Original Manuscript

Social Science Computer Review
1-22

DOI: 10.1177/0894439320983828
journals.sagepub.com/home/ssc
SAGE

The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory

Jildau Borwell[1,2,3], Jurjen Jansen[2], and Wouter Stol[1,2,4]

Abstract

While criminality is digitizing, a theory-based understanding of the impact of cybercrime on victims is lacking. Therefore, this study addresses the psychological and financial impact of cybercrime on victims, applying the shattered assumptions theory (SAT) to predict that impact. A secondary analysis was performed on a representative data set of Dutch citizens ($N = 33{,}702$), exploring the psychological and financial impact for different groups of cybercrime victims. The results showed a higher negative impact on emotional well-being for victims of person-centered cybercrime, victims for whom the offender was an acquaintance, and victims whose financial loss was not compensated and a lower negative impact on emotional well-being for victims with a higher income. The study led to novel scientific insights and showed the applicability of the SAT for developing hypotheses about cybercrime victimization impact. In this study, most hypotheses had to be rejected, leading to the conclusion that more work has to be done to test the applicability of the SAT in the field of cybercrime. Furthermore, policy implications were identified considering the prioritization of and approach to specific cybercrimes, treatment of victims, and financial loss compensation.

Keywords

cybercrime victimization, shattered assumptions theory, psychological impact, hacking, financial cybercrime, person-centered cybercrime

With the digitization of society, an important part of crime rates consists of online crimes (Holt & Bossler, 2014; Montoya et al., 2013; Reep-Van den Bergh & Junger, 2018). As a result, many

[1] Open University of the Netherlands, Heerlen, The Netherlands
[2] NHL Stenden University of Applied Sciences, Leeuwarden, The Netherlands
[3] Dutch National Police, The Netherlands
[4] Dutch Police Academy, The Netherlands

Corresponding Author:
Jildau Borwell, NHL Stenden University of Applied Sciences, Rengerslaan 8, 8917 DD Leeuwarden, The Netherlands.
Email: jildau.borwell@nhlstenden.com

victims are dealing with cybercrime. For example, 13% of Dutch citizens experienced cybercrime victimization in 2019, compared to 14% for traditional (violent, financial, or vandalism) crime (Statistics Netherlands, 2020). However, most theories and empirical studies on victimization and its impact focus on traditional crime (Aiken et al., 2015; Kunst et al., 2013; Lamet & Wittebrood, 2009). The results of those studies indicate that the impact of traditional crime on victims can be severe and long-lasting. Victimization can, for instance, lead to psychological problems, a lack of trust in other people, and a disruption of daily routines (Lamet & Wittebrood, 2009; Shapland & Hall, 2007). It is largely unclear whether the negative effects of victimization also apply to cybercrimes. This study therefore addresses the impact of cybercrime on victims.

Cybercrimes have some unique characteristics in a criminological and victimological sense, such as the possible physical distance between the victim and offender, the use of technology, and the intangibility of the means by which the crime is committed (Henson et al., 2016; Moitra, 2005). Some authors state that these characteristics urge to challenge existing theoretical and victimological frameworks in the cybercrime field (Hay & Ray, 2019; Van der Wagen & Pieters, 2018). However, there is a lack of theoretical advancement when it comes to cybercrime (Diamond & Bachmann, 2015). Most studies do not present an overarching theory to explain the victimization impact of cybercrime. Theories such as the shattered assumptions theory (SAT) and strain theory are commonly applied for the explanation of victimization impact resulting from traditional crime (Hay & Ray, 2019; Janoff-Bulman, 1999; Vanderstraeten et al., 2012). Nevertheless, it is unclear to what extent those theories are applicable to cybercrimes. As a result, a comprehensive, theory-based understanding of cybercrime impact on victims is lacking, and there is a need for studies to understand this impact (Li et al., 2019). Therefore, the aim of this study is to examine the impact of cybercrime on its victims and to explain that impact.

The few existing studies on the victimization impact of cybercrime suggest that this impact can be severe and can resemble that of traditional crime (Holt & Bossler, 2008). Cybercrime victims, for instance, seem to experience financial and psychological impacts in most cases (Leukfeldt et al., 2018). In some instances, cybercrime even led to victims committing suicide. This occurred, for example, after the hack of Ashley Madison, an online dating service for married people. The personal data of 30 million subscribers were disclosed, and some of them received extortion demands, resulting in two reported suicide cases (Chang et al., 2018). However, studies on the subject of cybercrime impact have limitations. They mostly focus on one or a few types of cybercrime, failing to establish a comprehensive overview (Jansen & Leukfeldt, 2018; Reep-Van den Bergh & Junger, 2018; Riek, 2017). For instance, the victimization impact of person-centered cybercrimes is often overlooked (Henson et al., 2016). Limitations also exist in the types of impact that are studied. The focus of most studies is on financial victimization impact, thereby ignoring psychological impact (Henson et al., 2016; Jansen & Leukfeldt, 2018; Leukfeldt et al., 2018; Li et al., 2019; Reep-Van den Bergh & Junger, 2018; Riek, 2017; Sipma & Van Leijsen, 2019). Hence, attention for the psychological impact of cybercrime is called for. Different types of impact are also not usually studied simultaneously, although such a combined approach can provide a more thorough insight because of the interdependencies between impact types (Li et al., 2019). For instance, the emotional impact of a burglary seems to be greater when the financial consequences are greater (Lamet & Wittebrood, 2009). In sum, more research is required to establish a comprehensive understanding of different impact types of different cybercrimes.

Since most studies on cybercrime victimization do not apply existing criminological and victimological theories to explain the impact of victimization, the applicability of those theories remains unclear. Nevertheless, the SAT seems suitable to explain the impact of cybercrime victimization. The SAT entails that victimization leads to the impairment of some basic, positive assumptions people have about themselves and the world, such as being invulnerable and autonomous, and the world being controllable and understandable (Janoff-Bulman & Frieze, 1983; Vanderstraeten et al., 2012). Shattering of those assumptions can have psychological, physical, social, and behavioral effects (Janoff-Bulman & Frieze, 1983), which may also apply to people who experienced cybercrime victimization. For instance, cybercrime victimization might lead to a reduced sense of invulnerability and the world being less controllable and understandable. This seems especially relevant for cybercrimes due to some specific characteristics such as the remoteness of cyberattacks and the technical complicatedness of the crimes (Jansen et al., 2013; Kerr et al., 2013; Leukfeldt et al., 2018).

This study focuses on the psychological and financial impacts of cybercrime victimization. The SAT is used to develop hypotheses about that impact. The hypotheses are tested for three different categories of cybercrimes that can be labeled as hacking, financial cybercrime, and person-centered cybercrime. The current study is unique in exploring the psychological and financial impacts of cybercrimes in different crime categories, thereby increasing our understanding of the subject. Furthermore, it contributes to theory building in the domain of cybercrime because the SAT, to the best of our knowledge, has not yet been applied here. Results of this study can help improve the social and judicial responses to victims by government agencies such as the police. Hence, insight into the victimization impact of cybercrime may help to set the right priorities and to treat victims appropriately (Jansen & Leukfeldt, 2018; Li et al., 2019).

Literature Review and Expectations From the SAT

Victimization Impact of Cybercrime

Cybercrime contains unique elements that might influence the victimization impact on victims. In this study, cybercrime is defined as a crime for which information and communication technology plays an essential role in the execution of the offense (Domenie et al., 2013). Victimization impact is defined as the seriousness or severity of the effects of criminality as perceived by victims (Dignan, 2005; Groenhuijsen, 1996). Examples of the unique cybercrime victimization elements are the scale on which victims can be approached, the technology that is part of the offense and its anonymity, intangibility, and remoteness (Agustina, 2015; Diamond & Bachmann, 2015; Kerr et al., 2013; Leukfeldt et al., 2018; Moitra, 2005; Wall, 2005). In addition, some cybercrimes have a permanent nature, resulting in a longer duration or multiple occurrences of victimization (Jahankhani et al., 2014; Leukfeldt et al., 2018; Van der Wagen & Pieters, 2018). For instance, images that are part of the cybercrime might remain online, and cybercrime offenders can reach victims in their homes at any time (Hay & Ray, 2019; Leukfeldt et al., 2018).

