The hybrid victim

Re-conceptualizing high-tech cyber victimization through actor-network theory

van der Wagen, Wytske; Pieters, Wolter

DOI
10.1177/1477370818812016

Publication date
2018

Document Version
Final published version

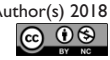
Published in
European Journal of Criminology

Article

European Journal of Criminology

The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory

European Journal of Criminology
1–18



DOI: 10.1177/1477370818812016
journals.sagepub.com/home/euc


Wytske van der Wagen
Erasmus School of Law, The Netherlands

Wolter Pieters
Technical University Delft, The Netherlands

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, in which the offender targets 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 analyses the cyber victim as a hybrid actor-network consisting of different entities that, together with the offender, make the victimization possible. The proposed concepts of victim composition, delegation and translation enable 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, ransomware, virtual theft

Keywords

Actor-network theory, botnet, cybercrime, cyber victimization, ransomware, virtual theft

Introduction

Although 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

Corresponding author:
Wytske van der Wagen, Assistant Professor of Criminology, Erasmus School of Law, Department of Criminology, PO Box 1738, DR Rotterdam, 3000, The Netherlands.
Email: vanderwagen@law.eur.nl

with all kinds of advanced malicious software (malware[1]), enabling an offender to take over computers and use them as 'bots' or 'slaves' in a cyber attack, or remotely take them 'hostage' by means of 'ransomware'. In the latter case, the computers or computer files are locked or encrypted, denying the victims access until the ransom has been paid (Gazet, 2010). Malware can also be used to steal personal credentials or to make fraudulent bank transactions (Bossler and Holt, 2009). 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 aspects. For instance, the interaction between the offender and victim is much more indirect (Reyns, 2013), and the offensive actions are often directed not only towards humans, but also towards vulnerable technical devices, which play a crucial role in the victimization process. This poses the question whether victimologists and criminologists are confronted with a different type of victimization 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 newly 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 cyber criminology (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 virtual, and the offending and the victimized (see also Brown, 2006; Franko Aas, 2007).

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 ANT approach to cybercrime proposed by Van der Wagen and Pieters (2015), 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 (Latour, 2005; Law, 1992). 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 has to be targeted, deceived and/or controlled in a relational manner by the offender(s) – the latter also being an actor-network (see Van der Wagen and Pieters, 2015). This alternative framework consists of three interrelated concepts: 'victim composition', 'victim delegation' and 'victim translation', 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 look at how the high-tech cyber victim is currently theorized in existing criminological research. We then 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.

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 (for example, online harassment, stalking), groups of individuals (for example, hate crimes), computer systems or networks (for example, hacking), (large) populations of computer users (for example, virus infections), virtual entities (for example, virtual rape), critical infrastructures (for example, 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 (for example, cyber stalking) in the sense that digital technology is not only a means to commit crime but a necessary condition for the type of crime committed (Koops, 2010). These crimes have gained relatively little attention in criminology (see, for example, Bossler and Holt, 2009, 2011; Leukfeldt, 2015), and their technical nature may 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 lifestyle approach (Hindelang, Gottfredson and Garofalo, 1978) and/or the routine activity theory (Cohen and Felson, 1979), theories that are also most influential in traditional victim studies. The lifestyle model supposes that certain behaviours (for example, related to work, school and leisure) expose certain individuals with certain demographic features to certain risky (crime-prone) situations (McNeeley, 2015). The Routine Activity Theory (RAT) on the other hand, focuses more on crime and victimization as an event (Pratt and Turanovic, 2016). It considers victimization to be 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, guardians being humans or objects that can prevent crime from occurring (for example, a fence, a surveillance camera or a police officer) (Yar, 2005). 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 lifestyle 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 of 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 offences, can still be applied in the cyber domain (see, for example, Leukfeldt and Yar, 2016; Reyns, 2013). 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 owing to the anti-spatial nature of cyberspace. Although such limitations are widely acknowledged, RAT remains the dominant perspective used to study cyber victimization, even in qualitative studies on cyber victimization (see, for example, Jansen and 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 and Holt, 2010).

