Article

The Significance of ‘Things’ in Cybercrime

How to Apply Actor-network Theory in (Cyber)criminological Research and Why it Matters

Wytske van der Wagen
Erasmus University

Abstract In recent years computer technologies and digital devices have become ubiquitous in all facets of human existence, including crime and deviant behavior. Various forms of criminality have emerged in which technical entities play a substantial role. It can be argued that such a development urges criminologists and anthropologists to draw more attention to the significance of things in crime. Latour’s (2005) actor-network theory (ANT), which considers non-human entities as active participants of the social, could be a useful approach for extending our analytical focus to the non-human. The article will not only asses why, but also *how* we can apply ANT as a more-than-human methodology in qualitative research, by discussing three ANT-based methodological principles: ‘follow the tool’, ‘follow the hybrid’ and ‘follow the network.’ In this scope, this article draws on earlier conducted qualitative ANT case studies on different forms of high-tech cybercrime. In a more general vein, the article aims to show that innovations in qualitative research methods can be also informed by theory.

Keywords Actor-network theory, cybercrime, qualitative research methods, non-human agency

> *ATLANTA (March 2018) — The City of Atlanta’s 8,000 employees got the word on Tuesday that they had been waiting for: It was O.K. to turn their computers on.*
>
> *But as the city government’s desktops, hard drives and printers flickered back to life for the first time in five days, residents still could not pay their traffic tickets or water bills online, or report potholes or graffiti on a city website. Travelers at the world’s busiest airport still could not use the free Wi-Fi.*
>
> *Atlanta’s municipal government has been brought to its knees since Thursday morning by a ransomware attack — one of the most sustained and consequential cyberattacks ever mounted against a major American city.*
>
> *The digital extortion aimed at Atlanta, which security experts have linked to a shadowy hacking crew known for its careful selection of targets, laid bare once again the vulnerabilities of governments as they rely on computer networks for day-to-day operations.*
>
> *(Alan Blinder and Nicole Perlroth, The New York Times, March 2018)*

The above newspaper article shows how devastating cyberattacks such as ransomware can be. Our lives have become so dependent on and intertwined with information and communication technology (ICT) that one single attack can paralyze the infrastructure of an entire city for days. The news article is also quite a clear contemporary illustration

DOI: http://dx.doi.org/10.5617/jea.6895
Journal of Extreme Anthropology, 2019, 3(1): 152-168, 2535-3241

of Bruno Latour's claim that various incommensurable elements, ranging from local cities to the World Wide Web, from governments to businesses, from hard drives to water bills, are all caught up in the same story (Latour 1993; 2005). A cyberattack can only be fully understood when we look at the various human and non-human entities that bring it together and when we consider their multiple associations. Furthermore, the article reveals the significance of 'things.' When objects like our computers or printers stop working they can cause a lot of trouble for humans, even drastically disrupt public life. It then becomes questionable, as Latour argues, whether we can view these things in a passive or mundane way (Latour 1992; 2005). They can permit, afford, support, enable or *disable* various activities we, humans, are involved in. Should we then not consider them as full-blown actors just like humans, as Latour argues?

Latour's plea for a more active treatment and consideration of 'things' in the social world and even granting them with agency has received praise, but also a lot of criticism (Vandenberghe 2002). Whether one agrees with Latour or not, it can be argued that his vision in respect to the significance of things is worth (re)considering in light of current cybercrime developments. In high-tech cybercrimes, such as ransomware or botnets, 'things' obviously play a prominent role in the commission of the crime. At the same time, we might be dealing with a different *kind* of things than those Latour and his associates[59] were referring to in their formulation of actor-network theory (hereafter ANT), such as hammers, seat belts, automated doors and guns. For example, most types of malicious software can replicate themselves without any human interventions and what (malicious) digital tools can do or cause in cyberspace is often not very predictable. This suggests that we criminologists and anthropologists might need to think differently about the relationship between the human (the perpetrator) and the machine.

In my dissertation, I argued that we should move beyond an anthropocentric view in criminology and treat nonhuman entities as more active participants in the study of high-tech cybercrime (Van der Wagen 2018a). Current studies in the field of cybercrime, whether positivistic or constructivist, still tend to place the human agent at the center of the criminological inquiry. Criminology, and the same goes for anthropology, also lacks a set of concepts that would enable us to study the agency of non-humans in crime and deviant behavior. Especially when we want to study the more high-tech cybercrimes like ransomware and botnets, crimes that are still underexplored in both criminology and anthropology, such framework becomes necessary. Against this background, I explored whether the constructivist lens of ANT, which *does* provide concepts for analyzing the role of non-humans, could be a valuable approach for the study of cybercrime. Based on my theoretical and empirical analysis, I concluded that ANT can enrich the theoretical repertoire of (cyber)criminology. In my engagement with ANT, however, I encountered that using the approach in empirical research is quite a methodological challenge. ANT studies provide methodological tools, but they remain still rather vague when it comes to praxis and are not particularly dedicated to (cyber)criminological research. Existing criminological literature does not offer much

---

[59] Actor-network theory is not solely the intellectual legacy of Latour, but also of his contemporaries including Michel Callon, John Law and Annemarie Mol. It is also important to stress that ANT is not a coherent and unified framework. The current article mainly (not only) discusses the ANT perspective of Latour.

guidance either. While various authors, including myself, have examined the theoretical potential of ANT for the study of crime (see e.g., Robert and Dufresne 2015), they do not extensively address the *methodological* aspect of engaging with ANT (e.g., Nimmo 2011; Sayes 2014; Adams & Thompson, 2011). In criminological handbooks on qualitative research methods, we rarely find any substantial text on ANT as a methodology. Therefore, it remains unclear how we can study the role of non-human entities in qualitative criminological research. How can we treat them more 'actively' in our analysis? How many and which non-humans should we include and what type of data is suitable for an ANT analysis? Is ANT a methodology in itself or should we interpret and use it as an extension of existing methods?

