als actor kan fungeren. Het stelt derhalve dat een hybride opvatting van actorschap hand in hand kan gaan met (iets meer) herkenning van de eigenheid van mens en machine. Tot slot werd nog op mogelijke juridische en praktische implicaties van (het) 'cyborg crime' (-perspectief) ingegaan. Het cyborg crime perspectief betekent niet dat (een deel van de) verantwoordelijkheid moet worden afgeschoven op technologie in plaats van de mens, maar stipt wel aan dat bepaalde aspecten (bijvoorbeeld waar het gaat om het vaststellen van causaliteit) lastiger zouden kunnen zijn bij cybercrime dan bij traditionele criminaliteit. In het kader van de bestrijding van hightech cybercrime, veronderstelt het 'cyborg crime' - perspectief dat de aanpak gericht moet

worden op zowel menselijke als niet-menselijke actoren (infrastructuur, malware, tools, marktplaatsen, etc) en ook dat dat er een netwerk van actoren nodig is om deze vormen van criminaliteit te bestrijden.

ANT en cybercriminologie: mogelijkheden en beperkingen

Hoewel de ideeën van ANT aanvankelijk vergezocht leken, kwam naar voren dat het perspectief interessante aanknopingspunten biedt voor de studie van cybercrime, vooral als het gaat om de duiding van de relatie tussen mens en technologie. Ook biedt ANT de mogelijkheid om cybercriminele fenomenen met een minder dualistische bril te bestuderen. Een enigszins provocatief perspectief zoals ANT is tegelijkertijd geschikt in het kader van theoretische vernieuwing. Het stelt minder voor de hand liggende vragen en stelt ook in staat om kritisch naar bestaande concepten te kijken. Zoals het proefschrift heeft laten zien, heeft het ANT het 'nieuwheidsdebat' in de cybercriminologie zeker een nieuwe impuls geven. Toch zijn er ook beperkingen te signaleren waar het gaat om de toepassing of het gebruik van ANT. Zo heeft ANT weinig te melden over hoe mensen (los van de dingen) tot morele keuzes komen en ook is het maar de vraag of het realistisch en wenselijk is om als onderzoeker, zoals Latour dat voorschrijft, weg te blijven van interpretatie en alleen te beschrijven. Desalniettemin lijkt ANT, althans daar ben ik zelf van overtuigd geraakt, een zeer passend perspectief te zijn voor de studie van cybercrime. Ik verwacht en hoop dan ook dat cybercriminologen vaker een beroep zullen gaan doen op ANT of andere perspectieven binnen de filosofie van de techniek.

Toekomstig onderzoek zou aanvullende of nieuwe casestudies kunnen doen op het gebied van dader- en slachtofferschap en/of het 'cyborg crime' - perspectief op een grotere dataset kunnen loslaten om bevindingen uit dit onderzoek nader te valideren. Tevens zou het perspectief op andere cyber-gerelateerde thema's kunnen worden toepast, zoals cyberverkrachting en de rol van bots en botnets in de manipulatie van de publieke opinie.

Curriculum Vitae

Wytske van der Wagen obtained her Bachelor's and Master's degree in Criminology at the Vrije Universiteit in Amsterdam (2011). During her studies she conducted research on various topics, including public private policing (in the tacking of illegal cannabis cultivation), prostitution and (Russian) organized crime. In the scope of the latter she completed an internship at the Royal Dutch Embassy in Moscow in 2010. She also worked at the Ministry of Justice (WODC) as a researcher in different research projects, including a research on the experiences of young offenders in detention (2010). From September 2011 until August 2016, Wytske worked as a PhD-candidate and junior lecturer in Criminology at Groningen University at the Faculty of Law. Here she conducted her PhD research in the scope of cybercrime. Since September 2016 she has been employed as a university lecturer at the Erasmus School of Law, the Department of Criminology. Her current position is assistant professor at the same department.

Publications

Peer reviewed journal articles

- Schuilenburg, M.B. & Van der Wagen, W. (2011). Samenwerking in de criminaliteitsbestrijding. Kwalitatief onderzoek naar de integrale aanpak van illegale hennepteelt, *Tijdschrift voor Veiligheid, 10*(1), p. 10 – 25.
- Van der Wagen, W. (2018). Het 'cyborg crime' perspectief. Theoretische vernieuwing in het digitale tijdperk. *Tijdschrift over Cultuur en Criminaliteit,* (8)1: 19-34.
- Van der Wagen, W. (2018/*forthcoming*). The Cyborgian Deviant: An Assessment of the Hacker through Actor-Network Theory, *Journal of Qualitative Criminal Justice & Criminology*.
- Van der Wagen, 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.
- Van der Wagen, W., Daalder, A. & Bijleveld, C. (2010). Geld, spanning en aandacht: een verkennende studie naar Nederlandse hoogopgeleide sekswerkers. *Tijdschrift voor de Seksuologie*, *34*(3), p. 124-142.
- Van der Wagen, W. & Pieters, W. (2015). From Cybercrime to Cyborg Crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578-595.