In short, criminological studies on high-tech cyber victimization generally apply an opportunity-based approach, thereby 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 victims in a similar vein as victims of traditional crime: as vulnerable (human) entities with certain risky characteristics that make them more visible, suitable and/or attractive for offenders. We question whether such a framework provides an adequate and sufficient basis for the analysis of high-tech crime victimization, because of the key role played by technological and virtual entities in the victimization process.

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 examine the applicability of current frameworks more concretely and expose how and why their analytical power is limited. 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, and each case also has distinguishing victimization elements, as discussed below. Secondly, we had the unique opportunity to gain 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.[2] The third case study is based on a face-to-face interview with an offender who was engaged in virtual theft by hacking the computer system of his fellow players.[3] He explained in great detail how he deceived and targeted his victims, thereby providing insights into 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 analysing 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 had emerged as early as 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 (Gazet, 2010). The current case concerns one of the earlier manifestations of ransomware, also denoted as 'scareware', which is relatively easy to remove from the computer[4] and strongly depends on techniques of deception to make the computer user pay. At least 65,000 computer users 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 ones such as newspaper and library sites. The targeted websites made use of an automated advertisement system involving banners and popups, based on a contract with an advertisement company. The offender(s)[5] 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 [for example, distributing child pornography or illegally downloading content] and should pay a 100 euro fine [within 48 hours] in order to avoid criminal charges as well as to regain access to your computer.' The popup message also included logos of the police and of the stores where a payment card could be bought. The users had to insert the code on 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 imagery, 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 did most users realize that they had been deceived, then 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 a 'botherder'), facilitating a broad range of crimes, including banking malware, credit card theft and distributed denial-of-service (DDoS) attacks (Wagenaar, 2012).[6] Whereas banking malware and credit card theft target the infected machines themselves, in DDoS attacks the infected machines are used to attack machines or systems outside of the network (Schless and

Vranken, 2013). The current case, which involved a botnet of at least 3 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 the advertisement space of at least 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 place an order in the 'botnet shop' of the botherder (see also De Graaf et al., 2013). This additional malware was, for instance, a Trojan that steals banking credentials from the compromised machines (Van der Wagen and Pieters, 2015).[7]

The malware spread at unprecedented speed. Within a relatively short time, multiple bots joined the network, even requiring the botherder 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 thereafter, law enforcement agencies traced the botherder and dismantled the entire botnet (for a full description, see Van der Wagen and Pieters, 2015; De Graaf et al., 2013).

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. Because the stolen virtual goods can have actual material value, virtual theft is considered an illegal activity, an issue widely discussed by legal scholars (see, for example, 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 gear and outfits. The offender stated that he was able to steal thousands of euros from his fellow players, for which he employed two distinct methods.

In the first method he installed a remote access tool (RAT) on the computer of the fellow player, a tool or Trojan that enables the remote take-over of someone's computer and webcam. He was able to install the RAT by luring the fellow players to a self-created (malicious) genuine-looking website that was related to the game. He started a chat conversation with the fellow players and then sent them the link of the fake website, for example 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 also sent the link of the fake website to the friends of the victim in order to infect them with the malware as well. The next step was to observe the fellow 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 traces of his presence. The second method is rather different. The offender, here in the capacity of a virtual player (he had about 14 accounts), attacked his fellow players during the game itself, while simultaneously launching a DDoS attack on their computer (IP address).[8] During this attack, the fellow player was not able to defend

him or herself because the system temporarily crashed. After killing the player, he could take ('win') their virtual belongings.

Limitations of existing frameworks in analysing high-tech crime cases

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 analysing such factors can contribute to more knowledge about cyber victims. For instance, not updating software, visiting certain websites and/or clicking on (malicious) advertisements most likely increase the likelihood of becoming infected with malware. However, when we look more closely at the process in which the victim is targeted and becomes a victim, existing criminological frameworks also seem to encounter certain conceptual problems and have some critical blind spots.

