JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 3, NO. 3, 2021, 85–110

COMPARING THE VICTIMIZATION IMPACT OF CYBERCRIME AND TRADITIONAL CRIME: LITERATURE REVIEW AND FUTURE RESEARCH DIRECTIONS

Jildau Borwell[abc], Jurjen Jansen[a] and Wouter Stol[abd]

ABSTRACT

This paper addresses the importance of building knowledge on the impact of cybercrime victimization. Because the topic is understudied, it is unclear whether the impact of cybercrime differs from that of traditional crime. Our understanding of potential impact differences needs to be improved, considering that society and criminality are digitizing and, consequently, more people are likely to become victims of cybercrime. From a practical perspective, knowledge about the impact of different crimes is important to develop victim policies within law enforcement and other relevant agencies, and to treat victims appropriately. In this paper, a literature review is provided, as well as future research directions to address the current knowledge gap. The future research directions are divided in three topics: (1) distinguishing between cybercrime and traditional crime, (2) classifying cybercrime and traditional crime, and (3) measuring the victimization impact of cybercrime and traditional crime.

Keywords: cybercrime; traditional crime; impact; effects; consequences; victimization.

[a] NHL Stenden University of Applied Sciences, the Netherlands.
[b] Open University of the Netherlands, the Netherlands.
[c] Dutch National Police, the Netherlands.
[d] Dutch Police Academy, the Netherlands.

1 INTRODUCTION

This paper argues that it is important to build knowledge on the impact of cybercrime victimization. Furthermore, we will demonstrate that in current literature, there is insufficient understanding of the differences between the impact of cybercrime and traditional crime on victims. An endeavour to fill this gap is called for. In this paper, cybercrime is defined as crime for which information and communication technology (ICT) plays an essential role in the execution of the offence (Domenie et al., 2013). Although cybercrime can consist of many different subcategories (e.g., from online harassment to hacking of bank accounts) (Hamby et al., 2018), the definition provides a common denominator. Moreover, there are some specific aspects to cybercrime that differ from traditional crime (e.g., the anonymity and intangibility of the offender, disappearance of boundaries in time and place, and the potential widespread dissemination and permanence of online content) (Leukfeldt et al., 2018; Nadim & Fladmoe, 2021; Suler, 2004) and that could affect the victimization impact of cybercrime. Victimization impact is defined in this study as the seriousness or severity of the effects of criminality as perceived by victims (Dignan, 2005; Groenhuijsen, 1996).

Until the 1970s, the judicial system and academic literature were centered around offenders. In the judicial system, victims were mainly seen as information sources, as opposed to being considered parties of interest (Leukfeldt, Notté, & Malsch, 2018). Since the 1970s, however, societal concerns about victims of crime have increased (Smit, Ghauharali, Van der Veen, & Willemsen, 2018; Van Dijk & Van Mierlo, 2009) and there has been a rise in the emphasis placed on the mental and material assistance to help victims process the offence (Lamet & Wittebrood, 2009). Academic attention for the impact of victimization has also risen, driven by population studies that were originally designed to measure national crime rates (Shapland & Hall, 2007). Since then, studies have shown that crime can have serious and long-lasting effects on victims (Shapland & Hall, 2007; Smit et al., 2018). For example, compared to non-victims, victims report more psychological problems and lower well-being (Lamet & Wittebrood, 2009; Shapland & Hall, 2007). In addition, they seem more distrustful of strangers and tend to adjust their daily routines (Lamet & Wittebrood, 2009; Shapland & Hall, 2007). However, the impact of crime may vary per crime form and also within crime forms (Dinisman & Moroz, 2017; Jansen & Leukfeldt, 2018; Shapland & Hall, 2007). Women, for example, often experience more or more severe psychological consequences than men, at least in offline financial crimes (Gale & Coupe, 2005; Lamet & Wittebrood, 2009).

Although an increased amount of studies on the impact of crime on victims has been conducted, most of the work in this field focusses on traditional crimes such as violent crime, theft and criminal destruction,

rather than cybercrime (e.g., Aiken et al., 2015; Kunst & Koster, 2017; Lamet & Wittebrood, 2009). For instance, the first Dutch population study on cybercrime was conducted in 2011 (Domenie et al., 2013), and the resulting inclusion in the national security survey took place from 2012 onwards (Statistics Netherlands (CBS), 2013). However, society and the techniques offenders use to commit crimes have been digitizing since long before that (Stol et al., 1999). This is demonstrated by the fact that the term cybercrime has been used since at least 1990 (Brenner, 2004). Currently, computers form an integral part of people's lives. People depend on computers for almost everything, which makes them vulnerable for cybercrime victimization (Diamond & Bachmann, 2015; Reep-Van den Bergh & Junger, 2018). Cybercrime has obtained an important place within the total crime rates, although it is difficult to estimate the exact extent (Montoya et al., 2013; Reep-Van den Bergh & Junger, 2018). The traditional crime rates are declining, while cybercrime is not trending downwards (CPB, 2018; Riek & Böhme, 2018; Statistics Netherlands, 2020; Statistics Netherlands (CBS), 2018). On the contrary, cybercrime rates seem to be on the rise, and are expected to increase even further in the future (Agustina, 2015; Aiken et al., 2015; CPB, 2018; Statistics Netherlands, 2020). Therefore, studying the victimization impact of cybercrime is of increasing importance.

The few studies that focused on the victimization impact of cybercrime have shortcomings. To begin with, they only included one or a few types of cybercrime (Golladay & Holtfreter, 2017; Jansen & Leukfeldt, 2018). Moreover, a comprehensive comparison with the victimization impact of traditional crime has, to the best of our knowledge, not been made. Drawing this comparison will contribute to a better scientific understanding of victimization impact and to more accurate victim policies, as we will explain in the next section. The current digitization of crime gives us a unique opportunity to better understand the impact of victimization, and to examine whether the specific aspects of cybercrime affect the victimization impact. As Walter Dearborn stated (Bronfenbrenner, 1979, p. 37): "If you want to understand something, try to change it". The current changes in crime can be seen as a natural experiment which can be systematically exploited to create a better understanding.

The remainder of this paper starts with the relevance of comparing the impact of cybercrime and traditional crime. Then the methods of our literature review are discussed. In the results section, studies comparing the victimization impact of cybercrime and traditional crime are addressed, as well as studies considering cybercrime from a victim's perspective. Thereafter, shortcomings in current literature are discussed and future research directions are proposed. The focus of this paper is on the European context, and particularly on the Netherlands. However, at several points we

will take a broader view and our literature study is naturally international in scope.

2 THE RELEVANCE OF COMPARING THE IMPACT OF CYBERCRIME AND TRADTIONAL CRIME

In criminology, cybercrime victimization is a rapidly evolving but complex field (Van der Wagen & Pieters, 2018). Cybercrime seems to challenge the principles upon which our conventional understandings of criminal harm and justice are based, because it results in the globalization of crime, new forms of victimization, extensive data trails, and changes in the organization of criminal activities (Wall, 2005). Likewise, cybercrime opened a new research area in victimology, which proves to be hard to study (Moitra, 2004). This partly has to do with new aspects of cybercrime in a victimological sense. Examples are the technology involved which makes it more complex to fathom a crime (Stol, 2020), the remoteness that allows for victimization taking place from a distance, and the potential of widespread victimization since many potential victims can be approached at once (Moitra, 2004). In order to expand our insight into this relatively new and evolving field in criminology and victimology, it is important to understand how cybercrime relates to other crimes (Wall, 2005). Determining how the victimization impact of cybercrimes compares to that of traditional crimes is an essential part of this. This comparison should take into account different types of cybercrime.