This article aims to enhance our knowledge about how a more active treatment of non-human entities in our analysis of crime and deviant behavior – as propagated by ANT scholars - can be accomplished, with a special emphasis on the study of high-tech cybercrime. The main research question of this article is then: How can ANT be applied as a *methodology* in qualitative research on crime and deviant behavior, high-tech cybercrime in particular, and what is the added value of such a 'more-than-human' approach? As will become clear in this article, departing from the constructivist angle of ANT also entails that this study employs a distinct approach to the question of what *is* cybercrime. Rather than perceiving cybercrime as crime carried by a human agent *using* ICT (e.g. Yar 2013), it defines cybercrime as illicit activities (or activities conceived illicit by certain parties) carried out by networks of (multiple) human and non-human entities. This entails that the unit of analysis is not the human nor ICT but a hybrid of both.

In a more general vein, the article aims to show that innovation in research methods can also be informed by (innovation in) theory. The article first briefly discusses whether and how existing approaches in criminology provide analytical tools for including non-human entities in qualitative inquiry. Then it discusses ANT's understanding of non-human agency and the ensuing methodological principles. Hereafter the article discusses how these methodological principles can be applied in qualitative research on cybercrime. In this scope I also draw on concrete examples from (mainly) my own qualitative case studies in which ANT was used. This section is divided in three subsections: 'follow the tool', 'follow the hybrid' and 'follow the network'. The article ends with some concluding remarks.

Studying the 'Non-human' in Qualitative Criminological Inquiry

Do We Actually Need ANT?

Before discussing ANT in greater detail, we should briefly consider whether and how existing frameworks that are influential in both offline and online qualitative research offer theoretical and methodological tools for studying the role of the non-humans in crime and deviant behavior. How do existing approaches, in a nutshell, conceptualize the role of non-humans in social life? How does ANT relate to these approaches and what is it doing differently?

As Dolwick points out, how frameworks theorize the role of non-human entities in the social is interconnected with the broader question of how they define the 'social' in the first place (Dolwick 2009). He places existing frameworks on a continuum from a narrow to a broad definition. Theorists who define 'the social' in terms of 'social structures' and 'social facts' (e.g. Durkheim) maintain the narrowest, most restricted and purest definition of the social and treat non-humans as passive, mundane and irrelevant for social analysis (Dolwick 2009). In Latourian terms, they are the ultimate 'sociologists of the social' (Latour 2005).

The next set of approaches, involving phenomenological and symbolic interactionist approaches – the 'root perspectives' of the qualitative criminological research tradition – can be grouped in the category of frameworks that adopt a less but still narrow and restricted meaning of the social. They consider the 'social' as 'what occurs when meanings and representations are passed from person to person' (Dolwick 2009, 22). The social then refers to 'human aggregates' or 'humans-among-themselves', entailing that the role of material objects or things is merely considered in terms of symbolic representation. In symbolic interactionist approaches this is reflected in concepts such 'intersubjectivity' and 'meaning making' (idem). Theorists such as Goffman examine, for example, how material objects play a role in face-to-face interactions and various types of social encounters – e.g. material objects such as furniture are part of the decoration of the front stage and items such as clothes can be seen as part of the 'expressive equipment' that people use for presenting themselves (Goffman 1959). However, the work of Goffman is not only restricted to the symbolic or expressive meaning of things. He also drew attention to how the *materiality* of certain objects can shape social interactions – for instance, in his work on the merry-go-arounds as a technical system shaping the relationship between riders and fellow riders and their audience (see Pinch 2010). Although the material dimension of the social is taken into consideration, symbolic interactionism is at its core still mainly human-centered. The interpersonal relationships between human 'performers' (with or without material objects) are the main unit for qualitative inquiry.

Similarly, phenomenology, which is at the same time a more philosophical orientation, views humans as the superior actors in the universe. This is reflected in concepts such as 'transcendental ego' (e.g. Sartre 1960 [1937]), 'Dasein' (Heidegger 1962; 1982) and 'lived experience' (e.g. Schutz 1967). Phenomenology pleas for the revival of the 'living contact with the world and to return to concrete, lived human experience in all its variegated richness' (Adams & Thompson 2011, 736). However, like symbolic interactionism, phenomenological theorists do not neglect the role of non-humans in social life either. They view material objects as entities that play a role in how humans experience and reflect upon the life world. They are conceived as 'things' that can co-shape human perceptions, emotions, spirituality and so on. Despite this attention paid to the human engagement with the material world, the central unit of analysis remains 'how humans are involved in their lifeworld'. Non-human entities are treated as the subordinate entities in the analysis (idem).