Firstly, in the lifestyle routine activity theory, risk and vulnerability are generally attributed or assigned to single entities. In the above cases, however, it is not one single homogeneous entity but rather a chain or *network* of various human, technical and/or virtual elements that has to be targeted by the offender, either chronologically or simultaneously. 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 does not merely entail 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 computer users are partly victimized through the vulnerability of *other* entities, for example, 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 therefore makes a single and homogeneous conception of vulnerability and risk problematic. At the same time, these various entities also become victimized and not just the eventual computer user. For instance, in the ransomware case, website owners also considered themselves to be victims and filed a complaint, although they *contributed* to the distribution of the malware as well (see the third limitation). In this respect, the question 'who is entitled to be classified as a victim, by whom and under which circumstance' (Mythen and McGowan, 2018) has a special significance 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 regard to victims of environmental crime, such as animals, plants and ecosystems (see, for example, Hall, 2011; Halsey and White, 1998). Green criminologists plead for a broadening or extension of the victim concept in order to qualify non-humans for 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 virtual and fictional ones. In the

case of virtual rape, for example, it is not the human body that is physically harmed, but rather the 'virtual self' that is 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 *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. A similar point is presented by Whitson and Haggerty (2008), who argue that 'the victim' of identity theft is neither merely human nor exclusively digital, but involves an assembly of both: a cyborgian entity. 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 way 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 a burglary. 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 grasp such blurriness sufficiently, since they still maintain binary oppositions (Brown, 2006; Franko Aas, 2007; Van der Wagen, 2018b).

This brings us also to the rather dualistic nature of criminological frameworks. Opportunity theories and also criminology in general maintain strict divisions between what is human and what is technological (see also Brown, 2006; Franko Aas, 2007), but also between who is the victim and who is the offender (Van der Wagen and 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 et al., 2012) – ontologically criminologists still consider the victim and the offender as two separate entities. As we can see in the cases, such a 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. So a botnet can simultaneously be a victim or victimized network and an infrastructure or tool for other crimes, and thus operate in the capacity of an offender. We also see this dynamic in the case of infected websites and in the use of already hacked accounts to spread the malware further. This contagious nature of the victimization process also makes it more difficult to determine when a victimization begins and ends, just as in the case of a biological virus. Lifestyle routine activity theory tends to analyse and conceptualize victimization in terms of a concrete event, whereas victimization in the digital age can have a long-lasting and unpredictable nature (see, again, Whitson and Haggerty, 2008).

Thirdly, lifestyle routine activity theory is more engaged in assessing the suitability of the victim than with the targeting process itself when it comes to explaining victimization. As we have pointed out already, victimization is conceptualized in terms of *exposure* and

proximity: when a motivated offender encounters 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, although it is essential for grasping the complexity of how a vulnerability is generated and exploited. Next, 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 and Pieters, 2015). In this respect, high-tech crime is clearly different from the not particularly interactive burglary (Rock, 2007), but rather has similarities with fraud and deceit. Consequently, we cannot understand high-tech cyber victimization as a process fully carried out and orchestrated by the offender.

When considering the conceptualization of the role of the victim in the victimization process, we can argue that opportunity theory, aside from 'being vulnerable' or 'putting themselves in risky situations', under-theorizes the role of the victim or takes it for granted. The role of the victim is however overemphasized in the traditional literature through the 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 analysing the interaction between offenders and victims (see Rock, 2007). Based on what we have seen in the cases, it can be argued that elements of victim precipitation also need further theoretical consideration if we fully want to grasp how high-tech cyber victimization takes shape as an interactive process. As Demant and Dilkes-Frayne (2015) point out in their discussion of the limitations of situational crime prevention, criminologists cannot understand how crime events unfold when they merely look at the (rational) choice making of offenders. In the footsteps of ANT, the authors conceptualize a crime event 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 further in this article).

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). In recent years, various studies have emerged that apply ANT in the context of crime (see Luppicini, 2014, for an overview; Robert and Dufresne, 2015). Also the value of ANT is increasingly recognized in the scope of cybercrime (Brown, 2006; Smith et al., 2017; Wood, 2017). Yet empirical criminological studies applying ANT in the cyber domain are still quite rare (see, for example, Hinduja, 2012; Van der Wagen and Pieters, 2015; Van der Wagen, 2018a).