From a more practical perspective, knowledge about the impact of crimes can enhance victim policies within law enforcement and other relevant agencies. Because the relative impact of cybercrime is currently unknown, it is unclear how much weight should be given to specific cybercrimes from a law enforcement perspective (Wall, 2005). The government's responsibility to support victims of crime increases with the weight of the consequences (Leukfeldt et al., 2018). Therefore, law enforcement agencies need to consider the impact of cybercrime to establish the relative seriousness of the crime and the nature of victimization (Moitra, 2005). Prosecution and sentencing are, for instance, dependent on the harm caused by crime (Moitra, 2004). Current cybercrime laws in European countries, such as the Convention on Cybercrime (2001), seem to be implemented without much knowledge about these aspects (Moitra, 2005). It should be noted that there are exceptions within countries. Sweden for example has taken into account the unique "cyber aspects" of crimes that can affect the impact on victims when drafting new legislation. An official inquiry with an extensive literature review underpinned this. Among other considerations, the inquiry stated that online disseminated privacy-sensitive information can remain in circulation for a long time and can

always be spread further. For victims, this can lead to distrust, feelings of insecurity, and self-censorship (Statens Offentliga Utredningar (SOU), 2016). The inquiry led to a bill with proposed changes in Swedish penal law (Swedish government, 2017). This in turn led to a legislative change where certain violations of personal integrity are punished more severely (i.e., if the act, considering the content of the image or information or the scope of dissemination, is liable to lead to very serious harm to the victim) (Chapter 4, section 6d of the Swedish criminal code). However, many nation-states have no specific cybercrime legislation (Mittal et al., 2017), let alone legislation specifically taking the victimization impact of cybercrime into account.

Apart from legislation, police priorities should also be based on the impact of crimes (Domenie et al., 2013). However, police agencies appear to consider the importance of cybercrime lower than that of traditional crime such as physical abuse, and priorities might be established accordingly (Boekhoorn, 2020; Veenstra et al., 2013). This, for instance, may result in police officers spending a relatively small proportion of time on those cases (Holt et al., 2019). Those priorities seem rather based on subjective ideas or media reports than on grounded research. To determine the appropriate social and judicial response and inform policy makers, the impact of cybercrime should be guiding and therefore precisely understood (Moitra, 2005; Wall, 2005). It can be considered self-evident that in legal measures, cybercrime should be conceived differently from traditional crime if specific features of cybercrime lead to a specific impact on victims.

Knowledge about the impact of cyber and traditional crimes is also important for police and other organizations that deal with victims in order to ensure appropriate treatment (Hageman & Loeffen, 2016; Modic & Anderson, 2015). The impact of crime on victims seems to be of direct influence on their needs (Boom, Kuijpers, & Moene, 2008; Dinisman & Moroz, 2017; Leukfeldt et al., 2018; Van Caem & Hageman, 2018). Therefore, knowledge about that impact can help to meet victims' needs and to treat victims properly. The needs of victims of (specific) cybercrimes may differ from the needs of victims of traditional crimes (De Kimpe et al., 2020; Leukfeldt et al., 2018). There are two paradigms about police work relevant to this context: the consent paradigm and the control paradigm. The dominant paradigm is the consent paradigm, which aligns with the aim to meet the needs of victims. From this perspective, the police mandate is broader than crime fighting and maintaining order by repressive action, as opposed to the more narrow control paradigm (Van Dijk & Hoogewoning, 2018). Sir Robert Peel may be seen as the founder of the consent paradigm. His nine policing principles from 1829 have given direction to modern policing in the Western world (Keane & Bell, 2013). Alongside police organizations in other Western countries, the Dutch police shifted to the

consent paradigm in the 1960s, which is still in play (Van Dijk & Hoogewoning, 2018). In the consent paradigm, the police are socially engaged, and the legitimacy of the police is derived from the consent of the public. The police should be available in and for the community and – apart from crime fighting and maintaining order – focused on increasing the safety and wellness of civilians. The impact of (cyber)crime needs to become clearer to successfully apply this paradigm and to approach victims correctly.

The Dutch context and the Dutch application of the consent paradigm illustrate how it can be particularly important to consider the differences in impact of cybercrime and traditional crime. Since the 1980s and 1990s, the Dutch police strived towards being a service organization. This is reflected in several policy programs with 'service' in the title, such as the Service Concept which was introduced in 2012, the Service Program which was implemented in 2016 (Biemolt et al., 2012; Van Bourgondien, 2017; Van Caem & Hageman, 2018; Van Dijk & Hoogewoning, 2018), and the term Intake and Service for the police units responsible for crime reporting. According to this 'service philosophy', the police should be cognizant on the needs of their 'clients' – because policing should follow the public interest – and the delivered services are partly derived from the publics' opinion about qualitatively good policing (Van Caem & Hageman, 2018; Van Dijk & Hoogewoning, 2018). The mission of the Dutch police to be vigilant and serving (Van Dijk & Hoogewoning, 2018) also fits this service-minded approach.

In some of the latest Dutch governmental policies of the Ministry of Justice and Security, victims occupy an important position, such as the Multiannual Agenda Victim Policy 2018-2021 (Dekker, 2018). The policies partly stem from the European Union minimum standards on the rights, support, and protection of crime victims, which were implemented in Dutch law in 2015 and obviously are incorporated in the laws of other European Union member states as well (Kunst & Koster, 2017; Ministerie van Veiligheid en Justitie, 2017). One of the goals of the new Dutch policies is the recognition of victims' suffering by society and the judicial system (Kunst & Koster, 2017; Maercker & Müller, 2004). For the upcoming period, the government has prioritized supporting victims to recover from the consequences of crimes on a financial, practical, and emotional level (Dekker, 2018). The impact of different crimes needs to be clear in order to truly recognize the suffering of those victims and to treat them accordingly. Moreover, as noted before, victims' needs depend on the impact of the crime (Dinisman & Moroz, 2017; Leukfeldt et al., 2018). Given the socially engaged character of victim policies in the Netherlands and other countries, it is important to consider the impact of cybercrimes more closely.

3 METHODS

We started the literature review by combining search terms such as "comparing", "difference", "victimization", "impact", "consequences", "effects", "crime", "cybercrime" and "online crime" and entering these into several academic literature search engines, such as Google Scholar, Web of Science and PsycINFO. No limits concerning the year of publication have been set because the subject is relatively new. The relevance of the literature was assessed by reading the abstracts. Publications were selected when the subject contained the impact of cybercrime or traditional crime on victims; the differences between cybercrime and traditional crime in general or classifications of both; or the role of law enforcement or victim support in relation to the impact of cybercrime or traditional crime. Selected publications were read and from these, other relevant titles were selected, using the snowball method.

To ensure that using this snowball method we did not omit any relevant publications on victimization impact comparisons for cyber and traditional crime, we added a systematic literature review. On May 4th 2021, we ran a query in the search engines Web of Science, SocIndex and PsycIndex[1]. We limited our search to the abstract, keywords, and title of publications. Through Web of Science, our query yielded eleven results, through SocIndex three and through PsycIndex six. Based on the title, we made a first selection of the potentially relevant articles. If the content seemed to discuss a comparison of the impact of cybercrime and traditional crime on victims, we obtained the reference and abstract for further evaluation. From Web of Science, we selected five titles of which we read the abstracts. Two of those were not about comparing the impact of online and offline crime. The three other articles, after positive quality assessment, were read in full. From SocIndex and PsycIndex, no additional relevant titles were selected.

Below, we provide an outline of the selected relevant studies. In the next section, we cover the impact of cybercrime compared to traditional crime. After that, we proceed to discuss studies that examine cybercrime from a victim's perspective.

