university of groningen

University Medical Center Groningen

University of Groningen

From cybercrime to cyborg crime

van der Wagen, Wytske

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2018

Link to publication in University of Groningen/UMCG research database

Citation for published version (APA):
van der Wagen, W. (2018). *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of Actor-Network Theory*. Rijksuniversiteit Groningen.

Copyright
Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

Take-down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): http://www.rug.nl/research/portal. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Download date: 27-01-2021

Chapter 2

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

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

Abstract

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

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

2.1. Introduction

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

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

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

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

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

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

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

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

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

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

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

2.2. Botnets: some basic features

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

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

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

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

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

2.3. Towards a criminological conceptualization of botnets

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

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

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

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

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

2.4. Actor-network theory in a nutshell

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

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

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

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

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

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

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

2.5.1. Composition

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

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

2.5.2. Delegation

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

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

2.5.3. Reversible black-boxing

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

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

2.5.4. Translation

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

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

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

2.6. Case study method

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

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

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

2.7. Short description of the case

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

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

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

2.8. Case analysis

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

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

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

2.8.1. (Building the) technological infrastructure of the botnet

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

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

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

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

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

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

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

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

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

2.8.2. The victimization process

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

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

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

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

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

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

2.8.3. The use and control of the botnet

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

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

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

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

2.8.4. The investigation and takedown of the botnet

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

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

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

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

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

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

2.9. Discussion

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

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

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

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

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

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

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