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 (for example, Giddens, Durkheim, Habermas, etc.) – to whom Latour refers 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 is also supportive of a 'material turn' or a 'turn to things' (see also Preda, 1999), arguing that non-human entities should be viewed and studied as *active* participants in the social. ANT thereby distances itself from anthropocentric or phenomenological constructivist approaches, which are mainly centred on humans or representations of humans.[9] Latour (2005) clarifies ANT's link with constructivism by referring to buildings that are still 'under construction'. If the researcher visited 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 (black boxes) (Van der Wagen, 2018b).

This is also reflected in the metaphor of *heterogeneous network*, indicating that many terms we are familiar with (for example, society, organization, machines, power, crime, offender, victim) are networks or *network effects* rather than single point actors or entities (Callon, 1986; Law, 1992). ANT considers it as its task to deconstruct the (network of) separate elements of the actor, thereby reversing the *reversible blackboxing*. It is important to stress that ANT's conceptualization of the network is different from the common use of the term in criminology and elsewhere. As the word *heterogeneous* already implies, the actor-network does not merely include humans, but also comprises non-humans such as texts, machines, architectures, tools and so on (Latour, 2005; Law, 2004). ANT does not make an a priori 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, 2005; Verbeek, 2006).

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; Dant, 2004; Latour, 2005). ANT presumes that the abilities and strengths of both humans and non-humans are often combined (in a network) when certain actions are carried out. In ANT terms, the *programmes of action* of the human and the non-human merge into a 'translated' programme of action, a process also termed *translation* (Latour, 1992, 1994). We can find the same principle of hybridity in Latour's concept of *complexity of actorship* or *composition*, which also seems to add a more organizational or strategic dimension. The classic example that is provided in this context is a hotel manager who wants to prevent the guests from forgetting to return their key. In order to achieve the programme of action (getting the key back) and to prevent or 'defeat' the *anti-programme* (not bringing the key back), the manager will add spoken notices, written notices and finally metal weights to the key (Latour, 1992). To make a connection with the earlier concept of heterogeneous networks, thinking

in terms of programmes of actions and anti-programmes 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 programme 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, because they are assigned a role that co-enables the programme of action. ANT's concept of delegation does not, however, merely refer to the outsourcing or automation of a certain task. It also emphasizes that, when we delegate a task, we cannot fully predict the outcomes and effects. It might, for instance, generate certain unforeseen events, interactions or usages that were not intended by the designer of the (delegated) object (see, further, Latour, 1992, 1994; Verbeek, 2006).

Conceptualizing high-tech cyber victimization through ANT

From the above description, it follows that ANT is a lens that requires actors and actions to be viewed in a more networked, hybrid and complex manner, a principle that is reflected 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, which is also an actor-network (Van der Wagen and Pieters, 2015). This analytical framework includes three main interrelated concepts: *victim composition, victim delegation* and *victim translation*, which we will now discuss in more detail, with references to the three 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 chronologically or simultaneously. 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, because it perceives notions such as risk and vulnerability as something distributed, relational and emergent. From this angle one asks and analyses how various entities *generate* this vulnerability, rather than (pre-)assigning vulnerability to the eventual victim/target, for example the computer user. Non-human entities such as websites and software are then also considered as an integrated 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 make a priori demarcations between a human and a technical vulnerability, but look at how a vulnerability is generated by a hybrid network of both.[10]

As we have seen in the cases, 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 the 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, for example, 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 virtual theft, on the other hand, the victim is a virtual player who is attacked in the 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 the capacity of both 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.

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 the study of which part of the victimization process is carried out by which actor, while being at the same time sensitive to 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, which is limited to the contribution of the traditional human victim, victim delegation includes the contribution of any (human or non-human) entity in the network, and does not have the undertone of victim blaming. 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 (Van der Wagen and 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 considered not 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 (for example, new visual tricks) to their

network to accomplish their programme of actions (for example, installing malware, stealing virtual goods), but also have to defeat the anti-programmes 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 the computer user from refusing to pay the ransom and prevent the computer user or virus scanner from detecting 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 the offender, most exemplified in the case of botnets where victimized machines are used in a cyber attack. This blurriness is 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.

Conclusion and discussion: Towards a hybrid victim theory

In this article we have aimed at outlining 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. 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* enables us to 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 – thereby also including the offending process in the analysis of victimization – 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 views victimization not as a concrete event but as a complex interplay between (human and non-human) programmes of actions and anti-programmes. Together, the three concepts emphasize the blurry boundaries between humans and non-humans, tools and guardians, and offenders and victims.