- Van der Wagen, W. & Pieters, W. (2018/under review). The hybrid victim: re-conceptualizing high-tech cyber victimization through actor-network theory.

Book chapters

- Van der Wagen, W. (2013). Een Hybridisering van mens en technologie. Over nieuwe dynamieken in de studie van cybercrime. In A. Dijkstra, B.F. Keulen & G. Knigge (Eds.), *Het Roer Recht. Liber amicorum aangeboden aan Wim Vellinga en Feikje Vellinga-Schootstra* (pp. 323-336). Zutphen: Uitgeverij Paris.

(Contributions to) reports

- Everhardt, V., Van der Wagen, W., Trautmann, F., Bless, R., Ketelaars, T. & B. Keizer (2009). H. 12. Internationale Samenwerking. In *Evaluatie Nederlands Drugsbeleid*. Den Haag: Ministerie van Justitie (WODC).
- Ooyen-Houben, M. van, Bieleman, B. Biesma, S., Snippe, J., Van der Wagen, W. & A. Beelen (2009). H. 11. Drugsgerelateerde overlast. In *Evaluatie Nederlands Drugsbeleid*. Den Haag: Ministerie van Justitie (WODC).
- Wagen, W. Van der & Dimitrova, E. (2017). *Mission Cyborg: Op naar een hybride kijk op de bestrijding van cybercriminele (actor-) netwerken*. Driebergen: Dienst Landelijke Recherche, *Report.*

Book reviews

- Van der Wagen, W. (2016). *Book review of "Actor-Network Theory and Crime Studies: Explorations in Science and Technology".* Rutger University's Criminal Law, and Criminal Justice books. Available at: http://clcjbooks.rutgers.edu

Other

- Van der Wagen, W. (2018/*forthcoming*). Botnet, *Sage Encyclopedia of the Internet.*
- Van der Wagen, W. (2017). Cyborg crime: sciencefiction of sciencefaction? Blog, available at: http://www.crimeur.nl/cyborg-crime-sciencefiction-of-sciencefaction/
- Van der Wagen, W. (2015). Crime and the rise of the machines. Een criminologische analyse van een botnet, *LISA e-magazine,* nr. 4.
- Van der Wagen, W. (2011). *De integrale aanpak van de (georganiseerde) hennepteelt. Een kwalitatieve studie naar randvoorwaarden van samenwerking*, masterscriptie.
- Van der Wagen, W. (2011). *De Russische georganiseerde misdaad: wat er nog van over is en wat ons nog te wachten staat.* Zoetermeer: KLPD (Dienst I-Pol), rapport/scriptie.
- Van der Wagen, W. & Calster, P.J.V. van (2013). Actor-Netwerk Theorie: een nieuwe kijk op cybercrime? *Panopticon Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, *34*(3), p. 215-219.

- Wagen, W. van der & Calster, P.J.V. van (2012). Criminologie 2.0: over de worsteling met cybercrime, *Panopticon Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, *33*(5), p. 470 – 475.
- Weulen Kranenbarg, M., Van der Laan, A., De Poot, C., Verhoeven, M., Van der Wagen, W. & Weijters, G. (2017). Individual Cybercrime Offenders. In E.R. Leukfeldt (Ed.), *Research Agenda: The Human Factor in Cybercrime and Cybersecurity* (pp. 23-31). Den Haag: Eleven International Publishing.

Conference papers and guest talks (in the scope of PhD project)

- Common Sessions Study Program in Critical Criminology, presentation entitled: 'Breaking the boundaries between the human and the machine: analysing cybercrime through an ANT lens,' Kent University, Canterbury, 23rd of April 2018.
- Lecture series 'Revenge of the Bots. Digital Opinion Formation and Democratic Integrity, Guest lecture entitled: 'The Criminology of Botnets', University of Hamburg, 23rd of November 2017.
- Common Sessions Study Program in Critical Criminology, presentation entitled 'Deviants without borders? A cyborgian journey through the world of hackers,' Rotterdam, 3rd of December 2015.
- The European Society of Criminology (Eurocrime), 'The cyborg dimension of cybercrime: an ANT study on hacking', Porto, 3rd of September 2015.

- Cultural Criminology, presentation entitled: 'Can Hackers be Cyborgs? A technosocial analysis of hacking', VU University Amsterdam, 25th of June 2015.
- Lunch seminar Team High Tech Crime, presentation entitled: 'De cyborg dimensie van high-tech crime', Driebergen, 27th of January 2015.
- NVC Conference, presentation entitled: 'Cybercrime en de verweving van mens en machine: Een criminologische analyse van een botnet', Leiden, 12th of June 2015.
- Common Sessions Study Program in Critical Criminology, presentation entitled: 'Crime & the rise of the machines: A criminological analysis of a botnet', Hamburg, 5th of May 2015.
- Conference Understanding Cybercrime: Social Science Perspectives, presentation entitled: 'Actor-Network Theory and cybercrime: the non-human as an actor?' Erasmus University Rotterdam, 6th of November 2014.
- NVC conference, presentation entitled: 'From cybercrime to cyborg crime: Naar een hybride kijk op cybercrime,' Leiden, 14th of June 2014.