The abovementioned cybercrime elements that can influence the impact of cybercrime might have an even stronger effect now the Internet is ubiquitous in daily life (Kerr et al., 2013). Moreover, this ubiquity might render it incorrect to view the computers involved in cybercrimes as mere tools. Computers are devices people are connected to and dependent upon (Van der Wagen & Pieters, 2018). According to the cyborg theory, people nowadays can experience devices as an extension of the self. Longo (2018) states that we relate ourselves to our devices as if they were human. In that sense, victims might experience a disappearance of boundaries between body and device (Agustina, 2015; Van der Wagen & Pieters, 2018). This can result in attacks on the devices we are connected to and dependent upon being experienced as particularly impactful.

Although the foregoing makes clear that cybercrimes can have a significant impact on its victims, cybercrime victims are often held accountable for their own victimization. "Blaming the victim" by the cybercrime victims' social surroundings and legal institutions takes place relatively often (Cross, 2015; Leukfeldt et al., 2018). This might be strengthened by the fact that many cybercrime victims actively contribute to the crime, in the sense that certain actions of the victim, such as providing login details, are needed to complete the crime (Burgard & Schlembach, 2013; Jansen & Leukfeldt, 2018; Leukfeldt et al., 2018; Van der Wagen & Pieters, 2018). This can heighten feelings of guilt and shame for victims and lead to a lack of support by their surroundings (Leukfeldt et al., 2018). Negative or unsupportive reactions can add to the psychological impact of victimization, for instance, by enhancing feelings of isolation, shame, and insecurity (Cross, 2015; Kerr et al., 2013; Van der Vijver, 1993). Therefore, blaming cybercrime victims might add to the already substantial victimization impact.

Some authors state that the impact of cybercrime victimization is relatively high (Hay & Ray, 2019; Leukfeldt et al., 2018), which seems plausible considering the foregoing. However, it is hard to draw conclusions about cybercrimes in general. The impact of different traditional crimes is known to differ a lot (Lamet & Wittebrood, 2009; Shapland & Hall, 2007). This is presumably also the case for cybercrimes, but there is insufficient insight in the impact of different cybercrime forms and how they compare to each other (Leukfeldt et al., 2018). Research on traditional crime shows that the causal mechanisms for victimization impact can be applied to different crime forms (Golladay & Holtfreter, 2017). Whether this is also the case for cybercrimes remains unclear. To acquire knowledge about this, a classification of cybercrimes and the different types of victimization impact needs to be established.

Categorizing Cybercrime and Victimization Impact

Cybercrime encompasses many different illegal activities and thus different forms of victimization (Correia, 2019; Van der Wagen & Pieters, 2018). Therefore, it is important to divide cybercrime into different subcategories. For example, cybercrimes can be person-centered, such as online stalking, but can also be less focused on an individual target, such as large-scale phishing campaigns (Van der Wagen & Pieters, 2018). Previous studies have chosen various classifications of cybercrimes. The current study employs a commonly used classification: cybercrime aimed at (1) a device, (2) money, or (3) the person of the victim (Correia, 2019; Furnell, 2001; Leukfeldt et al., 2018; Statistics Netherlands, 2019). Later in this article, this will be referred to as (1) hacking; (2) financial cybercrime such as payment fraud, consumer fraud, and Wangiri fraud; and (3) person-centered cybercrime such as online threat and online stalking.

Apart from the categorization of different cybercrimes, categorization of the resulting victimization impact also needs to be established. Previous literature suggests a broad division of four victimization impact types, namely physical, financial/material, psychological, and social/behavioral (Lamet & Wittebrood, 2009). Those impact types are often interrelated. For instance, the psychological impact of a crime can be more severe if the financial impact of that crime is greater (Kerr et al., 2013; Lamet & Wittebrood, 2009). Physical and emotional impacts are also often intertwined (Shapland & Hall, 2007). Physical impact can be direct such as injuries from physical assault (Lamet & Wittebrood, 2009; Vanderstraeten et al., 2012). Today, direct physical impact caused by cybercrimes does most probably not exist[1] (Kerr et al., 2013). Indirect physical impact such as skin problems, sleep deprivation, headaches, and weight loss is more common in cybercrime victimization. This often results from and can therefore be considered a part of the psychological impact of crime (Dinisman & Moroz, 2017; Huys, 2012; Kerr et al., 2013; Lamet & Wittebrood, 2009; Van der Vijver, 1993; Vanderstraeten et al., 2012). In this study, mere physical impact is not taken into account. Furthermore, we limit financial/material impact to financial impact since material impact other than financial impact is not included in the data set. Psychological impact is a focus point in this study. Finally, social/behavioral impact is not taken into account because the data set does not include this impact type. It can also be mentioned that social or behavioral impact often results from financial or psychological impact (Brands & Van Wilsem, 2019; Kerr et al., 2013; Sipma & Van Leijsen, 2019).

The focus of this study is on psychological and financial impact. Financial impact is often used to measure the impact of crime and applies to most cybercrimes (Kerr et al., 2013; Lamet & Wittebrood, 2009; Leukfeldt et al., 2018). Sometimes, indirect costs such as time and resources used to solve the problem, or loss of income due to inability to work, are also regarded as financial impact (Kerr et al., 2013; Shapland & Hall, 2007). Other authors only count direct costs such as stolen money or damaged goods (Shapland & Hall, 2007). In this study, financial loss is financial loss as perceived by the victim, not differentiating between direct and indirect costs. Psychological impact can for instance consist of fear, shock, and anger (Lamet & Wittebrood, 2009; Shapland & Hall, 2007). Over a longer time frame, those effects may lead to severe mental conditions such as post-traumatic stress disorder (PTSD; Dinisman & Moroz, 2017; Kunst & Koster, 2017; Shapland & Hall, 2007). For cybercrime victims, previous research shows that psychological impact can consist of stress, anxiety, anger, and fear of repeat victimization (Brands & Van Wilsem, 2019; Kerr et al., 2013; Sipma & Van Leijsen, 2019).

Theoretical Explanations for Cybercrime Victimization Impact

Although cybercrime victimization is a rapidly expanding field in criminology, theoretically oriented cybercrime research is a new development and provides a fragmented picture, requiring more research (Holt & Bossler, 2014; Van der Wagen & Pieters, 2018). Some traditional crime theories, such as routine activities theory, social learning theory, and self-control theory, seem applicable to cybercrime with a few small adjustments (Diamond & Bachmann, 2015; Hay & Ray, 2019; Holt & Bossler, 2008). However, those theories predict why people become cybercrime victims, while theories about the impact of their victimization seem absent. Some authors state that existing theoretical frameworks are not suitable for cybercrime because of the technical aspects involved, rendering cybercrime a victimologically and sociologically new phenomenon (Van der Wagen & Pieters, 2018). However, not all theories that could be applicable to cybercrime have yet been applied (Hay & Ray, 2019; Holt & Bossler, 2014). The applicability of traditional victim approaches in criminology and victimology to cybercrime victimization impact therefore remains unclear (Van der Wagen & Pieters, 2018). In this study, the applicability of the SAT will be explored.

The SAT Applied to Cybercrime Victimization Impact

According to the SAT, people have cognitive baggage that consists of assumptions and expectations they hold about themselves and the world (Janoff-Bulman & Frieze, 1983). People operate based on those assumptions to plan, set goals, and order their behavior. When people are victimized by, for instance, crime, those assumptions are challenged and cannot explain what happened. Their assumptions are therefore shattered, resulting in psychological reactions such as anxiety, fear, sleep disturbance, and helplessness. Relatively mild victimizations, such as burglary and robbery, can lead to severe suffering and disruption of victims' lives (Janoff-Bulman, 1985). Although reactions of individual victims differ, their psychological reactions often resemble each other (Janoff-Bulman & Frieze, 1983). Psychological reactions to victimization mostly start directly after the crime and can be intense. Reactions can vary from shock, helplessness, anxiety and depression to PTSD, feelings of detachment, and phobias (Janoff-Bulman & Frieze, 1983).