For the study of high-tech victimization, such an approach suggests that we should not only examine the actors that we usually consider to be 'the victim' (the eventual human computer users). In order to expose the (composition of) actors that generate or 'cause' victimization, we have to examine the offender and all the entities that he or she is targeting, including the computer of the user. More research on the role of entities such as website owners, whose website is used to distribute malware, also becomes more crucial (victim delegation). Furthermore, in light of the transformative and interactive nature of victimization (translation), the hybrid victim approach also opts for other research methods. For instance, experimental research in which computer users are exposed to certain conditions could gain insights into victims' programmes of action (for example, whether they will click on certain links) *and* anti-programmes.

The hybrid victim approach could also provide a basis for novel ways of thinking about crime prevention, or at least add a dimension to current approaches within situational crime prevention (see also Demant and 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 setting-up of a distributed network of (interconnected) anti-programmes to defeat or prevent cyber victimization. Fixing vulnerabilities and becoming more resilient is then perceived as a collaborative duty *and* responsibility of the different actors that play a role in generating the victimization. Of course, to some extent networks are already built in practice, also when it comes to tackling malware-related crimes such as botnets (see, for example, Dupont, 2017). ANT could be insightful for developing such initiatives further, since it draws attention to how different parties in an interdependent (hybrid) network can make a difference, even with relatively small contributions.

From the perspective of hybrid victim theory, measures could also be directed at (preventing) particular (inter)actions that play a role in enabling high-tech cyber victimization. Traditionally, one would stimulate potential victims (computer users) to change their password frequently, to not click on every link or attachment they encounter or to update their software, for example by means of awareness campaigns. From the perspective of hybrid victim theory, with the computer as part of the victim actor-network, an additional emphasis on technical encouragement or enforcement becomes more natural. Different forms of (in-built) 'technical assistance' could make the composite victims better equipped ('resilient') to combat and defend themselves against various cyber risks, including malware-based infections. Technical assistance could be also provided to victims that have *already* been infected (see, for example, Dupont, 2017), since this can prevent further spreading of the malware or additional infections with the same victim. Such measures, of course, also already exist, but they could be further prioritized and developed.

This study marks only 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 become more technically proficient and/or seek closer cooperation with computer scientists.

Acknowledgements

We would like to thank René van Swaaningen, Martina Althoff, and the two anonymous reviewers for their constructive and valuable comments on the earlier draft of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship and/or publication of this article: Wytske van der Wagen's research was conducted in the scope of a PhD project financed by the University of Groningen (Faculty of Law). Wolter Pieters' research has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 740920 (CYBECO). This publication reflects only the authors' views and the EU is not liable for any use that may be made of the information contained herein.

Notes

1. 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).
2. 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 and Pieters, 2015) for a full case description and analysis).
3. This interview took place in 2015 and was conducted in the scope of a research on hackers (see Van der Wagen, 2018a).
4. The newer generations of ransomware, often referred to as 'cryptolocker', cannot be removed this way. Owing to their sophistication they can force the victim to choose between payment and loss of the data.
5. The police officers presumed that a professional criminal organization was behind the scheme, including malware writers, ransomware designers and botnet owners.
6. 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/).
7. A Trojan is a type of malware that appears in the guise of something else (for example, a file or attachment) and 'requires some user interaction in order to execute the code' (Holt et al., 2015: 86).
8. In order to accomplish the DDoS, the offender first had to figure out the IP address of the fellow 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.
9. This is a claim that also holds for criminology (see Lindgren, 2005, for a discussion on constructionist and constructivist approaches in criminology).
10. In this respect we can also draw a 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 by Mähring et al., 2004).

References

Bossler AM and Holt TJ (2009) On-line activities, guardianship and malware infection: An examination of routine activity theory. *International Journal of Cyber Criminology* 3(1): 400–420.

Bossler AM and Holt TJ (2010) The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice* 38: 227–236.

Bossler AM and Holt TJ (2011) Malware victimization: A routine activities framework. In: Jaishankar K (ed.) *Cybercriminology: Exploring Internet Crime and Criminal Behaviors*. Boca Raton, FL: CRC Press, 317–346.