Now ANT, known for placing human and non-humans on a more equal level playing field, comes into the picture. ANT can be placed at the other extreme of the continuum, having the broadest understanding of 'the social'. For ANT, the social refers to 'association' – anything and everything that assembles together, including animals, plants and material objects (Dolwick 2009; Latour, 2005). Subsequently, its focal point is also the gathering or assemblage of many different 'non-social' elements. In ANT's social universe there are neither human nor non-human aggregates only hybrids of both. Let us now look in more detail into this line of thinking.

Actor-network Theory: Theory or Method?

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

Actor-network theory emerged already 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. ANT is not really a 'theory' of the social. 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). In this respect ANT is more a methodology of *how* to study the social than a theory *of* the social. The term 'theory' is therefore somewhat 'misleading', which also counts – as Latour argues himself – for the words actor, network and the hyphen (Latour 1999). ANT 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 and Jensen, 2011). As announced earlier, this article mainly focuses on the issue of non-human agency. This concerns a matter that has been a major source for debates and misunderstandings alike. For instance, some authors argue 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). Other scholars are skeptical about the fact that Latour gives so much credit to non-human entities in what they can bring about (e.g. Amsterdamska 1990). She finds it absurd that the approach does not differentiate between human and non-humans in their role/contribution to successes and failures. I, however, believe that the ANT principle of ontological symmetry does not automatically make ANT anti-human(ist) (see also Kipnis 2015; Latour 2013). I also think that the type of agency 'given' to non-humans by ANT theorists is more nuanced than often presented by the critics. Below I provide a comprehensive though brief outline of ANT theorists' view on non-human agency and related concepts and thereafter discuss the methodological implications of such a 'more than-a-human' approach.

ANT, like other constructivist approaches that call for a material turn or 'turn to things' (e.g. Preda 1999), claims that things, from small tools to large technical systems (see Sayes 2014), should be placed more in the forefront of sociological theory for the reason that they play an active role in the production of the social. As Mol explains: ANT '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). ANT theorists presume that objects have a crucial function in the interaction between people, but they also interact with humans and with other non-humans. For ANT theorists, things are also more than just 'instruments' or 'commodities' (e.g. Latour 1992; Latour & Venn, 2002): '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' (Dolwick 2009, 41). It is important to stress that ANT approaches do not argue that objects have a will of their own or have an intentionality or consciousness in the same manner as humans. They might however act differently than expected or generate a different outcome than anticipated – which is why they can be seen as actors or *mediators* in certain situations rather than (functional) *intermediaries* (see also Latour and Venn, 2002; Latour, 2005).

Along the same lines, ANT argues that agency 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, the 'car-human' hybrid that drives and not merely the human actor (see also Dant 2004; Lupton 1999). Accordingly, ANT scholars do not approach agency, morality and intentionality from a 'dualist paradigm that locates human beings and technological artifacts in two separate realms, humans being intentional and free, technologies being instrumental and mute' (Verbeek 2014, 75). Like other approaches in philosophy of technology that view the role of technology in terms of mediation, ANT does not view the role of technology in either deterministic or instrumental terms, but positions itself somewhere in between those extremes. ANT theorists 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). 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).

Another important aspect of ANT's understanding of the social, related to the above aspect, 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. Such a semiotic understanding of reality (Law 1999) not only dissolves dualisms (Gad and 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 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' (Mol 2010, 257-258). 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/actants) that produced them rather than by looking at some external causal force (idem). When we for example look at the ransomware attack mentioned in the introduction of this article, we can say that the city was 'offline' for quite some days due to the ransomware attack. However, in order to fully capture the causes, scope and impact of the attack, it is important to look at all the (interconnected) actors involved.

Methodological Implications of ANT's 'More-than-human' Approach

As outlined above, the standpoints of ANT theorists are not merely theoretical – or perhaps not even theoretical at all[60] – they also suggest, which is actually the *main*

---

[60] ANT does not include any statements about the nature and extent of non-human agency. Instead, it presents the issue of non-human agency as an 'uncertainty' (Latour, 2005), some 'thing' that we have to take into account when we conduct empirical research (see further Sayes 2014).

message, to do qualitative research differently and to adopt less-human-centered methodologies (Dowling, Lloyd and Suchet-Pearson 2017; Sayes, 2014).

When it comes to the application of specific research methods, Latour generally prefers ethnographic fieldwork to other methods for the reason that this type of research more profoundly enables us to capture what actors themselves have to say (Latour 2005; Law 2004). The latter is a key objective of ANT-based research. As Latour puts it: 'The task of defining and ordering the social should be left to the actors themselves, not taken up by the analyst' (Latour 2005, 23). In this respect ANT follows, at least for the most part, the earlier discussed interactionist approaches, which also seek to produce a rich account of the world of the actors under study and to learn from them. Both ethnographic researchers and ANT-scholars are particularly interested in people's everyday actions, activities and behaviors and want to describe these in all their complexity. They 'eschew neat analytic categories in favour of a sensitivity to messiness, contingency and non-coherence; both acknowledge the heterogeneity of practices and their interweaving of the social and the material; both are broadly inductive and place an emphasis on the detailed description of what takes place 'on the ground' (Nimmo 2011, 113).

ANT is, however, slightly more radical when it comes to describing what is taking place on the ground. ANT's so-called 'radical descriptivism', involves that the researcher has to completely abstain from any interpretation. As Krarup and Blok explain: ANT seeks to make a shift from 'theoretically interpreting human actions to obstinately 'following the actor' by tracking and mapping its multiple associations' (Krarup and Blok 2011, 43). This shift or view clarifies why Latour does not view ANT as a framework one can 'apply.' In a dialogue between a professor and a student, Latour 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' (Latour 2004, 64).