There are three assumptions that most people have in common and that are particularly shattered by victimization: (1) the belief in personal invulnerability, (2) the perception of the world as meaningful and comprehensible, and (3) the view of ourselves in a positive light. Those three assumptions are strongly interrelated (Janoff-Bulman & Frieze, 1983). In the following, the three assumptions are explained and subsequently applied to the impact of cybercrime victimization by formulating hypotheses. The hypotheses derived from the SAT are also compared with results and expectations from other studies on victimization impact.

The first assumption is *the belief in personal invulnerability*. This entails that people generally underestimate the chance of bad things, such as crime victimization, happening to them (Janoff-Bulman, 1985). This belief ensures that people do not live under constant anxiety, fear, and perceived threats of misfortune. When people become victims, the assumption of invulnerability is shattered, and they can see themselves in the role of a victim relatively easily. This assumption might be extended in the scope of cybercrime, including the assumption that nothing bad will happen to people's devices.

Crime in general can be particularly distressing when victimization is human-induced because the victim was deliberately damaged by another human being (Janoff-Bulman, 1985). After that, the world can seem like a threatening place with other people who cannot be trusted, which can lead to severe psychological effects. Because of the personal attack of an individual victim by another human being, the psychological impact is expected to be higher for person-centered cybercrime than for financially driven cybercrime or hacking. For person-centered cybercrimes such as stalking, liber/slander, or threat, the focus lies specifically on the victim as a person, which is expected to result in a higher psychological impact. This seems to be illustrated by earlier studies on cybercrime victimization concluding that person-centered cybercrimes can lead to emotional consequences resembling those of violent crime (e.g., Henson et al., 2016). For many financially or device-driven cybercrimes, the focus is not on the individual victim as a person, and direct contact with the offender is often absent (Van der Wagen & Pieters, 2018). This might make the crime feel less human-induced and less targeted, leading to less shattered assumptions. For instance in the case of phishing, emails are sent out to many, often random, potential victims. Furthermore, hacking seems more device-centered than person-centered, although the distinction is not always sharp. Other studies also suggest that the intentionality or targeting of the crime influences the impact on the victim (Dinisman & Moroz, 2017; Van der Vijver, 1993). Based on the notions above, we state our first hypothesis as follows:

Hypothesis 1: The psychological impact of person-centered cybercrime is higher than the psychological impact of financial cybercrime or hacking.

Another expectation from the assumption of belief in personal invulnerability is that the psychological victimization impact is higher if the offender was an acquaintance or if victims were in contact with the offender more intensively prior to the event. The assumption is expected to be more heavily shattered when people felt safe or familiar with the offender, which ends up not being justified. Other studies also suggest that crime by a known offender is more traumatic because it heightens the chance of repeat victimization and the risks of encountering the perpetrator again, evoking negative memories (Agnew, 1985; Lamet & Wittebrood, 2009). When the contact between offender and victim was shorter, less loss of trust in humanity seems to take place after victimization (Leukfeldt et al., 2018). Thus, we arrive at our next hypotheses:

Hypothesis 2: The psychological impact of cybercrime is higher if the offender was acquainted than if the offender was unacquainted.

Hypothesis 3: The psychological impact of cybercrime is higher if the victim was in contact with the offender more intensively prior to the offense.

The second assumption is the *perception of the world as meaningful and comprehensible*. This assumption rests on the idea that the world makes sense and that events are controllable and understandable (Janoff-Bulman, 1985). By behaving as good and worthy people and being cautious, people expect positive things to happen to them. This closely resembles Lerner's "just world theory," about the sense of justice and people getting what they deserve (Janoff-Bulman, 1985). The idea of this theory is that good things happen to good people and bad things happen to bad or at least irresponsible people (Pemberton, 2012). If people are victimized while they were cautious and decent people, the world does not seem to make sense anymore, and it is hard for victims to explain why they particularly had to become victimized ("why me?"; Janoff-Bulman, 1985).

For cybercrime victims, the world might seem meaningful and comprehensible again when financial loss is compensated since this could reconfirm that good things happen to good people (Van der Vijver, 1993). Therefore, the psychological impact is expected to be lower for victims who experienced loss, when that loss is compensated. However, some studies seem to challenge this idea (Button et al., 2014; Jansen & Leukfeldt, 2018). The former aligns with the idea about loss compensation from the just-world theory. From this theory, victim blaming is expected to take place less if victims are compensated (Pemberton, 2012; Van der Vijver, 1993). Financial compensation would have the symbolic function of taking victims seriously and demonstrating that they were not to blame for the crime (Van der Vijver, 1993). A study on online fraud also suggests that reimbursement of loss is an important way to overcome victimization impact (Kerr et al., 2013). Consequently, our fourth hypothesis is as follows:

Hypothesis 4: The psychological impact of cybercrime victims who experienced financial loss is lower when the loss was compensated.

Another expectation from the second assumption is that the victimization impact of cybercrime is lower for people who actively contributed to the crime because they can formulate an answer to the "why me?" question more easily. Indeed, those who actively contributed would also have a clearer idea of how to prevent the crime from happening in the future. This aligns with other research, suggesting that victimization impact is higher when a crime is more unpredictable and uncontrollable (Benight & Bandura, 2004; Brands & Van Wilsem, 2019; Kunst & Koster, 2017), assuming that this is less the case when people actively contribute to the crime. It also aligns with the concept of locus of control and self-efficacy. If victims perceive behavioral control over outcomes – internal locus of control – they feel able to prevent a crime from happening again (Ajzen, 2002). However, other studies expect a higher impact if victims feel like they could have prevented the crime and are blamed for it by themselves or others, especially if they actively contributed to it (Agnew, 1985; Burgard & Schlembach, 2013; Dinisman & Moroz, 2017; Kunst & Koster, 2017; Leukfeldt et al., 2018; Whitty, 2015). According to Kunst and Koster (2017), those victims might experience more problems with emotions and restoring agency. Thus, other studies point in a different direction than the expectations derived from the SAT. Based on the SAT, however, we expect:

Hypothesis 5: The psychological impact of cybercrime is lower for victims who actively contributed to the crime than for victims who did not actively contribute to the crime.

The third assumption is the *view of ourselves in a positive light* (Janoff-Bulman, 1985). Most people have an underlying idea of being a worthy, decent person, which is a precondition for building self-confidence (Janoff-Bulman, 1985). This also has to do with the perception of operating autonomous. Crime victimization can lead to the questioning of this assumption since it leads to negative self-images of weakness, helplessness, being needy, and being out of control. Victimization also feels like a threat to autonomy, experiencing this unwanted and unexpected misfortune (Janoff-Bulman, 1985). When applied to cybercrime victims, we expect people with less affected autonomy to experience less shattered assumptions. This might be the case for people actively contributed to the crime, which aligns with Hypothesis 5. Furthermore, it is likely that people whose assumptions have been challenged less during their lives experience more heavily shattered assumptions and therefore more severe psychological victimization impact (Janoff-Bulman, 1985). This could be related to socioeconomic status (SES): People with a higher standing might not have had to deal with a setback very often. Therefore, we expect people with a higher SES to experience higher victimization impact than people with lower SES. Other studies, however, contradict this expectation. For instance, people with low SES seem to experience a higher impact of identity theft victimization (Golladay & Holtfreter, 2017). Other research also suggest that people with a higher SES experience lower victimization impact for reasons such as access to resources (Agnew, 1985; Dinisman & Moroz, 2017). However, from the SAT, we arrive at our final hypothesis:

> **Hypothesis 6:** The psychological impact of cybercrime is higher for victims with a higher SES than for victims with a lower SES.

Materials and Methods

This study consists of a secondary analysis of a representative data set of Dutch citizens aged 18 and over (N = 33,702). The data were collected by Statistics Netherlands (2019) from October until December 2018. The original study used online surveys in order to gain insight into, among other topics, victimization of different cybercrimes and their financial and psychological impact. For the current study, new possible connections in the data were explored, leading to new results and insights. In the original data set, a weighing method was applied to correct for deviations, resulting in representative results for the goal population. Because the purpose of the current study was to compare the impact of cybercrimes and to uncover what related to this impact, as opposed to the prevalence of the several crimes, the weighing model was not applied.