[1] The following query was used: ((impact* OR influence* OR consequence* OR affect* OR effect* OR coping OR cope OR experience* OR result* OR implication* OR aftermath OR aftereffect) AND (cybercrime* OR "online crim*" OR "computer misuse crim*" OR "internet crim*" OR "internet-related crim*" OR "computer crim") AND (compar* OR difference* OR contrast* OR oppos* OR diverge* OR discrepancy OR chang* OR deviat* OR contrar* disctinct* OR variat* OR alternat*) AND (victim*) AND ("traditional crim*" OR "classic* crim*" OR "offline crim*" OR "conventional crim*" OR "regular crim*" OR "violent crim*" OR "property crim*" OR "face-to-face crim*" OR "face to face crim*" OR "F2F crim*")).

4 STUDIES COMPARING THE VICTIMIZATION IMPACT OF CYBERCRIME AND TRADITIONAL CRIME

As noted before, a comprehensive comparison between the victimization impact of cybercrime and traditional crime has not been made in current literature. However, some studies covered findings in one or several segments of the subject, which gives a preliminary indication of this comparison. One of the previous comparisons of traditional and cybercrime victimization impact was conducted in the national victimization survey of Luxembourg. This study compared the emotional impact of card fraud or online banking fraud and a few traditional crimes (Heinz et al., 2015). Whereas the emotional impact of card or online banking fraud was higher than that of some traditional, offline crimes, i.e., consumer fraud (e.g., by a seller or craftsman), theft of personal property, theft from a car, bicycle theft, and corruption or bribe seeking, it was lower than the emotional impact of other traditional crimes, i.e., physical violence, burglary and robbery (Heinz et al., 2015). Therefore, the emotional impact level of card or online banking fraud appears to be in between that of the traditional crimes. It must be noted that consumer fraud can also take place online, but because of the way the question was phrased ("by a seller or craftsman" (Heinz et al., 2015: 17)) this is expected to measure traditional crime. The study is limited because of the restriction to one type of cybercrime (card or online banking fraud) and one dimension of impact (emotional impact). Furthermore, it seems that no attention has been devoted to comparing the cybercrime in question to the most obvious or suitable traditional counterpart, which would arguably be offline fraud.

Another impact comparison was made between offline and online bullying in a study of Campbell, Spears, Slee, Butler, and Kift (2012). Although bullying cannot always be considered criminal behavior, it is at least 'deviant behavior'. Using a school-based survey among 647 traditional bullying victims, 187 cyberbullying victims and 140 mixed victims, the authors concluded that online bullying might have a greater impact than offline bullying. Victims of online bullying experienced higher levels of social problems, fear and depression (Campbell et al., 2012). They mentioned possible explanations relating to the characteristics of online bullying, namely the broad audience, anonymity of the bully, potential extended appearance of texts and images, and the ongoing possibility to reach the victims via the internet. It also seemed that online bullies apply severer techniques over a longer time period, possibly because they do not see the reaction of the victim and because they feel anonymous (Campbell et al., 2012).

A different approach was used in a vignette study by Kerr and colleagues (2013). In this study, 72 respondents – victims, and stakeholders

who are involved in addressing fraud and its impact – were asked whether online fraud should be perceived differently from offline fraud. Most stated that the importance lies in the commission of a fraud offence, and to a lesser extent in the applied method (online or offline). Some respondents argued that the consequences of online and offline fraud can be similar, and therefore should be regarded and punished equally. Others replied that the impact of online fraud is smaller because it is less personal, since there is no face-to-face contact with the offender. However, some stated that online fraud might be more serious than offline fraud because of the anonymous nature of the crime. Respondents also argued that because people cannot avoid making use of the internet, it would feel impossible to avoid online fraud.

Another study, although the impact of crime was an aspect, compared the reporting of online and offline fraud (Kemp, 2020). The authors did measure the victimization impact of online and offline fraud, but the impact scores were not reported. The authors did conclude that victims of online fraud were more likely to consider this a crime than victims of telephone fraud and in-person fraud. The subject of again another study by Graham and colleagues (2019), was also reporting cybercrime and traditional crime. Although the authors did mention taking the seriousness of the crime into account, they evaluated the seriousness themselves, rather than asking respondents to rate the severity.

Like us, Hamby and colleagues (2018) noted an absence of jointly examining the impact of online and offline crime. The primary focus of their study, however, was on multi-victimization of digital and traditional crime. The authors arrived at similar effects on anxiety/dysphoria symptoms for cyber and traditional victims. However, traditional victimization was focused on childhood experiences such as child abuse and exposure to domestic violence, while digital victimization was focused on negative experiences online or over the phone in general. A comparison with broader traditional victimization did not take place.

Although the foregoing shows that there are scarcely any studies empirically comparing the victimization impact of cybercrimes and traditional crime, there are some studies that focus on the impact of cybercrime and then discuss the character of this impact. In fact, those studies implicitly compare cybercrimes and traditional crimes, based on logic or assumptions rather than empirically studying the comparison. They provide an opportunity to reflect on the possible differences between online and offline crime, which we will do in the next section.

5 STUDIES CONSIDERING CYBERCRIME FROM A VICTIM PERSPECTIVE

Cybercrimes and cybercrime victimization seem to have unique patterns and characteristics, some of which might heighten the impact on victims (Agustina, 2015). In this section, those patterns and characteristics are explored.

To begin with, cybercrime can be scalable, boundless, intangible and permanent. These aspects might result in longer and recurring victimization, and might recidivate the consequences (Leukfeldt et al., 2018). For instance, with online harassment or bullying, the offence has no clear end, as opposed to offline harassment or bullying (Jahankhani et al., 2014; Nadim & Fladmoe, 2021). Online harassment may cause people to become more cautious about sharing their views openly, an obvious behavioral implication of this type of crime (Nadim & Fladmoe, 2021). Because of the online aspect, the offender is able to reach the victim at any time and from any place. This might result in the victim not feeling safe anywhere (Jahankhani et al., 2014; Jansen & Leukfeldt, 2018; Leukfeldt et al., 2018). Additionally, the offender seems intangible, because he or she operates anonymous and from a distance. Therefore, from a victims' perspective, the offender can always reappear to recommit the crime (Leukfeldt et al., 2018). The wide scope on which unwanted images or messages can be spread is relevant for the impact of cybercrimes such as sextortion, online threat, harassment, stalking, or libel/slander, and might induce anxiety (Leukfeldt et al., 2018; Nadim & Fladmoe, 2021). That this content might stay online can result in a sense of permanence of the crime and therefore lead to higher and enduring impact for victims.

Another reason for the possible high impact of cybercrimes is that people regard their devices as an extension of the self, leading to cybercrime feeling as invasive as or even more invasive than physical crime. Longo (2018) states that people regard their devices as a prosthesis of the mind. Distinguishing and delimiting the real from the digital self can therefore be difficult for people (Agustina, 2015). They might feel equally wounded when their virtual self is attacked, as when their embodied self is attacked (Agustina, 2015). Van der Wagen and Pieters (2018) therefore state that computers should not be considered mere tools, but devices that people are connected to and depend upon. The same probably applies to devices with apps that are connected to certain functions of the body, such as hearing or heartbeat (Gasson & Koops, 2013). A cyberattack on those devices can be literally as invasive as, for instance, violent crime. Another variation of the interconnectedness between technology and the human body is people being present in the digital world in the form of an avatar or a digital representation of the human body, which representation can be violated or

attacked (Stol, 2020). The impact this might have on the person behind the representation, and if such a violation can or should be seen as crime, is as yet unclear (Strikwerda, 2014).