The other difference between ANT and other interactionist approaches, as discussed already, is the fact that ANT theorists assign a more active role to non-human entities and thus also consider them as qualitative research participants (Adams and Thompson 2011). Methodologically this entails that the starting point in every ANT analysis should be that non-human objects (e.g. a gun, a hammer, a piece of paper or a computer) need just as much analytical attention as humans receive, at least *initially*. As Latour puts it himself: 'ANT is not, I repeat is not, the establishment of some absurd "symmetry between humans and non-humans". To be symmetric, for us [ANT theorists], simply means *not* to impose a priori some spurious *asymmetry* among human intentional action and a material world of causal relations' (Latour 2005, 76). Only afterwards (after following the actors), we can pinpoint the (network of) various actors in the story and their role and contribution (Mol 2010). An entity is then 'labeled' as an actor when it makes a difference, mediates, changes a certain state of affairs or brings some surprises or disturbances. In other words, rather than taking the human as 'the "standard measure" of agency, the "standard measure of agency" becomes dehumanized: the ability to make a difference' (Sayes 2014, 141). Apart from following both human and non-human entities, the ANT researcher should be sensitive to how non-humans can shape, affect, enable or disable certain actions, processes and outcomes.

ANT's symmetrical approach has been a main source of criticism. Krarup and Blok (2011), for example, point out that Latour's view places too much emphasis on the role of non-humans in the social. Although Latour recognizes that morality is not solely constituted by tools or objects alone, he has little to say about the human or subjective dimension that co-shapes moral decisions. According to these authors, ANT is not symmetrical enough. The counterargument that I would like to bring up is that the added value of ANT lies exactly in its attention to the active and even person-transformative abilities of non-humans. It fills an important blind spot of (most) approaches (also in criminology and anthropology) that are located at the other 'human-focused' extreme. Placing too much emphasis on the agency of non-humans on the other hand, might indeed run the risk of applying a too strong sense of symmetry or head to the 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 and Hassard 2004, 494).

Studying the Significance of 'Things' in Cybercrime

Now that we have a general idea of the theoretical and methodological assumptions of ANT, we move to the question of how such an approach could be applied in criminological research, high-tech cybercrime research in particular. At first sight, we could say that ANT's notions should not work out that much differently in the analysis of cybercrime. In cybercrime/cyberspace, obviously various human and technical entities gather together in the commission of the crime. At the same time, it can be argued that we might be dealing with non-human entities whose properties or 'abilities' are somewhat different than the physical tools or entities Latour was referring to such as guns and automated doors. This in turn might either strengthen or alter certain theoretical and methodological notions held by ANT theorists. Below, I will discuss three ANT-based interconnected methodological principles that can be applied in cybercrime research which are based on ANT's more general principle of 'follow the actor', namely: 'follow the tool', 'follow the hybrid' and 'follow the network'. Each subsection first outlines why we should apply this methodological principle in cybercrime research and thereafter provides leads for the data and methods that can be used. I will draw on examples from the literature and on three earlier conducted ANT case studies (Van der Wagen & Bernaards 2018; Van der Wagen 2018b, Van der Wagen and Pieters 2015). I refer to these case studies for the aim of illustrating how we can include non-humans as research participants and why it matters.

Follow the Tool

As outlined before, ANT assigns a more active role to non-human entities in the course of action for the reason that they can provoke, shape, enable or disable certain actions. In many cases, tools are not merely tools. Take, for example, the 'delete button', which we press when we want to remove things and move on. As Adams and Thompson point out, such a button is not just a tool for deletion: 'when we accept its invitation, we enter into a socio-material assemblage: we are "deleting" and we could not do this without our delete button' (Adams and Thompson 2011, 738). When we follow tools such as delete buttons and assess how they (dis)assemble with human actants, we get a better grip of what role they play in particular practices and activities, like writing a scientific article for example! For the qualitative researcher it invites questions such as what are the affordances of the tools? What does the tool do in specific actions?

It can be argued that digital tools that are used by cyber offenders bring a new aspect into play since they have a less clear-cut functionality than tools such as delete buttons. One of those aspects is related to foreseeability. Lehman et al. for example reveal that computer programs are inherently unpredictable in terms of what they will do: 'the outcome *cannot* be predicted without actually running it [the program]' (Lehman et al. 2018, 5). The authors provide an overview of examples in which computer programs produced unanticipated (strange, surprising or creative) results. They concluded that digital or artificial entities (like biological ones) can subvert human expectations and intentions. A level of unpredictability can also be found in the use of malicious computer programs. Although the script or functionality of a certain malicious tool might be quite fixed - e.g., the script of a distributed denial of service (DDoS) attack-tool (termed 'booter' or 'stresser') will most likely be: 'send a lot of traffic to a server in order to paralyze it' – how much damage will be done is not predictable in advance. Hence, with cybercrime, more than with any other crime, we should not only follow the actions of the human actor that carries out the crime, but also study the role, contribution or even the *agency* of the tool. Treating tools as research participants 'helps researchers catch glimpses of objects in motion' (Adams and Thompson 2011, 738) which is particularly relevant in the scope of cybercrime research, where it is more likely than in the physical world, that an entity goes rogue. As Balzacq and Dunn Cavelty 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' (Balzacq and Dunn Cavelty 2016, 183).