Distributions and Divisions

Of the 33,702 respondents, 51.3% were administrated as male and 48.7% as female. Their average age was 51.6 (SD = 17.29). Most respondents used the Internet daily, namely 91.8%. Note that respondents who did not use the Internet were already excluded from the original data set. Ten types of cybercrime were selected from the original data set, which can be divided into hacking, six financial cybercrimes, and three person-centered cybercrimes.

In the questionnaire, hacking is defined as breaking into a device. Financial cybercrime is divided into six categories: (1) online banking fraud, where the offender has direct access to the bank account of the victim with the goal to withdraw money or make payments; (2) identity fraud (orders), where the offender had direct access to an account where orders can be placed for a loan, subscription, goods, or services; (3) consumer fraud, where victims payed for something they did not receive or delivered something they did not get payed for; (4) fake fine/bill/campaign, where victims payed for a fine, bill, or campaign which later appeared fraudulent; (5) Microsoft scam, where offenders called victims about a so-called problem with their computer and offered to resolve it against payment; and (6) Wangiri fraud, where offenders called many victims and redirected them to an expensive pay phone number. Person-centered cybercrime is divided into three categories: (1) stalking, where an offender consciously and repeatedly harassed a victim online; (2) violent threat, where a victim received online threats of violence; (3) libel/slander, where stories, gossip, pictures, or videos about the victim were distributed online, messages were posted under their name on an Internet forum or social media, or an embarrassing or insulting website or profile was created about them.

Operationalization

Cybercrime victimization. For each type of cybercrime, respondents were asked whether they had been victimized in the past five years, and if so, whether this happened in the last twelve months.

Follow-up questions were asked about the last occurring crime in the last twelve months. We have excluded the 364 respondents who reported victimization of multiple cybercrime types from the data set since this number was too small for a comprehensive comparison, while multiple victimization might alter the impact of crime on victims (Van der Vijver, 1993).

For consumer fraud and fake fine/bill/campaign, victims without financial loss were not included in the original data set (Statistics Netherlands, 2019). For consumer fraud, the answers of victims who reported being partially compensated were also not included as victims by Statistics Netherlands because this was considered unlikely for this crime form. However, we included respondents who experienced payment and identity fraud (orders) without financial loss as victims. In those cases, the offender gained access to their online accounts, which we consider to be victimization. However, we excluded Microsoft fraud and Wangiri fraud without financial loss because those crimes can be considered as mere attempts to victimize the respondents. Furthermore, when hacking was part of the modus operandi (MO) of another offense, the case was included under that particular crime. In total, 2,415 cybercrime victims were included in our data set: 502 victims of hacking, 1,482 victims of financial cybercrime, and 431 victims of person-centered cybercrime.

Financial impact. Per type of cybercrime, respondents were asked whether they suffered any financial loss as a result of the crime, and if so, if they were compensated for the loss: (1) financial loss, fully compensated; (2) financial loss, partly compensated; (3) financial loss, not compensated; (4) no financial loss; and (5) do not know. The "do not know" category was not included in the data set. Because the N for partial compensation was low ($N = 17$), we added those cases to the "fully compensated" group, resulting in the group "compensated."

Psychological impact. Per crime type, victims were asked whether one or more of the following consequences applied to them as a result of the offense: (1) less trust in digital safety; (2) less trust in own digital skills; (3) fear of repeat victimization; (4) keep thinking about it; (5) anger; (6) sleep deprivation; (7) other, namely . . . ; and (8) none of the above. This resulted in dichotomous variables for every impact type of each crime (0 = no; 1 = yes). Sleep deprivation is regarded as physical impact in some studies (Averdijk, 2010; Golladay & Holtfreter, 2017; Randa & Reyns, 2019). Because of earlier mentioned reasons, namely indirect physical impact being a result of psychological impact, it is included under psychological impact in this study.

For scale construction, the different impact items for every included crime type were computed. Subsequently, the constructed variables were subjected to principal component analysis (PCA). The Kaiser–Meyer–Olkin value was 0.67, exceeding the recommended value of 0.6 (Tabachnick et al., 2007). The Bartlett test of sphericity reached statistical significance ($p < .01$). Factor analysis was therefore considered suitable. PCA revealed the presence of two components with an eigenvalue above 1, namely 1.83 (component 1) and 1.15 (component 2), explaining, respectively, 30.41% and 19.23% of the variance. The impact variables "keep thinking about it," "anger," and "sleep deprivation" loaded strongly (respectively, .74, .69, and .68) on the first component. The impact variables "less trust in digital safety," "less trust in own digital skills," and "fear of repeat victimization" loaded strongly (respectively, .78, .66, and .61) on the second component.

Thus, our analysis shows two different types of psychological impact. The first component concerns a direct impact on the inner emotional condition of the victim, which we shall henceforth call "emotional well-being" (e.g., Button et al., 2009). The second component has to do with trust in the digital environment and with expecting and fearing a potential cybercrime victimization situation in the future. In other words, this component refers to how secure victims feel in the "outside" digital world. We name the second component 'cybercrime-related sense of security," henceforth called "sense of security." See Berg and Johansson (2016) for prior use of the term "crime-related insecurity." Cronbach's α coefficient for emotional well-being was .48 and for sense of security .44.

This is considered low, which may have been caused by the small number of items in each scale. Therefore, we also examined the mean interitem correlations. Those were all between the recommended range of .2–.4 for the Emotional Well-Being Scale, and all except one, which was .19, for the Sense of Security Scale (Briggs & Cheek, 1986). This was considered sufficient to conduct further analyses with the two psychological impact scales.

Acquainted offender and intensity of contact. To operationalize whether the offender was acquainted and how much contact a victim had with them prior to the offense, different survey questions were used. The answers of victims were included in the data set for the person-centered cybercrimes types. They were asked whether they knew who the offender was (yes or no), and if so, whether the offender was a partner, an ex-partner, a family member, a neighbor, a friend, someone from school, a colleague, or another acquaintance. Victims who knew the offender were also asked how much contact they had with them prior to the offense: (1) daily, (2) at least once a week but not daily, (3) at least once a month but not weekly, (4) less than once a month, and (5) never. Because the number of respondents who were in contact with the offender at least once a month but not weekly was low ($N = 25$), they were added to the group "at least once a week but not daily," thereby creating the category "at least once a month but not daily."

Active contribution to the crime. In order to include active contribution for the different crime types, several indicators of victims contributing or not contributing were used. In all cases, the questions were focused on how the crime took place. Victims could also give open answers, which were not taken into account.

For the hacking variables, victims were asked in what way the device was broken into. Eleven different options were presented, of which they could choose several. When they (consciously or by accident) installed a program via the computer in the Internet, this was counted as an active contribution. If victims responded that someone else installed a program or someone gained physical access to the computer, this was counted as nonactive contribution.

For the financial cybercrimes online banking fraud and identity fraud (orders), victims were asked how someone (presumably) attained their personal information. Fourteen options were presented, of which they could choose several. If they responded handing over someone their banking card in good faith; transferring their personal credentials in good faith, being transferred to a fake or untrustworthy website via email (phishing/pharming); or transferring data on a webshop or via the telephone, this was considered as an active contribution. The following options were counted as nonactive contribution: taking over the victim's identity by theft of passport or ID card; theft of banking card/credit card; skimming of banking card/credit card; scanning of mobile phone, for instance, with contactless payment (shimming); copying of personal data via the Internet by breaking into the device (e.g., computer/tablet/telephone), social media, or email account; via malware (computer virus or Trojan horse); via registering keystrokes (keylogging); or by a hack at a company or bank where the personal data were stored. It should be noted that active contribution in the latter cases cannot be dismissed entirely. For instance, malware could have been installed because a victim clicked on a malicious link.

For all person-centered cybercrimes, victims were asked how their data were obtained. Eight options were presented. The following answers were counted as actively contributing: spreading information or photos themselves in good faith; transferring personal credentials in good faith, being transferred to a fake or untrustworthy website via email (phishing/pharming); or transferring data on a webshop or via the telephone. Copying of personal data via the Internet by breaking into a device (e.g., computer/tablet/telephone), social media, or email account was counted as nonactive contribution.

