From cybercrime to cyborg crime

van der Wagen, Wytske

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.