From cybercrime to cyborg crime

van der Wagen, Wytske

Chapter 6

General conclusion and discussion*

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

6.1. Introduction: the departure of the journey

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

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

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

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

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

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

6.2. Key findings from the case studies

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

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

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

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

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

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

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

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

6.2.2. The other 'others' (chapter 3)

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

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

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

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

6.2.3. The cyborgian deviant (chapter 4)

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

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

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

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

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

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

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

6.2.4. The hybrid victim (chapter 5)

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

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

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

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

6.3. Arrival: The ANT-based cyborg crime perspective

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.4. Critical reflection on the results

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

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

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

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

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

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

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

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

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

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

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

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

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

6.6. Possible legal and practical implications

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

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

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

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

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

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

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

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

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

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

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

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

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

6.7. Opportunities and possible pitfalls of travelling with ANT

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

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

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

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

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

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

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

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

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

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

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

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

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

6.8. The journey continues: future research directions

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

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

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

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

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

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