SES. SES was measured by asking respondents which description suits them best: (1) working with payed job/self-employed, (2) unemployed, (3) volunteer, (4) incapacitated, (5) student, (6) house-father or househusband/housemother or housewife, (7) pensioner, (8) none of the above, and (9) refusal. Options 2, 3, 4, and 6 were regarded as "unemployed." The last two options were considered missing. An income variable was added to the data set based on background information about the respondents in possession of Statistics Netherlands. Respondents were subdivided into five ascending income categories of 20%.

Results

To provide an overview of the data, the mean impact scores that were computed for every cybercrime type on emotional well-being and sense of security are shown in Table 1. Impact in this study refers to a negative effect; things are getting worse. All impact variables can rank from 1 (no psychological impact) to 4 (psychological impact on every item of the scale).

To assess whether the psychological victimization impact of person-centered cybercrime is higher than the psychological impact of financial cybercrime or hacking (Hypothesis 1), two one-way analysis of variance (ANOVA) tests were conducted. Respondents were divided into three groups according to crime type, and their psychological impact scores were compared. The mean impact score on emotional well-being was 1.27 ($SD = .58$) for hacking, 1.50 ($SD = .72$) for financial cybercrime, and 1.62 ($SD = .85$) for person-centered cybercrime, see Table 2. A Welch test was performed because Levene's test indicated that the variance in scores differed for the three groups. It showed a statistically significant difference between the groups: $F2(2, 922.79) = 36.72, p < .01$. Post hoc comparisons using the Tukey honestly significant difference (HSD) test indicated a difference between each of the groups with $p < .01$, supporting the hypothesis that the psychological impact of person-centered cybercrime is higher than that of financial cybercrime or hacking. The second ANOVA test showed that the mean impact score on sense of security was 1.80 ($SD = .94$) for hacking, 1.71 ($SD = .83$) for financial cybercrime, and 1.42 ($SD = .71$) for person-centered cybercrime. A Welch test showed a statistically significant difference between the groups: $F2(2, 929.86)$, $p < .01$. Post hoc tests revealed differences between the mean impact scores of person-centered cybercrime and hacking and of person-centered crime and financial cybercrime at $p < .01$. Those results were opposite to what was expected from the first hypothesis. Hypothesis 1, therefore, was confirmed for emotional well-being and not confirmed for sense of security.

To test whether the psychological impact of cybercrime was higher if the offender was acquainted than if the offender was unacquainted (Hypothesis 2), two independent samples t tests were performed comparing the two groups. The mean impact score on emotional well-being for victims who were acquainted with the offender was 1.75 ($SD = .89$). This was higher than the mean score for victims who were not acquainted with the offender, namely 1.43 ($SD = .75$). The result was significant and supported Hypothesis 2: $t(396.38) = -3.96$, $p < .01$ (two-tailed, equal variances not assumed). There was no statistically significant difference between the mean impact scores on sense of security for victims who were and who were not acquainted to the offender: $t(343.16) = 1.95$, $p = .05$ (two-tailed, equal variances not assumed), not supporting Hypothesis 2. Further analysis showed no significant effect from the type of known offender for both psychological impact types. In conclusion, Hypothesis 2 was confirmed for emotional well-being but not for sense of security.

Two one-way ANOVA tests were performed to compare the mean impact scores for emotional well-being and sense of security of victims grouped according to the amount of contact with the offender (Hypothesis 3). No significant differences in emotional well-being means were found $F(3, 259) = 2.08$, $p = .1$. Although Levene's test showed a difference in variances, the Welch test was not used because it showed a significant result while post hoc comparisons did not. A Welch test

Table 1. Descriptive Psychological Victimization Impact Different Crime Types.

Cybercrime Types	Mean Psychological Impact—Emotional Well-Being (*SD*)	Mean Psychological Impact—Sense of Security (*SD*)	*N*
Hacking[a]	1.27 (.58)	1.80 (0.94)	502
Financial cybercrime[b]			
Online banking fraud	1.42 (.71)	1.85 (0.88)	212
Identity fraud (orders)	1.46 (.76)	1.91 (0.92)	178
Consumer fraud	1.53 (.70)	1.64 (0.77)	856
Fake fine/bill/campaign	1.67 (.98)	1.87 (0.92)	75
Microsoft fraud	1.52 (.89)	1.62 (0.79)	42
Wangiri fraud	1.38 (.55)	2.01 (1.08)	119
Person-centered cybercrime			
Stalking	1.68 (.90)	1.50 (0.79)	119
Libel/slander	1.61 (.85)	1.44 (0.70)	273
Violent threat	1.54 (.76)	1.05 (0.22)	39

[a]When hacking was part of the modus operandi of another offense, the case was included under that particular crime.
[b]For consumer fraud and fake fine/bill/campaign, victims without financial loss were not included in the original data set. Cases without financial loss were excluded for Microsoft fraud and Wangiri fraud.

to compare the mean impact scores on sense of security showed no significant difference between the means: $F2(3, 132.19) = 1.65$, $p = .18$. Hypothesis 3, therefore, was not supported.

To test whether the psychological impact of cybercrime victims who experienced financial loss is lower when that loss was compensated (Hypothesis 4), two one-way between-groups ANOVA tests were conducted. Hereby, the mean impact scores on emotional well-being and sense of security of the three groups (no financial loss; financial loss, compensated; and financial loss, not compensated) were compared. For emotional well-being, a Welch test was performed, which showed a difference between the groups: $F2(2, 801.25) = 11.15, p < .01$. Post hoc comparisons using the Tukey HSD test indicated that the mean impact score of the group with compensated loss ($M = 1.39$, $SD = .69$) was lower than that of the group with uncompensated loss ($M = 1.56$, $SD = .74$) with $p < .01$. There was no significant difference with the group without loss ($M = 1.42$, $SD = .72$). The mean of the group without loss was also lower than the group with uncompensated loss at $p < .01$. The results support Hypothesis 4. A Welch test was conducted to compare the mean sense of security impact scores for the three groups. No significant differences were found: $F2(2, 783.25) = 1.65, p = .19$. Therefore, Hypothesis 4 was confirmed for emotional well-being but not for sense of security.

Two independent samples *t* tests were conducted to compare the impact on emotional well-being and sense of security for cybercrime victims who did and who did not actively contribute to the crime (Hypothesis 5). The differences in means were not statistically significant for emotional well-being: $t(307) = -1.59, p = .11$ (two-tailed; equal variances not assumed), nor for sense of security: $t(344) = 0.16, p = .88$ (two-tailed; equal variances assumed). Hypothesis 5 was therefore rejected.

To test whether the psychological impact of cybercrime is higher for victims with a higher SES (Hypothesis 6), two two-way between-groups ANOVA tests were conducted. Respondents were grouped according to income level (Group 1: lowest 20%–Group 5: highest 20%) and employment situation. There was no significant interaction effect between income level and employment situation for emotional well-being, $F(12, 2296) = 0.70, p = .75$. There was a significant main effect of income level, $F(4, 2296) = 3.98$, $p = < .01$. Post hoc comparisons using the Tukey HSD test showed a lower mean impact score on emotional well-being for income Group 5 ($M = 1.36$, $SD = .63$) than for Groups 1 ($M = 1.53$, $SD = .80$), 2 ($M = 1.50$, $SD = .76$), 3 ($M = 1.56$, $SD = .79$), and 4 ($M = 1.49$, $SD = .74$). Although a main effect of employment situation had a

Table 2. ANOVA and *t* Tests of Differences in Mean Psychological Impact.