The impact cybercrime victims experience might be heightened due to victim blaming and stigmatization, which occurs relatively often. Victims are not always recognized or acknowledged appropriately because society is less familiar with and knowledgeable about cybercrimes (Jansen & Leukfeldt, 2018; Leukfeldt et al., 2018). Studies suggest that law enforcement, the victim's social environment or unknown people on the internet relatively often blame victims of cybercrime for their victimization (Cross et al., 2016; Kerr et al., 2013; Leukfeldt et al., 2018; Whitty & Buchanan, 2016). Furthermore, the police may not prioritize crimes such as online fraud, because they sometimes consider them self-inflicted (Leukfeldt et al., 2012). This might have to do with victims often actively contributing to the crime. Victim blaming and stigmatization can result in victims not feeling taken seriously. This is especially relevant considering receiving recognition seems to be one of the most important needs of crime victims (Boom et al., 2008; Van der Vijver, 1993).

Although the aforementioned studies indicate that the impact of cybercrime on victims might be severe compared with traditional crime, they do not provide a comprehensive understanding of this impact, due to several limitations. In the next section, the shortcomings in current literature on the impact of cybercrime and crime in general are discussed.

6 SHORTCOMINGS IN CURRENT LITERATURE ON THE IMPACT OF CRIME

Although cybercrime is currently recognized as an important topic of research, a well-established, nuanced view on the victimization impact of cybercrime is lacking. There are relatively few studies on cybercrime victimization, let alone studies providing a deeper understanding about cybercrime victimization (Diamond & Bachmann, 2015). The prevailing image about the impact of cybercrime seems to be based on anecdotes, one-sided hypes or news messages (Henson et al., 2013; Moitra, 2005). An unfounded public opinion because of media sensationalizing should be prevented, as this may lead to misplaced, exaggerated or understated demands for policies of criminal justice agencies (Wall, 2005). This calls for a more nuanced, scientifically sound view on this topic.

The lack of research on cybercrime victimization manifests itself in studies being offence-centered instead of victim-centered and in a lack of focus on the impact for individual victims. Most studies focus on the committed offences and on how to prevent or fight these, rather than on their consequences for victims (Riek, 2017; Sarre et al., 2018). The impact on

the individual victim is often ignored in the studies that do focus on the consequences of cybercrime, many of which are limited to the broader economic impact in terms of monetary losses (Canetti et al., 2017). The few studies on individual cybercrime victimization often solely address victim characteristics, or vulnerability factors for victimization (Jansen & Leukfeldt, 2018; Reep-Van den Bergh & Junger, 2018; Riek & Böhme, 2018; Van der Wagen & Pieters, 2018).

The studies that do focus on individual cybercrime victimization impact fall short when it comes to certain impact and cybercrime types, as well as the comparison with the impact of traditional crime. Studies on individual victimization impact tend to focus on financial impact (Reep-Van den Bergh & Junger, 2018; Riek & Böhme, 2018). As Li and colleagues (2019) have identified, other forms of victimization impact, namely emotional or psychological, behavioral or social and physical impact, are largely insufficiently studied. Moreover, existing studies usually focus on one or few types of cybercrime, failing in establishing a comprehensive overview (Leukfeldt et al., 2018; Riek, 2017). For instance, little attention has been devoted to the victimization impact of financially motivated cybercrime, such as identity theft and online fraud, as was concluded earlier by Hamby and colleagues (2018). Most importantly, virtually no attention has been given to the comparison of cybercrime and traditional crime (Riek, 2017), which is also demonstrated by the results of our literature review. Cyberbullying is an exception, which is relatively well-studied and often compared to the offline counterpart (Canetti et al., 2017; Hamby et al., 2018; Henson et al., 2013; Smith et al., 2008). However, bullying cannot always be defined as crime, and only juveniles are included in those studies (Smith et al., 2008). The impact of online harassment and online hate speech has been relatively well studied, but as Nadim and Fladmoe (2021) note, a comparison with the impact of offline harassment and hate speech is lacking. Moreover, similar to bullying, harassment and hate speech cannot always be considered crimes.

The lack of research on the impact of cybercrime may be due to the perception that cybercrime victimization is less serious than, for instance, street crime victimization (Henson et al., 2013). Traditionally, the severity of crime is often derived from the physical impact on the victim (Lamet & Wittebrood, 2009). For most cybercrimes, no physical contact takes place between perpetrator and victim, and in the case of online banking fraud, victims are often compensated for financial damage. Because victimization impact cannot be measured based on physical injury and not always on actual financial damage, the impact of cybercrime seems to be underestimated, or cybercrime is even considered a victimless crime (Button et al., 2014; Cross et al., 2016; Henson et al., 2013; Jansen & Leukfeldt, 2018). Contrary to this perception, previous studies have

indicated that crimes can be impactful for victims despite a lack of physical violence (Button et al., 2020; Golladay & Holtfreter, 2017; Jansen & Leukfeldt, 2018; Lamet & Wittebrood, 2009). Previous research suggests that the victimization impact of cybercrime may even be comparable to the impact of severe violent crime (Henson et al., 2013; Jansen & Leukfeldt, 2018). This is illustrated by a victim who claimed that online banking fraud can be compared to domestic burglary, which is considered to be a "high impact crime" by the Dutch police, or hacking victims comparing the experience to rape (Button et al., 2020; Jansen & Leukfeldt, 2018). However, these were just single observations; the victims' responses to domestic burglary and rape were not measured, and no comparison to the victimization impact of traditional crime took place. The next section covers possibilities for future research that take into account the limitations in current research.

7 FUTURE RESEARCH DIRECTIONS

Based on the aforementioned shortcomings and to establish the field of future research, we present some future research directions. As was previously clarified, the impact of cybercrime can be serious and comparable to or even more profound than that of traditional crimes. However, there is insufficient insight into the impact of specific cybercrimes (Leukfeldt et al., 2018). Cybercrime in itself might seem like a specific subject, but it contains many different forms of victimization (Van der Wagen & Pieters, 2018). Moreover, there is little insight into the impact of specific cybercrimes compared to traditional crimes. The research directions are divided into, firstly, distinguishing between cybercrime and traditional crime, secondly, classifying of cybercrime and traditional crime, and finally, measuring the victimization impact of cybercrime and traditional crime.

7.1 Distinguishing between cybercrime and traditional crime

First of all, an acceptable boundary to distinguish between cybercrime and traditional crime is a prerequisite to compare the impact of both. In establishing this boundary, opinions from academics and practitioners about an acceptable demarcation should be taken into account for the results to be accepted and acted upon. This presents some difficulties, because of an ongoing discussion about the definition of cybercrime and its different forms (Riek & Böhme, 2018; Stol & Strikwerda, 2019; Yar, 2005). Current literature suggests that the boundary between digital and traditional crime is narrow and not always clear (Correia, 2019; Montoya et al., 2013). Many crimes contain both offline and online components (Lamet

& Wittebrood, 2009; Montoya et al., 2013). This can be the case with, for instance, stalking, harassment, fraud, and threat (Leukfeldt et al., 2018; Montoya et al., 2013). Moreover, because of the omnipresence of cybercrime in daily life, the question is sometimes raised whether cybercrimes should be seen as a separate category of crime, or if it is more accurate to consider them ordinary crimes in a digitized society (Jansen et al., 2013). A lot of cybercrimes seem to be electronic parallels of a traditional counterpart (Henson et al., 2013). Some authors state that traditional crime merely developed and has been made easier because ICT is now used in the execution of the offence, while the fundamentals, such as how they are committed, motives and consequences such as victimization impact, have not significantly changed (Correia, 2019; Kerr et al., 2013; Yar, 2005).