The follow up question is then how to 'follow the tool': which data and which qualitative research methods could be suitable? Of course, we are social scientists and not computer scientists and are thus not able to study the more advanced features or the entire 'life cycle' of cyber tools or malware. Instead, we could draw more attention to how such tools co-shape criminal practices in terms of enabling, disturbing, inviting and so on. To illustrate how, I would like to refer to a case study (Van der Wagen & Bernaards 2018) in which private chat conversations between cyber offenders involved in the spread of banking malware, botnets, fraud and other financial cybercrimes were analyzed. In the analysis, we drew explicit attention to the role of the tools in their encounters. What role do they play in these crimes? What problems do offenders face in respect to the tools? How do offenders speak about the tools that they use? By analyzing the data through this angle, we found out that certain non-human entities play a more fundamental and active role in cybercrime than merely being a tool facilitating the crime. For example, they can cause disturbances in carrying out the crime (technical problems) – and hereby altering the modus operandi, decision-making and successes of the offenders – and can cause friction in the cooperation among the involved offenders as well (e.g., the purchased malware or tool does not do the job). Interestingly, we also found indications that offenders themselves consider tools more than just tools. They sometimes speak about tools as if they are 'living creatures', visible in formulations such as 'the tool is dead or alive'. In other words, by applying the principle of 'follow the tool' we can unravel what the tools concretely *do* in a crime event and accordingly, we might be able to unravel certain crime dynamics more profoundly, including the coincidences, transformations and translations that unfold in the course of criminal events. These might stay 'black-boxed' if we would consider the tool as a passive and mundane entity and consider the human actors as the only significant agents. Such a principle can be also applied in the scope of other types of data and research settings. We could, for example, study cybercriminal forums where all the ins and outs of tools are discussed or examine actual cybercriminal cases by analyzing police files. High-tech crime police investigations contain quite some information about what tools were used and how they co-shaped the criminal process (see further section 'follow the network').

Follow the Hybrid

Closely related to the previous methodological principle of follow the tool, which emphasizes that we have to treat tools as research participants, we can distinguish the principle of 'follow the hybrid' alias 'follow the cyborg.' As discussed before, ANT presumes that actions are carried out by hybrids of human and non-human entities. It thereby constantly reminds the researcher 'that research is always likely to encounter conglomerates or hybrids of action rather than pure entities' (Gad and Jensen 2010, 75). Humans never act alone, our actions are always intertwined with and shaped by other non-human entities such as credit cards, pencils, books, cars, cigarettes, guns and so on. They also affect how we behave and feel, which e.g. becomes clear when we look at the act of driving a car (see Dant 2004; Lupton 1999). As qualitative (ANT) researchers we then have to include such influences in our studies as well. Methodologically, this entails not only focusing on interpersonal relationships (which is the focus of symbolic interactionists), but also assessing how humans relate to and interact with non-humans. In this respect we can learn from education researchers who, for example, analyze how tools or software like Power Point shape the performance, knowledge and experiences of educators. The educator is perceived as an agent that is '*caught* up in the particular design imperatives, decisions, and suggestions in this software [Power Point]' (Adams and Thomson 2011, 740). According to these authors, you have to include the 'invitational quality of things' in your analysis. You should not only look at what the object does, but also 'listen' to what objects themselves have to 'say' (e.g. water invites/screams for a swim and sand cries out for digging). In any case, 'follow the hybrid' implies that the researcher has to focus on how human and non-human entities mutually shape one another's actions by taking the invitational properties of objects into account.

Such a principle seems to be definitely valuable in the scope of cybercrime research as well. In cybercrime, offenders constantly use, interact with, depend on, create and/or attack all kinds of non-human entities. However, there is also a difference here. Rather than being engaged with software such as Power Point, a program that basically has quite a straightforward use and functionality, cyber offenders engage with digital entities/computers/programs that are more transformative and adaptable and less static. This latter aspect I also found in my own study of the hacker phenomenon (Van der Wagen 2018b), for which I conducted 10 interviews with hackers. When hackers speak about tools that they use or create, they tend to emphasize the transformative qualities of the software: *'Every hacker has his weapons tank with his own tools he has chosen to use. Usually you use an already created and existing code someone else has written and you adapt it to* *your problem.'* The interviewed hackers also described their relationship with technology in terms of an interplay ('what will it do when I do this', 'playing-wise you have to learn how to hack'), spoke in terms of a trial and error, and also mentioned that they got feedback from the system itself. These findings are mirrored in Turgeman-Goldschmidt standpoint that 'despite (or because of) the fact that the computer is a machine, it invites play and movement' (Turgeman-Goldschmidt 2005, 20; see also Turkle 1984). In other words, hackers seem to experience that they do not act alone, but in close alliance with the tool (see further Van der Wagen 2018b). Accordingly, the principle of 'follow the hybrid' stresses that we should neither merely study the offender nor the technology, but take a look at hybrid configurations of both. This enables the researcher to more profoundly grasp the relationship between the human and the machine.