Variables and Statistical Tests	Mean Psychological Impact—Emotional Well-Being (*SD*)	Mean Psychological Impact—Sense of Security (*SD*)	*N*
Cybercrime type			
Hacking	1.27 (.58)	1.80 (.94)	502
Financial	1.50 (.72)	1.71 (.82)	1,482
Person-centered	1.62 (.85)	1.42 (.71)	431
ANOVA *F*	36.72**[a]	33.00**[a]	
Acquainted offender			
No	1.43 (.75)	1.51 (.73)	168
Yes	1.75 (.89)	1.37 (.69)	263
t test	−3.96**[b]	1.95[b]	
Contact with offender			
Daily	1.77 (.97)	1.46 (.83)	78
≥once per month	1.86 (.85)	1.40 (.64)	85
<once per month	1.79 (1.01)	1.33 (.63)	48
Never	1.48 (.67)	1.21 (.57)	52
ANOVA *F*	2.08	1.65[a]	
Loss			
No	1.42 (.72)	1.66 (.87)	1,097
Yes, compensated	1.39 (.69)	1.77 (.85)	281
Yes, not compensated	1.56 (.74)	1.68 (.80)	945
ANOVA *F*	11.15**[a]	1.65[a]	
Active contribution to crime			
No	1.38 (.73)	1.93 (.92)	135
Yes	1.51 (.81)	1.91 (.92)	211
t test	−1.59[b]	0.16	
Socioeconomic status			
Income level			
1st 20%	1.53 (.80)	1.66 (.82)	288
2nd 20%	1.50 (.76)	1.73 (.84)	309
3rd 20%	1.56 (.79)	1.72 (.86)	454
4th 20%	1.49 (.74)	1.69 (.87)	566
5th 20%	1.36 (.63)	1.67 (.81)	699
ANOVA *F*	3.98**[b]	0.22	
Employment situation			
Payed job/self-employed	1.43 (.70)	1.69 (.84)	1,366
Unemployed	1.54 (.82)	1.76 (.86)	239
Student	1.49 (.74)	1.57 (.80)	489
Pensioner	1.59 (.79)	1.84 (.86)	252
ANOVA *F*	2.83*[b]	4.25**	

Note. ANOVA = analysis of variance.
[a]Welch test. [b]Equal variances not assumed.
*$p < .05$. **$p < .01$.

p value of .04 and $F(3, 2296) = 2.83$, this was not considered significant. Namely, because a Levene's test showed a difference in variances, a significance level of $p < .01$ was chosen. For sense of security, there was no significant interaction effect between income level and employment situation either, $F(12, 2296) = 1.13$, $p = .33$. There was also no significant main effect of income level $F(4, 2296) = 0.22$, $p = .93$. However, there was a significant main effect of employment situation $F(3, 2296) = 4.25$, $p = < .01$. Post hoc tests showed that student victims experienced a lower impact on sense of security ($M = 1.57$, $SD = .80$) than victims with a payed job or who were self-employed ($M = 1.69$, $SD = .84$, $p = .04$), unemployed victims ($M = 1.76$, $SD = .86$, $p = .03$), or retired victims ($M = 1.84$, $SD = .86$, $p < .01$). Therefore, Hypothesis 6 was rejected. Notably, with respect to emotional well-being, the outcomes for income are the opposite of what was hypothesized: The impact of cybercrime victimization on emotional well-being seems higher for victims with a lower SES since the highest income group showed the lowest mean impact scores. Table 3 summarizes the findings for all hypotheses.

Discussion and Conclusion

Interpretation of Findings

The aim of our study was to examine the impact of cybercrime on its victims and to explain that impact. This study showed that different cybercrime types have various effects on victims. Furthermore, we discovered that, when studying the psychological impact of cybercrime victimization, we need to distinguish between impact on emotional well-being and impact on someone's belief in being secure in a digital environment: cybercrime-related sense of security. Other victimization studies also discerned multiple dimensions of psychological impact, such as emotional distress, strain, and life disruption (Golladay & Holtfreter, 2017), emotional effect versus emotional reaction (Shapland & Hall, 2007), and primary and secondary impacts of stress and anxiety (Kerr et al., 2013). The current study provides a new distinction, which seems particularly valuable in the cybercrime area. Future research should further elaborate this distinction.

The SAT proved suitable for developing expectations about the psychological impact of cybercrime victimization. However, the SAT was not particularly strong in predicting that impact. It failed in predicting the impact on sense of security, and it showed mixed results with respect to the emotional well-being of cybercrime victims. The SAT therefore seems less suitable to explain cybercrime-related sense of security. It can be argued that emotional well-being encompasses a more direct impact on the victim as described in the SAT, while sense of security concerns feelings of digital safety and specific situations in which cybercrime victimization could occur. The latter is expected to have been less relevant during the development of the SAT in the 1980s. Although in other traditional crime and cybercrime research, general factors such as sense of safety and fear of repeated victimization are also taken into account (Golladay & Holtfreter, 2017; Lamet & Wittebrood, 2009; Randa & Reyns, 2019; Winkel, 1998), the underlying explanatory factors might be different in a digital context. We will elaborate on this in more detail below.

The results of this study showed varying psychological victimization impact for three key cybercrime categories (Hypothesis 1). The impact scores on emotional well-being were highest for person-centered cybercrime, followed by financial cybercrime (money-centered) and hacking (device-centered). This aligns with expectations from the SAT, namely that human-induced crime, focused on the individual, results in more shattered assumptions (Janoff-Bulman, 1985). However, the impact scores on sense of security were lower for person-centered cybercrime than for financial cybercrime and hacking, contradicting the expectation from the SAT. This again shows that the SAT might be less applicable to cybercrime-related sense of security. An explanation is that this sense of security concerns trust in digital safety and potential future victimization situations rather than

Table 3. Results Summary.

Hypotheses	Emotional Well-Being	Cybercrime-Related Sense of Security
Hypothesis 1: The psychological impact of person-centered cybercrime is higher than the psychological impact of financial cybercrime or hacking	TRUE	FALSE (reversed)
Hypothesis 2: The psychological impact of cybercrime is higher if the offender was acquainted than if the offender was unacquainted	TRUE	FALSE
Hypothesis 3: The psychological impact of cybercrime is higher if the victim was in contact with the offender more intensively prior to the offense	FALSE	FALSE
Hypothesis 4: The psychological impact of cybercrime victims who experienced financial loss is lower when the loss was compensated	TRUE	FALSE
Hypothesis 5: The psychological impact of cybercrime is lower for victims who actively contributed to the crime than for victims who did not actively contribute to the crime	FALSE	FALSE
Hypothesis 6: The psychological impact of cybercrime is higher for victims with a higher SES than for victims with a lower SES	FALSE (reversed)	FALSE

Note. SES = socioeconomic status.

direct, focused harm by another person. Furthermore, hacking and financial cybercrime seem to contain more unique cybercrime elements such as the scale on which victims can be approached and the intangibility of the crime (Diamond & Bachmann, 2015; Kerr et al., 2013; Leukfeldt et al., 2018; Moitra, 2005). This might lead to the expectation and fear of repeat victimization and feelings of unsafety, resulting in a relatively higher impact on sense of security. In sum, the SAT seems less suitable to explain this second type of psychological impact.

The results showed higher impact scores on emotional well-being for victims for whom the offender was acquainted than for victims for whom the offender was not as was expected based on literature (Hypothesis 2). There were no differences considering sense of security. In contrast, the intensity of contact with an acquainted offender did not seem to be of influence (Hypothesis 3). Based on the SAT, assumptions were expected to be more shattered when someone close and trusted to the victim commits the offense. This was only confirmed with regard to emotional well-being and only for an offender being acquainted or not. In cybercrime, the offender is more likely to be unknown because of the possible remoteness and anonymity of the offense (Brands & Van Wilsem, 2019; Jansen et al., 2013). This potential anonymity does not seem to influence a victim's sense of security. Therefore, even though the offender is often unknown in cybercrimes, this does not entail that victims experience less impact by those crimes. This renders the view unsubstantiated that the aspects of anonymity and remoteness would result in lower impact of online crime than of face-to-face crime (Kerr et al., 2013).

The current study also suggests that financial loss and whether victims were compensated for it lead to differences in psychological victimization impact (Hypothesis 4). Victims who received loss compensation – albeit in full or partially experienced lower impact on emotional well-being than victims who did not receive loss compensation. This corresponds with the expectations from the SAT, about the reconfirmation of the world being meaningful, comprehensible, and just when loss compensation takes place (Janoff-Bulman, 1985). The results could also have to do with less occurring victim blaming and victims feeling acknowledged when loss is compensated (Pemberton, 2012; Van der Vijver, 1993). However, the impact on sense of security did not differ for victims who were and who were not compensated. Apparently, loss compensation predominantly impacts victims' emotional well-being. Future research should elaborate into the mentioned potential underlying mechanisms.