The foregoing indicates how some authors argue that distinguishing between online and offline modi operandi is not of great importance and will not influence victimization impact. From this point of view, comparing different cybercrimes to traditional crimes would not even be necessary. However, this opinion is unsubstantiated as long as the potential difference in victimization impact is not comprehensively studied. Other authors are therefore undecided and raise the question if certain cybercrimes are an old problem through a new medium, or qualitatively and quantitatively new problems (Mitchell et al., 2007). Additionally, authors such as Henson, Reyns, and Fisher (2016), state that now technology and the internet advance, cybercrime victimization should be seen as a unique form of victimization and therefore treated as such. This is supported by the unique characteristics which are known to be associated with cybercrime (Leukfeldt et al., 2018; Nadim & Fladmoe, 2021; Suler, 2004). Research comparing the impact of cybercrime and traditional crime should shed light on which view comes closest to reality, which still requires an acceptable demarcation.

Yar (2005) distinguishes between defining cybercrime as a distinct crime form, and classifying cybercrime. According to Yar, 'defining' means that one tries to establish a general theoretical definition for cybercrime, while 'classifying' means producing an overview of thecrimes that fall under the concept of cybercrime. We argue that it is unnecessary to have an exact academic definition of cybercrime and traditional crime (defining) to compare the impact of both. Instead, it seems sufficient to establish a working definition of cybercrime, and to subsequently signify a range of different crime types falling under the definition (classifying). Classification was, for instance, undertaken as part of the Convention on Cybercrime, without giving a definition of cybercrime (Counsil of Europe, 2001). To compare the impact of cybercrime and traditional crime, the definition of cybercrime might only be used as a temporary concept, as Blumer (1954) would call a sensitizing concept, necessary to indicate what kind of crimes

we are talking about and to study them. A sensitizing concept is not clearly linked to its exact content, but gives a general sense of where to look and what is relevant (Blumer, 1954). This aligns with what Yar (2005) calls a working definition of cybercrime. Montoya and colleagues (2013), as well as Domenie and colleagues (2013), have already proposed to distinguish between cybercrime and traditional crime by following a working definition of cybercrime. Pursuing this approach, every crime form can be assessed on the conformity with the earlier mentioned 'sensitizing concept' of cybercrime as crime in which ICT plays an essential role in the execution of the offence. To subsequently make a comparison between the impact of cybercrime and traditional crime, it is important to classify different subtypes of both in a meaningful way. In doing so, the sensitizing concept cybercrime is further specified. This classification will be discussed in the next section.

7.2 Classifying cybercrime and traditional crime

The literature on this topic shows that victimization impact differs for different cybercrimes and traditional crimes, as well as for individual victims (Kunst & Koster, 2017; Shapland & Hall, 2007). Therefore, it is not possible to make an overall comparison between cybercrime and traditional crime. A division in subcategories is required to study cybercrime because it covers so many different illegal activities (Correia, 2019). Up to now, many different divisions and typologies of cybercrime types have been developed, which is also the case for traditional crime. An accurate perception of the different types therefore has become difficult. There is an overlap within the distinguished subcategories of cybercrimes, such as hacking and online fraud (Anderson et al., 2013; Furnell, 2001; Moitra, 2005; Tsakalidis & Vergidis, 2017). On the other hand, the chosen divisions result in omissions (Furnell, 2001). Within a crime such as fraud, there are a lot of different categories, which differ in severity of the crime (Moitra, 2005; Tsakalidis & Vergidis, 2017). A division should therefore be sufficiently specific, meaning at least, not so broad that oversight is lost (Moitra, 2005).

This contribution has shown that different types of cyber and traditional crime need to be compared to each other, which demands a meaningful division in crime groups or pairs. The crime types that are added to the comparison need to be chosen prudently. In previous research, crimes have been often grouped by the offender's motive (Domenie et al., 2013; Leukfeldt et al., 2018; Leukfeldt, Kentgens, Prins, & Stol, 2015; Neufeld, 2010; Sabillon, Cano, Cavaller, & Serra, 2016). Although this appears to be a viable option to decide which cybercrimes to compare with which traditional crimes, the motive could influence the victimization impact. This would therefore lead to a dependent variable being added as

an independent variable, infringing statistical standards. In other words, ideally speaking, crimes must be selected on the basis of the role ICT plays in the execution of the offence – an essential role or not – and nothing else.

Classifications from existing research can be used to determine suitable pairs or groups of crimes. For instance, for traditional crime, the International Classification of Crime for Statistical Purposes (ICCS) can be used (UNODC, 2015). Because the focus in this classification is less on cybercrime, it should be supplemented by the different types of cybercrime as described in previous research (Furnell, 2001; Hulst & Neve, 2008; Reep-Van den Bergh & Junger, 2018; Tsakalidis & Vergidis, 2017). We therefore propose comparing the most prevalent cyber-enabled crimes – crimes for which ICT plays an essential role in the execution of the offence (Domenie et al., 2013; Riek, 2017) – with their traditional counterpart. Comparing crime pairs that have many similarities allows for assessing what the unique aspects of cybercrime imply about the impact on victims. Cyber-dependent crimes – crimes in which ICT plays an essential role in the execution of the offence and which are also focused on ICT (such as a hack or DDoS-attack) – might be treated as separate categories, because an obvious counterpart does not exist. Another option is to select a defendable traditional counterpart for comparison; for instance, DDoS-attacks versus vandalism, and hacking versus burglary.

7.3 Measuring the victimization impact of cybercrime and traditional crime

Once suitable groups or pairs of crimes have been selected for comparison, measurement methods for victimization impact need to be established. Comparing the severity in the judicial sense will not suffice. Research shows that high-penalty crimes do not always greatly impact victims, while low-penalty crimes can greatly impact victims (Lamet & Wittebrood, 2009). It is therefore important to have a clear picture of the factors that victimization impact can be broken down into.

Literature shows that victimization impact can roughly be divided into psychological/emotional, financial/material, social/behavioral, and physical impact (Dinisman & Moroz, 2017; Huys, 2012; Kerr et al., 2013; Lamet & Wittebrood, 2009; Riek & Böhme, 2018; Shapland & Hall, 2007). The different types of impact might overlap, or might be dependent on each other (Kerr et al., 2013; Lamet & Wittebrood, 2009; Modic & Anderson, 2015). To establish a comprehensive insight of the different types of victimization impact, they need to be clearly defined and measured, and the overlap and dependency has to be taken into account. Earlier studies, for instance, recommended measuring emotional and behavioral reactions to cybercrime in tandem, because the reactions influence each other (Li et al.,

2019). Therefore, different types of impact should be studied simultaneously to establish a more comprehensive view of victimization impact.

Previous research also clarifies that impact should be measured over time, because the impact consists of different stages (Jansen & Leukfeldt, 2018). Crime victims live through a first phase, lasting hours to days; a second phase, lasting three to eight months; and a last phase, in which they eventually learn to successfully cope with the crime (Frieze et al., 1987; Jansen & Leukfeldt, 2018). Victimization impact manifests itself differently during those phases. For instance, shock often remains for a short period of time, while loss of trust in people can remain for years (Shapland & Hall, 2007). Also, the duration of victimization impact apparently varies for different crimes (Shapland & Hall, 2007). Therefore, longitudinal research on victimization impact is advised, or at least the time of occurrence of the offence should be taken into account. An interesting first longitudinal study in this area is performed by Sipma and Van Leijsen (2019). They discovered that victims of cybercrime experienced increased fear of cybercrime and took more protective measures. According to their study, the mental health of the victims did not deteriorate after the distinguished cybercrimes, except for victims of online threat.