The next question is then how to 'follow the hybrid'. Which data and which methods could be suitable for studying offender-technology configurations? It can be argued that the 'human-tool hybrid' or the 'hacker-software hybrid' can be studied in various ways. We could simply interview offenders and ask them to talk about the tools that they use, buy or create, why they use it, how they interact with it and so on. We could also ask them to describe what they do and how they give meaning to their actions, which is the approach I took in my own study of the hacker phenomenon. Such detailed descriptions can offer rich insights into the process of how hackers and tools mutually shape one another's actions. The most ideal way of applying the 'follow the hybrid' principle, however, would be to literally follow and observe hackers aka 'hacker-tool hybrids' in their practice and produce a rich account of what they are doing. This approach fits best with ANT's preference for doing ethnography extended to non-humans, but might be a challenge to accomplish. Although the principle of 'follow the hybrid' is suitable for online research setting (e.g. hacker forums), it might be also suitable for offline research (e.g. conducting research in hacker spaces where hackers tinker with software, hardware and all kinds of electronics).

Follow the Network

As discussed earlier, ANT presumes that relational and heterogeneous networks of human and non-human entities produce actions rather than 'solistic' actors. It does not a priori make a distinction between what is human or technical, everyone and everything is treated as a hybrid collective of multiple interacting elements and should be studied as such (Latour 1993; 2005), which also explain the hyphen between actor and network. Graham Harman provides an analogy that captures the idea of 'following the network' fairly well: 'We cannot discover the nature of a thing by looking into its heart, but must follow the blood that circulates from that thing through all its arteries and far-flung capillaries' (Harman 2007, in Adams and Thompson 2011, 738). 'Following the network' does not entail that we have to map all possible entities in a network/actor-network, but to search for the 'mediators' that make a difference (Latour 2005). This can only be determined afterwards and is different in each single case. 'Every time a new case is considered it suggests different lessons about what "an actor" might be' (Mol 2010, 257). Exactly here also lies the methodological challenge of following the network: where to begin and where to stop? Which actors to include and to exclude (Adams and Thomson 2011)? ANT scholars do not provide very clear guidelines in this respect, but want to encourage researchers not to select the actors beforehand.

It can be argued that the principle of 'following the network' is very valuable and applicable in the scope of cybercrime as well. To illustrate this point, I would like to refer to a different case study in which a large-scale botnet was studied based on the analysis of police files (Van der Wagen and Pieters 2015). In this study, we were mapping the human and non-human entities involved in the botnet. We showed that a myriad of human and technical entities was involved in (shaping the) various stages of the botnet, from the initiation (creation of the botnet) to the dismantling (taking it down). Putting an end to this botnet required a dismantling of the entire offender-technology conglomeration: arresting the human botherder, taking the infrastructure offline (in this case a very complex network of different interconnected servers) and ending the infections of all the compromised computers. When this would not have been done properly, the crime and harm would go on. The latter occurred in some later botnets, which I did not study. The so-called 'Avalanche' botnet and the 'Conficker' botnet remained active, despite the fact that the human controller(s) were arrested and the infrastructure was taken down. Through a so-called 'peer-to-peer' construction, the infected machines kept infecting other machines, keeping the botnet active (Security 2018). This example shows that in cyberspace technical entities may eventually also lead a 'life' on their own, establishing new relationships with other human and technical entities and then generate new crimes. Following the network then requires the qualitative researcher to examine the grouping and re-grouping of such hybrid networks.

When it comes to the question of how to apply the principle of 'follow the network' in the analysis of crime, there is no straightforward answer. As mentioned already, you cannot escape from making choices when it comes to which actors in the network to follow and where to start. In the earlier mentioned case study in which chat conversations between offenders were analyzed (Van der Wagen & Bernaards 2018), we had access to millions of chat lines. We obviously had to start somewhere, but also to choose a starting point that fits within an ANT-based methodology. Accordingly, we decided to start with the technical entities rather than the human ones, which is also in accordance with the earlier discussed principle of 'follow the tool'. We started by collecting and analyzing all of the conversations in which the keyword 'bot' or 'botnet' was used, since these entities/networks are an essential component in many types of cybercrime. From here, we sought to follow the (network of) human and non-human actors that were involved in the botnet and the related activities and assessed how all the human (e.g. botherders, crypters, spammers and coders) and non-human entities (e.g. servers, exploit kits, exploits, malware, files, passwords and so on) were interconnected in the cybercriminal chain.

Follow the network can be also applied in the analysis of police files, the approach we took in the other botnet study (Van der Wagen & Pieters 2015). Such files are actually quite suitable for mapping networks of human and non-human entities. Such investigations, although they do not always provide the full picture of all events and are eventually produced by humans (see also Nimmo's (2011) discussion on the use of historical texts as data in an ANT study), include quite some information on how both human offenders and tools or other non-human entities are assembled together. They also provide more or less a chronological description of what occurred over time, enabling us to study the grouping and regrouping of networks of entities (in this case the creation, maintenance and 'death' of the botnet). We could even say that police detectives are actually involved in 'a more-than-human methodology' themselves. They have to establish all the connections between the human (the offenders) and the non-human elements (e.g. IP addresses, mail accounts, exploit kits, pay pal accounts) in order to construct the criminal fact and present the evidence.[61] Hence, such data is definitely useful in an ANT study of cybercrime. Of course, the ANT researcher should keep in mind that the mapping of the network of human and non-human elements by police officers serves the ultimate purpose of capturing the *human* offender, who they consider as the primary agent within the network. The ANT researcher decides who/what the actors are after mapping them all.