Brown S (2006) The criminology of hybrids. Rethinking crime and law in technosocial networks. *Theoretical Criminology* 1(4): 223–244.

Callon M (1986) The sociology of an actor-network: The case of the electric vehicle. In: Callon M, Law J and Rip A (eds) *Mapping the Dynamics of Science and Technology*. Basingstoke, UK: Macmillan Press, 19–34.

Cohen LE and Felson M (1979) Social change and crime rates trends: A routine activity approach. *American Sociological Review* 44(4): 588–608.

Cross C (2013) 'Nobody's holding a gun to your head.' Examining current discourses surrounding victims of online fraud. In: Richards K and Tauri J (eds) *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference*. Brisbane: Queensland University of Technology, 25–32.

Dant T (2004) The driver-car. *Theory, Culture & Society* 21(4/5): 61–79.

De Graaf D, Shosha AF and Gladyshev P (2013) Bredolab: Shopping in the cybercrime underworld. In: Rogers M and Seigfried-Spellar KC (eds) *Digital Forensics and Cybercrime*. 4th International Conference, ICDF@C 2012, 302–313.

Demant J and Dilkes-Frayne E (2015) Situational crime prevention in nightlife spaces: An ANT examination of PAD dogs and doorwork. In: Robert D and Dufresne M (eds) *Actor-Network Theory and Crime studies. Explorations in Science and Technology*. Surrey: Ashgate, 5–19.

Dupont B (2017) Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime Law & Social Change* 67(1): 97–116.

Franko Aas K (2007) Beyond 'The desert of the real': Crime control in a virtual(ised) Reality. In: Jewkes Y (ed.) *Crime Online*. Cullompton: Willan Publishing, 160–178.

Gazet A (2010) Comparative analysis of various ransomware virii. *Journal in Computer Virology* 6(1): 77–90.

Gottfredson M and Hirschi T (1990) *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Hall M (2011) Environmental victims. Challenges for criminology in the 21st century. *Journal of Criminal Justice and Security* 4: 371–391.

Halsey M and White R (1998) Crime, ecophilosophy and environmental harm. *Theoretical Criminology* 2(3): 345–371.

Hindelang MJ, Gottfredson MR and Garofalo J (1978) *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Cambridge, MA: Ballinger Publishing Co.

Hinduja S (2012) The heterogeneous engineering of music piracy: Applying actor-network theory to internet-based wrongdoing. *Policy and Internet* 4(3–4): 229–248.

Holt TJ and Bossler AM (2014) An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35(1): 20–40.

Holt TJ, Bossler AM and Seigfried-Spellar (2015) *Cybercrime and Digital Forensics. An Introduction*. New York: Routledge.

Jansen J and Leukfeldt R (2016) Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology* 10 (1): 79–91.

Jennings WG, Piquero AR and Reingle JM (2012) On the overlap between victimization and offending: A review of the literature. *Aggression and Violent Behavior* 17(1): 16–26.

Kearon T and Leach R (2000) Invasion of the 'body snatchers': Burglary reconsidered. *Theoretical Criminology* 4(4): 451–472.

Koops BJ (2010) The Internet and its opportunities for cybercrime. Tilburg Institute for Law, Technology, and Society (TILT), Tilburg Law School Legal Studies. Research Paper Series. No. 09/2011.

Latour B (1992) Where are the missing masses? The sociology of a few mundane artifacts. In: Bijker WE and Law J (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press, 225–258.

Latour B (1994) On technical mediation – Philosophy, sociology, genealogy. *Common Knowledge* 3(2): 29–64.

Latour B (2005) *Reassembling the Social. An Introduction to Actor-Network-Theory*. New York: Oxford University Press.

Law J (1992) Notes on the theory of the actor-network: Ordering, strategy and heterogeneity. *Systems Practice* 5(4): 379–393.

Law J (2004) *After Method: Mess in Social Science Research*. London: Routledge.

Leukfeldt ER (2015) Comparing victims of phishing and malware attacks. Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering* 4(4): 26–32.

Leukfeldt ER and Yar M (2016) Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior* 37(3): 263–280.

