Chapter 5

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

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

Abstract

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

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

5.1. Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Case 1: Ransomware victimization

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

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

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

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

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

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

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

Case 2: Botnet victimization

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

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

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

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

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

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

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

Case 3: High-tech virtual theft victimization

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.5. The lens of actor-Network theory

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

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

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

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

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

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

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

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

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

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

5.6. Conceptualizing high-tech cyber victimization through ANT

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

Victim composition

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

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

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

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

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

Victim delegation

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

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

Victim translation

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

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

5.8. Conclusion and discussion: towards a hybrid victim theory

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

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

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

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

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

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

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

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

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

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

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