Active contribution to the crime did not seem to influence either emotional well-being or sense of security (Hypothesis 5). From the SAT and theories about locus of control, impact was expected to be lower when victims actively contributed to the crime (Ajzen, 2002; Janoff-Bulman, 1985). That is, actively contributing victims were expected to be able to explain the event and to prevent recurrence in the future. However, some authors stated the opposite because of shame and guilt as well as a lack of social support victims could experience because of actively contributing to the crime (Cross, 2015; Kerr et al., 2013; Leukfeldt et al., 2018). Opposite underlying mechanisms may therefore account for the absence of a significant result. Furthermore, possibly the strongest feelings of victims are that injustice was inflicted upon them or that they have fallen for the persuasion techniques of a scammer. This might not directly concern the idea that they themselves may have played a role in the execution of the crime. Active contribution is often mentioned in studies on cybercrime victimization impact and less often in traditional crime research. However, an active contribution might also occur in traditional crime, for instance, with victims letting doorstep scammers into their house. Active contribution is also hard to pinpoint since victims often play a role in the cause of the offense, while they have no desire for it to happen. Future research should give more attention to the potential role of an active contribution in the crime, while also taking factors such as feelings of guilt and shame into account.

The current study indicated a lower impact on emotional well-being for victims with a higher SES than for victims with a lower SES, contrary to the expectations (Hypothesis 6). This was only true for income; no significant effects were found for employment situation. Conversely, no significant effects of income were found on sense of security, while there was an effect of employment situation. Namely, student victims experienced less impact on sense of security than employed, unemployed, or retired victims did. From the SAT, victims with a higher SES were expected to experience more shattered assumptions from victimization because they were more likely to have led relatively unchallenged lives up to that point (Janoff-Bulman, 1985).

Our study indicates that a higher SES, in terms of income, prevents victims from experiencing a high impact of cybercrime victimization on emotional well-being. This is in line with studies stating that the impact of victimization is higher when SES is lower, for reasons such as access to resources (Agnew, 1985; Dinisman & Moroz, 2017). The result of students experiencing a lower impact on sense of security might still align with the SAT since it might be argued that younger people are more likely to have led relatively unchallenged lives up to that point. In future research, life experiences and personal factors should be included in addition to SES since the impact of a particular cybercrime can vary widely per victim (Holt & Bossler, 2008). Furthermore, people considering themselves more invulnerable beforehand might experience more victimization impact than people already considering themselves weak. The potential effects of such perceived vulnerability factors should also be explored.

Limitations and Future Research Directions

This study has several limitations. To begin with, the coping aspect of the SAT was not explicitly taken into account. For future research, it is recommended to do so. According to the theory, victims need to apply coping strategies after victimization to rebuild or come to terms with their shattered assumptions (Janoff-Bulman, 1985). Coping strategies can consist of redefining what happened, finding meaning in the event, engaging in specific actions to adjust to the new situation, and seeking social support. The capability to apply these coping mechanisms successfully differs for every victim, which relates to certain background factors and social circumstances. Demographic and socioeconomic factors might also be of importance. In this study, only employment situation and income were included, while it is also important to take factors such as gender, age, origin, marital status, household composition, and education level into account. More thorough analysis of coping strategies allows for shaping the supporting role of government agencies such as police and victim care (Jansen & Leukfeldt, 2018).

Future work should also consider longitudinal studying of victimization impact using different methods, instead of merely cross-sectional asking victims about their victimization experiences in the last twelve months. After all, the effects of crime consist of different stages with differing intensity (Frieze et al., 1987; Jansen & Leukfeldt, 2018; Shapland & Hall, 2007). One of the few longitudinal studies on this subject showed that victims experienced impact of online threat three months after the occurrence, while this had disappeared after nine months (Sipma & Van Leijsen, 2019). Some effects, such as PTSD, occur only long after the event (Dunn, 2007). Furthermore, although the use of victim surveys has many advantages, such as not being dependent on police data, it could be that victims do not remember occurrences correctly or do not position them in the right timeframe (Sipma & Van Leijsen, 2019). People also tend to lack in linking their feelings to experienced events (Dunn, 2007). In addition, some psychological effects, such as anger, are considered more accepted than others, such as sadness, which might influence reporting (Mawby & Walklate, 1994). For future research, observations or other real-time measurements of victimization impact on a longitudinal basis are advised. This would also allow for successfully measuring how multiple or repeated victimization is related to the impact of cybercrime, while those victims could not be included in the current study. Stronger statistical methods, such as multivariate regression and path analysis, are also recommended for future research.

The included cybercrime and impact types should also be reconsidered in future work. For instance, hacking was seen as a separate crime in this study but included under the other crimes if it was considered part of the MO of that crime. To explore the impact of hacking further in future research, the aspects of MO and motivation of the offender could be separated. This is also the case for sexually and nonsexually motivated person-centered cybercrime. The psychological impact of both types might differ, for instance, because of sexually explicit images potentially remaining online (Leukfeldt et al., 2018). Additionally, more research is needed to establish a comprehensive overview of the different types of impact cybercrime victims experience. This study focused on psychological and financial impacts. A connection between the two was discovered in the case of loss compensation. Financial impact should be studied more extensively in future studies, for instance, by including loss amounts and relating those to the financial position of victims. Physical, behavioral, and social impact should also be included to complete the picture.

In the current study, no comparison with the impact of traditional crime took place, while it is advisable to do so. This would put the impact of cybercrimes in perspective and could show if the type of crime, acquainted offender, loss compensation, income, and employment situation lead to similar differences in victimization impact of traditional crime. The importance of the other aspects, namely, the contact intensity with the offender as well as actively contributing to the crime, could also be explored for traditional crimes. The included aspects are not unique to cybercrimes, while it is not certain how they would play out in traditional crime. For instance, it could be that loss compensation is of relatively great importance for cybercrime victims because they feel recognized after possibly being blamed or not being taken seriously by their environment (Cross, 2015; Leukfeldt et al., 2018). Furthermore, it would be insightful to compare the psychological impact of cybercrimes to that of traditional crimes and to rank the severity of those crimes for victims. The differences between the impact on emotional well-being and on sense of security and how this relates to cybercrime and traditional crime should also be explored further because this study showed divergent results for both types of psychological impacts. To explain the results in more detail, the role of particular devices and to what extent victims are attached to them should also be taken into account, considering the connectedness of people and their devices according to the cyborg theory (Agustina, 2015; Van der Wagen & Pieters, 2018).

In future work, the applicability of the SAT on cybercrime victimization could be explored further. This study demonstrated that the SAT is suitable for developing expectations about the psychological impact of cybercrime and thus might help to understand the impact of cybercrime, even though the SAT more often than not predicted victimization impact right. Further research on other data sets of cybercrime victims should derive new expectations about different forms of victimization impact and discover underlying mechanisms. For instance, from the SAT, repeat victimization is also expected to result in higher psychological impact, which could not be tested in the current study. Furthermore, it would make sense to test the applicability of the SAT as a whole instead of as an underlying explanation. Thus, studying the shattering of assumptions resulting from cybercrime victimization, instead of merely the effects this shattering, might have on psychological impact.

In sum, the current study was of an exploratory nature and limited, partly because it made use of existing data. Notwithstanding the limitations, differences in psychological victimization impact according to different cybercrimes and crime characteristics were laid bare. Future research can build onto those findings by focusing specifically on this topic and collecting data tailored to this topic. This could lead to the production of more reliable results and to the uncovering of underlying mechanisms. Besides, to the best of our knowledge, the current study applied the SAT on cybercrime victimization for the first time. At a minimum, this study showed that the SAT could not be discredited altogether to explain the victimization impact of cybercrime. Conversely, application of the SAT resulted in a first step toward a more theory-based understanding of the psychological impact for cybercrime victims. Yet, the fact that no more than three of six hypotheses were confirmed regarding emotional well-being and none regarding sense of security shows that additional research is needed to better understand the power of the SAT in explaining the victimization impact of cybercrime, especially when it comes to cybercrime-related sense of security. The position of some authors on the inability to apply traditional theories to cybercrime because of its unique characteristics that would challenge existing theoretical and victimological frameworks in the cybercrime field (Hay & Ray, 2019; Van der Wagen & Pieters, 2018) could be further explored for this specific type of psychological impact.