Lindgren S-A (2005). Social constructionism and criminology. Traditions, problems and possibilities. *Journal of Scandinavian Studies in Criminology and Crime Prevention* 6(1): 4–22.

Luppicini R (2014) Illuminating the dark side of the Internet with actor-network theory: An integrative review of current cybercrime research. *Global Media Journal* (Canadian Edition) 7(1): 35–49.

McNeeley S (2015) Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice* 31(1): 30–52.

Mähring M, Holmström J and Montealegre R (2004) Trojan actor-networks and swift translation: Bringing actor-network theory to project escalation studies. *Information Technology & People* 17(2): 210–238.

Maimon D et al. (2015) On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology* 55(3): 615–634.

Masys AJ (2014) Critical infrastructure and vulnerability: A relational analysis through actor network theory. In Masys A (ed.) *Networks and Network Analysis for Defence and Security. Lecture Notes in Social Networks*. Cham: Springer, 265–280.

Mol A (2010) Actor-network theory: Sensitive terms and enduring tensions. *Kölner Zeitschrift für Soziologie und Sozialpsychologie* 50: 253–269.

Mythen G and McGowan W (2018) Cultural victimology revisited. Synergies of risk, fear and resilience. In Walklate S (ed.) *Handbook of Victims and Victimology*. London: Routledge, 364–378.

Overill RE (1998) Trends in computer crime. *Journal of Financial Crime* 6(2): 157–162.

Pratt TC and Turanovic JJ (2016) Lifestyle and routine activity theories revisited: The importance of 'risk' to the study of victimization. *Victims & Offenders* 11(3): 335–354.

Preda A (1999) The turn to things: Arguments for a sociological theory of things. *Sociological Quarterly* 40(2): 347–366.

Reyns BW (2013) Online routines and identity theft victimization further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency* 50(2): 216–238.

Robert D and Dufresne M (eds) (2015) *Actor-Network Theory and Crime Studies. Explorations in Science and Technology*. Surrey: Ashgate.

Rock P (2007) Theoretical perspectives on victimization. In: Walklate S (ed.) *Handbook of Victims and Victimology*. Cullompton: Willan Publishing, 37–61.

Schless T and Vranken H (2013) Counter botnet activity in the Netherlands: A study on organization and effectiveness. The 8th Annual Computer Software and Applications Conference, 413–419.

Smith GJD, Bennet Moses L and Chan J (2017) Challenges of doing criminological research in the big data area: Towards a digital and data-driven approach. *British Journal of Criminology* 57: 259–274.

Strikwerda L (2012) Theft of virtual items in online multiplayer computer games: An ontological and moral analysis. *Ethics and Information Technology* 14(2): 89–97.

Strikwerda L (2015) Present and future instances of virtual rape in light of three categories of legal philosophical theories on rape. *Philosophy & Technology* 28(4): 491–510.

Van der Wagen W (2018a) The Cyborgian deviant: An assessment of the hacker through the lens of actor-network theory. *Journal of Qualitative Criminal Justice and Criminology* 6(2): 157–178.

Van der Wagen W (2018b). From cybercrime to Cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory. PhD Thesis, University of Groningen, Netherlands.

Van der Wagen W and Pieters W (2015). From cybercrime to Cyborg crime. Botnets as hybrid criminal actor-networks. *British Journal of Criminology* 55(3): 578–595.

Van Wilsem JA (2011) Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology* 8(2): 115–127.

Verbeek P-P (2006) *What Things Do: Philosophical Reflections on Technology, Agency and Design*. University Park, PA: Pennsylvania State University Press.

Von Hentig H (1940) Remarks on the interaction of perpetrator and victim. *Journal of Criminal Law and Criminology* 31(3): 303–309.

Von Hentig H (1948) *The Criminal and His Victim*. Hamden, CT: Archon Books.

Wagenaar P (2012) Detecting botnets using file system indicators. Master's thesis, University of Twente, The Netherlands.

Wall DS (2007) *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Whitson JR and Haggerty KD (2008) Identity theft and the care of the virtual self. *Economy and Society* 37(4): 572–594.

Wood MA (2017) Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's technological unconscious. *Theoretical Criminology* 21(2): 168–195.

Yar M (2005) The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology* 2(4): 407–427.