A subsequent step for measuring the impact of cyber and traditional crimes is establishing the determinants influencing this impact. Those determinants include the characteristics of the crime, and personal and social factors. Most of the determinants are established in general literature on the victimization impact of crime, which is not focused on cybercrime. This is important to note, considering the previously mentioned argument that cybercrime might challenge existing theoretical frameworks (Borwell et al., 2021; Van der Wagen & Pieters, 2018). Furthermore, determinants influencing the impact can be specific to cybercrimes, such as the anonymity, permanence and geographical independence (Leukfeldt et al., 2018; Nadim & Fladmoe, 2021; Suler, 2004). Because of this, new theoretical concepts such as that of cyborg theory might be applied in future research. The idea behind this concept was introduced in section 4, and states that users of devices such as smartphones and computers have become a blend between human and machine. Those people may therefore be seen as transformed into a new sort of organism which Haraway (1985) called ‘cyborgs’ for short. This is expected to result in a disappearance of the experienced or actual boundaries between technology and the self in the event of an attacked device (Longo, 2018; Van der Wagen & Pieters, 2018). Some theoretical frameworks developed in the literature on the impact of traditional crime could also be successfully applied to the victimization impact of cybercrime. These include, for example, firstly the Shattered Assumptions Theory, which states that crime victimization leads to

impairment of positive basic assumptions about life, such as controllability, predictability, and righteousness (Janoff-Bulman & Frieze, 1983; Vanderstraeten et al., 2012); and secondly the General Strain Theory, which assumes that crime victimization produces 'strain' that leads to negative emotions and behaviors (Agnew, 1992; Hay & Ray, 2019).

To successfully compare the victimization impact of cybercrime and traditional crime, hypotheses based on studies about the determinants of victimization impact should be developed. The characteristics of crimes that, according to previous research, might influence victimization impact of crimes in general are 1) the intrusion into private or daily life of the victim; 2) the unpredictability, uncontrollability and intangibility of the crime; 3) the intentionality and purposefulness of the perpetrator; 4) the potential social distance between offender and victim; and 5) the degree of victim contribution to the crime (Agnew, 1985; Benight & Bandura, 2004; Borwell et al., 2021; Burgard & Schlembach, 2013; Dinisman & Moroz, 2017; Jahankhani et al., 2014; Jansen et al., 2013; Kunst & Koster, 2017; Lamet & Wittebrood, 2009; Leukfeldt et al., 2018; Moore, 2016). Those characteristics, as well as general theoretical frameworks, provide a resource to derive expectations about the victimization impact of different crimes and to explain established empirical results. In addition, they are the causal mechanisms explaining the victimization impact of different crimes, and thus form an opportunity to further study the applicability of those mechanisms. If necessary, they can be enhanced or developed when it comes to the victimization impact of cybercrime.

Personal and social factors are also related to victimization impact, and therefore need to be controlled for when measuring the impact of crime. Firstly, personal factors such as demographic and socio-economic factors, coping skills, personality, but also important life events such as previous victimization might influence victimization impact (Borwell et al., 2021; Button et al., 2014; Cross, 2015; Dinisman & Moroz, 2017; Golladay & Holtfreter, 2017; Lamet & Wittebrood, 2009; Li et al., 2019; Shapland & Hall, 2007). Therefore, the same crime can have varying effects for different victims, and the impact of a particular offence on an individual victim is hard to predict (Jansen & Leukfeldt, 2018; Shapland & Hall, 2007). Secondly, social factors are of influence on victimization impact, such as the degree of social support and the reaction of a victim's partner, social environment or law enforcement (Cross, 2015; Lamet & Wittebrood, 2009; Leukfeldt et al., 2018; Whitty & Buchanan, 2016). Victim blaming, mentioned earlier, can also be seen as a social factor that might heighten the victimization impact (Cross et al., 2016; Kerr et al., 2013; Leukfeldt et al., 2018; Whitty & Buchanan, 2016).

8 CONCLUDING REMARKS

This paper highlighted the importance of comparing the victimization impact of cyber and traditional crime. Based on a literature review, we gave an impression of the current state of literature on the subject, and what is yet to be discovered. It became clear that cybercrime can severely impact victims, while this impact seems to be underestimated and not thoroughly studied. Moreover, a comprehensive comparison with the impact of traditional crime has not been made. Cybercrimes have unique aspects that could affect the impact those crimes have for victims (Leukfeldt et al., 2018; Nadim & Fladmoe, 2021; Suler, 2004). The digitization of crime provides a unique opportunity to better understand the impact of crime on victims. Recommendations for future research were provided in order to address the gaps in the current state of literature. These are 1) distinguishing between cybercrime and traditional crime, 2) classifying cybercrime and traditional crime, i.e., determining what crimes can meaningfully be compared, and 3) measuring the victimization impact of cybercrime and traditional crime.

Ultimately, as long as the victimization impact of cybercrime compared to that of traditional crime is unclear, a nuanced and grounded discussion about the societal consequences of cybercrime and about policies that help victims to recover from the negative events they have experienced is deemed impossible.

REFERENCES

Agnew, R. S. (1985). Neutralizing the impact of crime. *Criminal Justice and Behavior*, *12*(2), 221–239. https://doi.org/10.1177%2F0093854885012002005

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, *9*(1), 35–54. https://doi.org/10.5281/zenodo.22239

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2015). A consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, *11*(4), 373–391. https://doi.org/10.1080/21582041.2015.1117648

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg.

Benight, C. C., & Bandura, A. (2004). Social cognitive theory of posttraumatic recovery: The role of perceived self-efficacy. *Behaviour Research and Therapy*, *42*(10), 1129–1148. https://doi.org/10.1016/j.brat.2003.08.008

Biemolt, J., Doeser, A., Glorioso, A. G., Hoogebeen, H. M., Oost, J., & Wansink, O. (2012). *Dienstverleningsconcept Nationale Politie* [National Police Service Concept]. Nationale Politie.

Blumer, H. (1954). What is wrong with social theory? *American Sociological Review*, *19*(1), 3-10. https://doi.org/10.2307/2088165

Boekhoorn, P. (2020). *De aanpak van cybercrime door regionale eenheden van de politie: Van intake van cybercrime naar opsporing en vervolging* [The handling of cybercrime by regional units of the police: From intake of cybercrime to investigation and prosecution]. BBSO.

Borwell, J., Jansen, J., & Stol, W. (2021). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review*, 1–22. https://doi.org/10.1177/0894439320983828

Brenner, S. W. (2004). Cybercrime metrics: Old wine, new bottles? *Virginia Journal of Law & Technology*, *9*(13), 1–52.

Bronfenbrenner, U. (1979). *The ecology of human development: Experiments by nature and design*. Harvard University Press.

Burgard, A., & Schlembach, C. (2013). Frames of fraud: A qualitative analysis of the structure and process of victimization on the internet. *International Journal of Cyber Criminology*, *7*(2), 112–124.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54. https://doi.org/10.1057/sj.2012.11

Button, M., Sugiura, L., Blackbourn, D., Shepherd, D. W. J., Wang, V., & Kapend, R. (2020). *Victims of computer misuse: Main findings*. University of Portsmouth.

Campbell, M., Spears, B., Slee, P., Butler, D., & Kift, S. (2012). Victims' perceptions of traditional and cyberbullying, and the psychosocial correlates of their victimisation. *Emotional and Behavioural Difficulties*, *17*(3–4), 389–401. https://doi.org/10.1080/13632752.2012.704316

Canetti, D., Gross, M., Waismel-Manor, I., Levanon, A., & Cohen, H. (2017). How cyberattacks terrorize: Cortisol and personal insecurity jump in the wake of cyberattacks. *Cyberpsychology, Behavior, and Social Networking*, *20*(2), 72–77. https://doi.org/10.1089/cyber.2016.0338

Correia, S. G. (2019). Responding to victimisation in a digital world: A case study of fraud and computer misuse reported in Wales. *Crime Science*, *8*(4), 1–12. https://doi.org/10.1186/s40163-019-0099-7

Council of Europe (2001). *Convention on Cybercrime, 185 European Treaty Series*. Council of Europe.

CPB. (2018). *Risicorapportage cyberveiligheid economie 2018* [Cybersecurity risk report economy 2018]. Centraal Planbureau.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187–204.