Policy Recommendations

The results of this study provide insights that can help improve social and judicial responses to victims by government agencies such as police and victim care. Specifically, recognition of victims and their situation can be substantiated only if those agencies understand victims' situations (Kunst & Koster, 2017). Insights from this study into the victimization impact of different cybercrime types can help set priorities and treat victims appropriately. For instance, person-centered cybercrime could be prioritized more when it comes to the emotional support of victims. Furthermore, hacking and financial cybercrime could be prioritized more when it comes to ensuring perceptions about safe digital circumstances for victims and helping them to prevent future victimization. Specific crimes that resulted in the highest victimization impact could also be prioritized, see Table 2. Additionally, this study shows the importance of loss compensation. For violent crime, funding can be offered by the Dutch government when victims experience severe physical or psychological impact (Kunst et al., 2017). Something similar could be established for cybercrime victims to temper the severity of the impact on emotional well-being they experience.

Data Availability

The records of the data set "Digital Safety & Criminality 2018" from Statistics Netherlands are available at https://www.cbs.nl/nl-nl/onze-diensten/maatwerk-en-microdata/microdata-zelf-onderzoek-doen/microdatabes tanden/dvc-2018-digitale-veiligheid-criminaliteit-2018. The data are available for use under specific conditions. Information or purchase requests can be sent to microdata@cbs.nl.

Software Information

SPSS Version 25.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Note

1. In the future, cybercriminals might have more opportunities than today to also harm their victims physically, for instance, by attacking human implants (Gasson & Koops, 2013).

References

Agnew, R. S. (1985). Neutralizing the impact of crime. *Criminal Justice and Behavior*, *12*(2), 221–239.

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

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.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683.

Averdijk, M. D. E. (2010). *Individuals' victimization patterns over time*. VU.

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.

Berg, M., & Johansson, T. (2016). Trust and safety in the segregated city: Contextualizing the relationship between institutional trust, crime-related insecurity and generalized trust. *Scandinavian Political Studies*, *39*(4), 458–481.

Brands, J., & Van Wilsem, J. (2019). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*, *1*, 1–22.

Briggs, S. R., & Cheek, J. M. (1986). The role of factor analysis in the development and evaluation of personality scales. *Journal of Personality*, *54*(1), 106–148.

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. (2009). *A better deal for fraud victims: Research into victims' needs and experiences*. National Fraud Authority.

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.

Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, *12*(1), 101–114.

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.

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

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.

Dignan, J. (2005). *Understanding victims and restorative justice*. Open University Press.

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

Domenie, M. M. L., Leukfeldt, E. R., Van Wilsem, J. A., Jansen, J., & Stol, W. (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 on e-fraud, hacking and other common crimes]. Boom Lemma Uitgevers.

Dunn, P. (2007). Matching service delivery to need. In S. Walklate (Ed.), *Handbook of victims and victimology* (pp. 255–281). William Publishing.

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.

Furnell, S. (2001). Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare*, *1*(2), 35–44.

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

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.

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

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.

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.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40.

Huys, H. W. J. M. (2012). Criminaliteit en slachtofferschap [Criminality and victimization]. In M. M. Van Rosmalen, S. N. Kalidien, & N. E. De Heer-de Lange (Eds.), *Criminaliteit en rechtshandhaving 2011: Ontwikkelingen en samenhangen* (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. (1985). The aftermath of victimization: Rebuilding shattered assumptions. In C. R. Figley (Ed.), *Trauma and its wake* (pp. 15–35). Brunner/Mazel.

Janoff-Bulman, R. (1999). Rebuilding shattered assumptions after traumatic life events. In C. R. Snyder (Ed.), *Coping: The psychology of what works* (pp. 305–323). Oxford University Press.

Janoff-Bulman, R., & Frieze, I. H. (1983). A theoretical perspective for understanding reactions to victimization. *Journal of Social Issues*, *39*(2), 1–17.

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* (pp. 31–46). Boom Lemma Uitgevers.

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.

Kunst, M. J. J., Koster, N. N., & Van Heugten, J. (2017). Performance evaluations and victim satisfaction with state compensation for violent crime: A prospective study. *Journal of Interpersonal Violence*, *32*(19), 3027–3044.

Kunst, M. J. J., Rutten, S., & Knijf, E. (2013). Satisfaction with the initial police response and development of posttraumatic stress disorder symptoms in victims of domestic burglary. *Journal of Traumatic Stress*, *26*(1), 111–118.

Lamet, W., & Wittebrood, K. (2009). *Nooit meer dezelfde: Gevolgen van misdrijven voor slachtoffers* [Never being the same again: Effects of crimes on 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* [Victims of online crime: A study on the needs, consequences and responsibilities following the victimization of cybercrime and digitized crime]. WODC.

Li, Y., Yazdanmehr, A., Wang, J., & Rao, H. R. (2019). Responding to identity theft: A victimization perspective. *Decision Support Systems*, *121*, 13–24.

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.

Mawby, R. I., & Walklate, S. (1994). *Critical victimology: International perspectives*. Sage.

Moitra, S. D. (2005). Developing policies for cybercrime. *European Journal of Crime Criminal Law and Criminal Justice*, *13*(3), 435–464.

Montoya, L., Junger, M., & Hartel, P. (2013, August 12–14). *How "digital" is traditional crime?* [Conference session]. *2013 European Intelligence and Security Informatics Conference*, IEEE, Uppsala, Sweden (pp. 31–37).

Pemberton, A. (2012). De emotionele hond en zijn rationele staart in recent onderzoek naar slachtoffers van een misdrijf [The emotional dog and its rational tail in recent research into crime victims]. *Tijdschrift Voor Herstelrecht*, *11*(4), 17–27.

Randa, R., & Reyns, B. W. (2019). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the national crime victimization survey. *Deviant Behavior*, *41*, 1290–1304.

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.

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

Shapland, J., & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology*, *14*(2), 175–217.

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

Statistics Netherlands. (2019). *Digitale veiligheid & criminaliteit 2018* [Digital safety & crime 2018]. https://www.cbs.nl/nl-nl/publicatie/2019/29/digitale-veiligheid-criminaliteit-2018

Statistics Netherlands. (2020). *Veiligheidsmonitor 2019* [Safety monitor 2019]. https://www.cbs.nl/nl-nl/publicatie/2020/10/veiligheidsmonitor-2019

Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2007). *Using multivariate statistics*. Pearson.

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

Van der Vijver, C. D. (1993). *De burger en de zin van strafrecht* [The citizen and the purpose 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.

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. (2015). Mass-marketing fraud: A growing concern. *IEEE Security & Privacy*, *13*(4), 84–87.

Winkel, F. W. (1998). Fear of crime and criminal victimization: Testing a theory of psychological incapacitation of the 'stressor' based on downward comparison processes. *British Journal of Criminology*, *38*(3), 473–484.

Author Biographies

Jildau Borwell, MSc, is a PhD candidate at the Cyber Science Center, a collaboration between NHL Stenden University of Applied Sciences, the Dutch Police Academy and the Open University of the Netherlands. Her research subject is the impact of cybercrime on victims compared to traditional crime and its consequences for the role of the police. She also works as a senior cybercrime analyst at the cybercrime team of the Northern Netherlands police unit.

Jurjen Jansen, PhD, is a senior researcher at the Cybersafety Research Group of NHL Stenden University of Applied Sciences. In 2018, he obtained his PhD in behavioural information security from the Open University of the Netherlands. His research interests include human aspects of information security, cybercrime, victimization, human-computer interaction and behaviour change.

Wouter Stol, Prof., Dr., received his doctorate on 'Police action and information technology' at the Vrije Universiteit of Amsterdam in 1996. He is currently professor of Cybersafety at NHL University of Applied Sciences and the Dutch Police Academy and professor of Police Studies at the Open University of the Netherlands. Main themes in his work include police practice and information use, cybercrime, perpetratorship and victimisation of cybercrime, and measures against cybercrime (especially criminal law).