Concluding Remarks

As qualitative researchers we always seek to find novel and innovative ways of conducting research, especially when we are confronted with new research subjects. Cybercrime, especially high-tech cybercrime, is one of those phenomena that bring new challenges, both for our theories and methods. These crimes are very technical in nature, involving that various technical entities (e.g. exploit kits, malware, stressors) play a key role in the commission of these crimes. As a consequence, our existing anthropocentric frameworks, which are mainly preoccupied with studying human agents and human interactions, seem to be not completely suitable anymore. As discussed in my dissertation (Van der Wagen 2018a), actor-network theory could be a valuable alternative to consider in the scope of cybercrime research. ANT provides a way of thinking that treats (technical) 'things' in a more active way and also promotes a less anthropocentric and more hybrid and complex way of grasping the phenomena that we study. ANT's theoretical notions, specifically those concerning the role of non-human agency, can be positioned in the scope of 'mediating approaches' in the field of philosophy of technology, while methodologically ANT fits in the tradition of ethnography. This makes the approach to some extent quite unique, but difficult to grasp at the same time. As many scholars before me (including Latour himself) have also pointed out, getting engaged with ANT is not a clear-cut or pre-definable path. The main instruction you get as a researcher is: go into the field and just 'follow the actor' and make sure that your notebook is filled with maps and traces of various human and non-human actants, their connections, disconnections and so on.

This article addressed what such a 'more-than-a-human' methodology might look like in practice, by discussing three ANT-based methodological principles in light of findings from my own case studies in the field of cybercrime. 'Follow the tool' incites researchers to look at the active role of non-human entities in criminal actions and events, presuming that cybercriminal events are not merely orchestrated by human offenders. 'Follow the hybrid' aka 'follow the cyborg' sensitizes the cyborgian nature of cyberoffending: it helps to identity the various way in which offenders and technology configure together (become one). 'Follow the network' resembles the principle that we have to map the range of human and non-human actors involved in the story, which enables to capture the complexity of the phenomenon under study. Obviously, these

---

[61] Obviously, this principle of mapping the connections between humans and non-human and starting of things themselves also applies to traditional crimes such as murder in which police officers e.g. have to connect a murder weapon with a human agent.

principles are complementary and not mutually exclusive. They can also be applied in the analysis of different types of data ranging from interviews, (online) observations to police files.

Of course, there are also some critical questions or issues to address when it comes to the more-than-human methodology as propagated by ANT. Does ANT truly bring you to different places that cannot be reached by using more conventional methods? Based on my own research, I would say that ANT is definitely able to explore new paths, to add a new dimension to existing methods and to put things into a different perspective. Its hybrid and symmetrical view of agency is particularly valuable in cybercrime research, since it enables to look at both the role of human and technical entities in shaping these crimes. However, this does not mean that I consider ANT as a 'theory of everything' or a 'magic method' that is able to get it all right. Instead, I consider ANT as a lens – a 'hybrid' of theory and method – that is particularly suitable for shedding light on certain dimensions that are crucial in grasping high-tech crime and deviant behavior, as outlined in this article. It is complementary to existing qualitative methods that we already employ and can enrich and broaden our focus. I think qualitative criminological researchers, not only those that are involved in studying cybercrime, should take ANT more seriously and further assess it possibilities and value. As I tried to demonstrate in this article: innovation in research methods can be informed and accomplished by innovations in theory as well. However, the opposite is also true, especially in the case of ANT. As Sayes points out: 'by foregrounding the role of methodology, we better understand what it means to say that nonhumans have agency' (Sayes 2014, 144).

Obviously, granting agency to non-humans might also have some social implications. For example, it definitely raises questions about responsibility and guilt. Does ANT's hybrid conception of agency take the blame away from the human agent? Verbeek provides a clear answer to this issue by arguing that it 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' (Verbeek 2014, 80). Indeed, I would also not like to 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. 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 would 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 all actors and actions that led to the eventual outcome? ANT does not (aim to) provide clear answers to questions related to intentionality and responsibility (see also Sayes 2014 on this matter), but it can serve as a suitable approach to exactly unravel the complexity of cyber-crime events and to map and reconstruct the involved network of (human and non-human) entities. It *then* becomes again a matter of methodology.

Adams, Catharina A., and Terry L. Thompson. 2011. "Interviewing objects: including educational technologies as qualitative research participants." International Journal of Qualitative Studies in Education 24:733-750.

Amsterdamska O. 1990. "Surely you are joking, Monsieur Latour!" Science, Technology & Human Value 15:495-504.

Balzacq, Thierry and Myriam Dunn Cavelty. 2016. "A theory of actor-network for cyber-security." European Journal of International Security 1:176-198.

Blinder, Alan and Nicole Perlroth. 2018. "A Cyberattack Hobbles Atlanta, and Security Experts Shudder." The New York Times, March 27, 2018, accessed April 10 2019.https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer

Dant, Tim. 2004. "The driver-car." Theory, Culture Society 21:61-79.

Dolwick, Jim S. 2009. "'The Social' and Beyond: Introducing Actor-Network Theory." J Mart Arch 4:21-49.

Dowling, Robyn. Lloyd, Kate and Sandra Suchet-Pearson. 2017. Qualitative methods II: 'More-than-human' methodologies and/in praxis. Progress in Human Geography 41:823-831.

Gad, Christopher and Casper B Jensen. 2010. "On the Consequences of Post-ANT." Science, Technology & Human Values 35:55-80.

Goffman, Ervin. 1959. The presentation of self in everyday life. London: Penguin Books.

Harman, Graham. 2009. Prince of Networks: Bruno Latour and Metaphysics. Melbourne: Re-pres & Graham Harman.