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, *518*, 1–14. https://doi.org/10.1177/0269758015571471

De Kimpe, L., Snaphaan, T., Hardyns, W., Walrave, M., Pauwels, L., & Ponnet, K. (2020). Zwijgen is zilver, spreken is goud? Het zoeken van formele en informele steun door slachtoffers van cybercriminaliteit [Silence is silver, speaking is gold? Seeking of formal and informal support by victims of cybercrime]. *Cahiers Politiestudies*, *56*, 151–176.

Dekker, S. (2018). *Meerjarenagenda slachtofferbeleid 2018-2021* [Multi-year agenda for victim policy 2018-2021]. Ministerie van Justitie en Veiligheid.

Diamond, B., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology*, *9*(1), 24–34. https://doi.org/10.5281/zenodo.22196

Dignan, J. (2005). *Understanding victims and restorative justice*. Open University Press. https://doi.org/10.1080/10345329.2007.12036410

Dinisman, T., & Moroz, A. (2017). *Understanding victims of crime: The impact of the crime and support needs*. Victim Support.

Domenie, M. M. L., Leukfeldt, E. R., Van Wilsem, J. A., Jansen, J., & Stol, W. Ph. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit* [Victimization in a digitized society: A study among citizens of e-fraud, hacking, and other common crimes]. Boom Lemma Uitgevers.

Frieze, I. H., Hymer, S., & Greenberg, M. S. (1987). Describing the crime victim: Psychological reactions to victimization. *Professional Psychology: Research and Practice*, *18*(4), 299–315. https://doi.org/10.1037/0735-7028.18.4.299

Furnell, S. (2001). The problem of categorising cybercrime and cybercriminals. *Proceedings of 2nd Australian Information Warfare and Security Conference 2001, 2*, 29-36.

Gale, J. A., & Coupe, T. (2005). The behavioural, emotional and psychological effects of street robbery on victims. *International Review of Victimology*, *12*(1), 1–22. https://doi.org/10.1177/026975800501200101

Gasson, M. N., & Koops, B. J. (2013). Attacking human implants: A new generation of cybercrime. *Law, Innovation and Technology*, *5*(2), 248–277. https://doi.org/10.5235/17579961.5.2.248

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, *12*(5), 741–760. https://doi.org/10.1080/15564886.2016.1177766

Graham, A., Kulig, T. C., & Cullen, F. T. (2019). Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing: An International Journal*, *43*(1), 1–16. https://doi.org/10.1108/PIJPSM-07-2019-0115

Groenhuijsen, M. (1996). Straftoemeting en de consequenties van een delict voor het slachtoffer [Punishment and the consequences of an offence for the victim]. *Delikt En Delinkwent*, *26*(7), 605–613.

Hageman, H., & Loeffen, B. (2016). *Individuele beoordeling slachtoffers: Plan van aanpak project IB politie 2016-2019* [Individual assessment of victims: Action plan project IB police 2016-2019]. Politie.

Hamby, S., Blount, Z., Smith, A., Jones, L., Mitchell, K., & Taylor, E. (2018). Digital poly-victimization: The increasing importance of online crime and harassment to the burden of victimization. *Journal of Trauma & Dissociation*, *19*(3), 382–398. https://doi.org/10.1080/15299732.2018.1441357

Haraway, D. (1985). A manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s. *Socialist Review*, *80*(1), 65–108. https://doi.org/10.1080/08164649.1987.9961538

Hay, C., & Ray, K. (2019). General strain theory and cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 583–600). Springer International Publishing AG.

Heinz, A., Steffgen, G., & Willems, H. (2015). *Victimization and Safety in Luxembourg—Findings of the "Enquête sur la sécurité 2013."* STATEC.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 475–497. https://doi.org/10.1177/1043986213507403

Henson, B., Reyns, B. W., & Fisher, B. S. (2016). Cybercrime victimization. In C. A. Cuevas & C. M. Rennison (Eds.), *The Wiley Handbook on the Psychology of Violence* (pp. 553–570). John Wiley & Sons, Ltd.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2019). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society*, *29*(8), 906–921. https://doi.org/10.1080/10439463.2018.1450409

Hulst, R. C. van der, & Neve, R. J. M. (2008). *High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie* [High-tech crime, types of crime and their perpetrators: A literature review]. Boom Juridische Uitgevers.

Huys, H. W. J. M. (2012). Criminaliteit en slachtofferschap [Crime and victimization]. In M. M. Van Rosmalen, S. N. Kalidien, & N. E. De Heer-de Lange (Eds.), *Criminaliteit en rechtshandhaving 2011: Ontwikkelingen en samenhangen* [Crime and law enforcement 2011: Developments and connections] (pp. 47–84). Boom Lemma Uitgevers.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In B. Akhgar, A. Staniforth, & F. Bosco (Eds.), *Cyber crime and cyber terrorism: Investigator's handbook* (pp. 149–164). Elsevier.

Janoff-Bulman, R., & Frieze, I. H. (1983). A theoretical perspective for understanding reactions to victimization. *Journal of Social Issues*, *39*(2), 1–17. https://doi.org/10.1111/j.1540-4560.1983.tb00138.x

Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 205–228.

Jansen, J., Leukfeldt, R., Kerstens, J., Veenstra, S., Van Wilsem, J., & Stol, W. (2013). Slachtofferschap in een gedigitaliseerde samenleving en kansen voor preventie [Victimization in a digitized society and opportunities for prevention]. In W. Stol & J. Jansen (Eds.), *Cybercrime en de politie* [Cybercrime and the police] (pp. 31–46). Boom Lemma uitgevers.

Keane, J., & Bell, P. (2013). Confidence in the police: Balancing public image with community safety – A comparative review of the literature. *International Journal of Law, Crime and Justice*, *41*(3), 233–246. https://doi.org/10.1016/j.ijlcj.2013.06.003

Kemp, S. (2020). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology,* 147737082094140. https://doi.org/10.1177/1477370820941405

Kerr, J., Owen, R., McNaughton Nicholls, C., & Button, M. (2013). *Research on sentencing online fraud offences*. Crown Copyright.

Kunst, M. J. J., & Koster, N. N. (2017). Psychological distress following crime victimization: An exploratory study from an agency perspective. *Stress and Health*, *33*(4), 405–414. https://doi.org/10.1002/smi.2725

Lamet, W., & Wittebrood, K. (2009). *Nooit meer dezelfde: Gevolgen van misdrijven voor slachtoffers* [Never the same again: Consequences of crime for victims]. Sociaal en Cultureel Planbureau (SCP).

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit* [Victimization of online crime: An examination of needs, consequences, and responsibilities following victimization of cybercrime and digitized crime]. WODC.

Leukfeldt, R., Kentgens, A., Prins, E., & Stol, W. (2015). *Alledaags politiewerk in een gedigitaliseerde wereld: Handreiking voor de intake van delicten met een digitale component* [Everyday policing in a digitized world: Guidance for the intake of crimes with a digital component]. Lectoraat Cybersafety.

Leukfeldt, R., Veenstra, S., Domenie, M., Stol, W., & Cybersafety, L. (2012). *De strafrechtketen in een gedigitaliseerde samenleving: Een onderzoek naar de strafrechtelijke afhandeling van cybercrime* [The criminal justice system in a digitized society: A study of the penal treatment of cybercrime]. Sdu Uitgevers.

Li, Y., Yazdanmehr, A., Wang, J., & Rao, H. R. (2019). Responding to identity theft: A victimization perspective. *Decision Support Systems*, *121*, 13–24. https://doi.org/10.1016/j.dss.2019.04.002

Swedish government (2017). *Regeringens proposition 2016/17:222: Ett starkt straffrättsligt skydd för den personliga integriteten* [Government proposal 2016/17:222: Robustcriminal law protection of the personal integrity]. Justitiedepartementet.

Longo, M. (2018). Exploring the subtle mental boundary between the real and the virtual. In A. Marzi (Ed.), *Psychoanalysis, Identity, and the Internet* (pp. 51–74). Routledge.

Maercker, A., & Müller, J. (2004). Social acknowledgment as a victim or survivor: A scale to measure a recovery factor of PTSD. *Journal of Traumatic Stress*, *17*(4), 345–351. https://doi.org/10.1023/B:JOTS.0000038484.15488.3d

Ministerie van Veiligheid en Justitie. (2017). *Informatieblad over de wet ter implementatie van de EU richtlijn minimumnormen slachtoffers* [Information sheet on the law implementing the EU Directive on minimum standards for victims]. Ministerie van Veiligheid en Justitie.

Mitchell, K. J., Finkelhor, D., & Becker-Blease, K. A. (2007). Linking youth internet and conventional problems: Findings from a clinical perspective. *Journal of Aggression, Maltreatment & Trauma*, *15*(2), 39–58. https://doi.org/10.1300/J146v15n02_03

Mittal, S. & Sharma, P. (2017). A review of international legal framework to combat cybercrime. *International Journal of Advanced Research in Computer Science, 8*(5), 1372-1374. https://doi.org/ 10.2139/ssrn.2978744

Modic, D., & Anderson, R. (2015). It's all over but the crying: The emotional and financial impact of internet fraud. *IEEE Security & Privacy*, *13*(5), 99–103.

Moitra, S. D. (2004). Cybercrime: Towards an assessment of its nature and impact. *International Journal of Comparative and Applied Criminal Justice*, *28*(2), 105–123. https://doi.org /10.1080/01924036.2004.9678719

Moitra, S. D. (2005). Developing policies for cybercrime. *European Journal of Crime Criminal Law and Criminal Justice*, *13*(3), 435–464. https://doi.org/10.1163/1571817054604119

Montoya, L., Junger, M., & Hartel, P. (2013). How "digital" is traditional crime? *2013 European Intelligence and Security Informatics Conference*, 31–37.

Moore, J. W. (2016). What is the sense of agency and why does it matter? *Frontiers in Psychology*, *7*, 1272. https://doi.org/10.3389/fpsyg.2016.01272

Nadim, M., & Fladmoe, A. (2021). Silencing women? Gender and online harassment. *Social Science Computer Review*, *39*(2), 245–258. https://doi.org/10.1177/0894439319865518

Neufeld, D. J. (2010). Understanding cybercrime. *Proceeding of the 43rd Hawaii International Conference On System Sciences*, 1–10.

Reep-Van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, *7*(5), 1–15. https://doi.org/10.1186/s40163-018-0079-3

Riek, M. (2017). *Towards a robust quantification of the societal impacts of consumer-facing cybercrime* [PhD Thesis]. Universitäts-und Landesbibliothek Münster.

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, *4*(1), 1–16. https://doi.org/10.1093/cybsec/tyy004

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, *4*(6), 165–176.

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. C. (2018). Responding to cybercrime: Current trends. *Police Practice and Research*, *19*(6), 515–518. https://doi.org/10.1080/15614263.2018.1507888

Shapland, J., & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology*, *14*(2), 175–217. https://doi.org/10.1177%2F026975800701400202

Sipma, T., & van Leijsen, E. M. C. (2019). *Slachtofferschap van online criminaliteit: Prevalentie, risicofactoren en gevolgen* [Victimization of online crime: Prevalence, risk factors, and consequences]. WODC.

Smit, P. R., Ghauharali, R., van der Veen, H. C. J., & Willemsen, F. (2018). *Tasten in het duister: Een verkenning naar bronnen en methoden om de aard en omvang van de criminaliteit te meten* [Groping in the dark: An exploration of sources and methods for measuring the nature and extent of crime]. WODC.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Statens Offentliga Utredningar (SOU). (2016). *Integritet och straffskydd* [Integrity and criminal law]. Wolters Kluwers.

Statistics Netherlands. (2020). *Veiligheidsmonitor 2019* [Safety monitor 2019]. Statistics Netherlands.

Statistics Netherlands (CBS). (2013). *Veiligheidsmonitor 2012* [Safety monitor 2012]. Statistics Netherlands.

Statistics Netherlands (CBS). (2018). *Cybersecuritymonitor 2018: Een verkenning van dreigingen, incidenten en maatregelen* [Cybersecurity Monitor 2018: An exploration of threats, incidents and measures]. Statistics Netherlands.

Stol, W. (2020). Digitalisering en criminaliteit: Een beknopte inleiding op cybercrime [Digitization and crime: A brief introduction to cybercrime]. *Cahiers Politiestudies*, *56*(3), 13–22.

Stol, W. P., van Treeck, R., & van der Ven, A. (1999). *Criminaliteit in cyberspace* [Criminaliteit in cyberspace] Elsevier.

Stol, W., & Strikwerda, L. (2019). *Law enforcement in digital society*. Boom Juridische Uitgevers.

Strikwerda, L. (2014). *Virtual acts, real crimes? A legal-philosophical analysis of virtual cybercrime* [PhD Thesis]. University of Twente. https://doi.org/10.3990/1.9789036537131

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, *7*(3), 321–326. https://doi.org/10.1089/1094931041291295

Ten Boom, A., Kuijpers, K. F., & Moene, M. H. (2008). *Behoeften van slachtoffers van delicten: Een systematische literatuurstudie naar behoeften zoals door slachtoffers zelf*

geuit [Needs of victims of crime: A systematic literature review of needs as expressed by victims themselves]. WODC.

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 1–20. https://doi.org/10.1109/TSMC.2017.2700495

UNODC. (2015). *International classification of crime for statistical purposes*. United Nations Office on Drugs and Crime.

Van Bourgondien, C. M. J. (2017). *Jaarverslag 2017 Programma Dienstverlening* [Annual Report 2017 Program Services]. Politie.

Van Caem, B., & Hageman, H. (2018). Dienstverlening en slachtofferzorg: Hoe krijgt de politie de basis op orde? [Services and victim care: How do police get the fundamentals right?]. In *Dienstverlening door de politie* [Services provided by the police] (pp. 33–48). Gompel & Svacina.

Van der Vijver, C. D. (1993). *De burger en de zin van strafrecht* [The citizen and the meaning of criminal law]. Koninklijke Vermande.

Van der Wagen, W., & Pieters, W. (2018). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, *17*(4), 480–497. https://doi.org/10.1177/1477370818812016

Van Dijk, A. J., & Hoogewoning, F. (2018). Dienstverlening in de context van de politie [Service delivery in the context of policing]. In *Dienstverlening door de politie* [Services provided by the police] (pp. 19–32). Gompel & Svacina.

Van Dijk, J. J. M., & van Mierlo, F. (2009). *Leemten in de slachtofferhulpverlening* [Shortcomings in victim support services]. Intervict.

Vanderstraeten, B., Mestdagh, K., Vanfraechem, I., & Aertsen, I. (2012). Slachtofferschap bij diefstal in woningen [Victimization in residential theft]. *Cahiers Integrale Veiligheid*, *2012*(2), 227–257.

Veenstra, S., Leukfeldt, R., & Boes, S. (2013). Criminaliteitsbestrijding in een gedigitaliseerde samenleving [Fighting crime in a digitized society]. In W. Stol & J. Jansen (Eds.), *Cybercrime en de politie* [Cybercrime and the police] (pp. 77–90). Boom Lemma Uitgevers.

Wall, D. S. (2005). The internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 77–98) Sage.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176–194.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177%2F147737080556056