Heidegger, Martin. 1962. Being and Time. Trans. John Macquarrie and Edward Robin- son. New York: Harper and Row.

Heidegger, Martin. 1982. The basic problems of phenomenology. Trans. Albert Hofstadter. Bloomington: Indiana University Press.

Kipnis, Andrew B. 2015. "Agency between humanism and posthumanism." Hau: Journal of Ethnographic Theory 5:43-58.

Latour, Bruno. 1992. "Where are the missing masses? The sociology of a few mundane artifacts." In Shaping technology/building society: Studies in sociotechnical change, edited by Wiebe E. Bijker and John Law, 225-258. Cambridge, MA: MIT Press.

Latour, Bruno. 1993. We have never been modern. Cambridge: Harvard University. Press.

Latour, Bruno. 1999. "On recalling ANT." In Actor Network Theory and After, edited by John Law and J. Hassard, 15-25. Blackwell.

Latour, Bruno. 2005. Reassembling the social. An introduction to actor-network-theory. New York: Oxford University Press.

Latour, Bruno and Venn, Couze. 2002. “Morality and Technology: The End of the Means.” Theory Culture Society 19:247-260.

Law, John. 1999. “After Ant: Topology, naming and complexity.” In Actor Network Theory and After, edited by John Law and John Hassard, 1-14. Blackwell.

Law, John. 2004. After Method: Mess in Social Science Research. London: Routledge.

Lehman, Joel. et al. 2018. The Surprising Creativity of Digital Evolution: A Collective of Anecdotes from the Evolutionary Computation and Artificial Life Research Communities, Accessed April 10, 2019: arXiv:1803.03453

Lupton, Deborah. 1999. “Monsters in metal cocoons: ‘Road range’ and cyborg bodies.” Body & Society 5:57-72.

McLean, Chris and John Hassard. 2004. “Symmetrical Absence/Symmetrical Absurdity: Critical Notes on the Production of Actor-Network Accounts.” Journal of Management Studies 41:493-519.

Mol, Annemarie. 2010. “Actor-Network Theory: sensitive terms and enduring tensions.” Kölner Zeitschrift für Soziologie und Sozialpsychologie 50:253-269.

Nimmo, Richie. 2011. “Actor-network theory and methodology: social research in a more-than-human world.” Methodological Innovations Online 6:108-119.

Pinch, Trevor. 2010. “The Invisible Technologies of Goffman’s Sociology From the Merry-go Round to the Internet.” Technology and Culture 51:409-424.

Robert, Dominique and Martin Dufresne. 2015. Actor-Network Theory and Crime studies. Explorations in Science and Technology. London/New York: Ashgate.

Sartre, Jean-Paul. 1960 [1937]. The transcendence of the ego. An existentialist theory of consciousness. New York: Hill and Wang.

Sayes, Edwin. 2014. “Actor-Network Theory and methodology: Just what does it mean to say that nonhumans have agency?” Social Studies of Science 44:134-149.

Schutz, Alfred. 1967 [1932] The Phenomenology of the Social World. Evanston, IL: Northwestern University Press.

Security. 2018. “Miljoenen nieuwe ip-adressen onderdeel van twee botnets” Accessed April 10, 2019. https://www.security.nl/posting/584714/Miljoenen+nieuwe+ip-adressen+onderdeel+van+twee+botnets

Thompson, Terry L., and Catherine Adams. 2014. “Speaking with things: encoded researchers, social data and other posthuman concoctions.” Distinktion: Scandinavian Journal of Social Theory 14:342-361.

Turgeman-Goldschmidt, Orly. 2005. “Hacker’s Accounts: Hacking as a Social Entertainment. Social Science Computer Review 23:8-23.

Turkle, Sherry. 1984. Hackers: Loving the machine for itself, In The Second Self: Computers and the Human Spirit by Sherry Turkle, 196-238. New York: Simon & Schuste.

Vandenberghe, Frederic. 2002. “Reconstructing Humants: A Humanist Critique of Actant-Network Theory.” Theory, Culture Society 19:51-67.

Van der Wagen, Wytske. 2018a. ”From Cybercrime to Cyborg Crime: An Exploration of High-Tech Cybercrime, Offenders and Victims through the Lens of Actor-Network Theory”. PhD diss., University of Groningen.

Van der Wagen, Wytske. 2018b. “The Cyborgian Deviant. An Assessment of the Hacker through the lens of Actor-Network Theory.” Journal of Qualitative Criminal Justice and Criminology 6:157-178.

Van der Wagen, Wytske and Frank Bernaards. 2018. Cybercriminele netwerken beschouwd vanuit het ‘cyborg crime’ –perspectief. Justitiele Verkenningen 44:54-67.

Van der Wagen, Wytske and Wolter Pieters. 2015. “From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks.” British Journal of Criminology, 55:578-595.

Verbeek, Peter-Paul. 2014. “Some Misunderstandings About the Moral Significance of Technology”. In The Moral Status of Technical Artefacts, edited by P. Kroes and Peter-Paul Verbeek, 75-88. Dordrecht: Springer.

Vicini, Andrea V., and Agnes, M. Brazal. 2015. “Longing for Transcendence: Cyborgs and Trans- and Posthumans.” Theological Studies 76:148-165.

Acknowledgements

I would like to thank Wolter Pieters and the two anonymous reviewers for their constructive feedback on the earlier draft of this article.