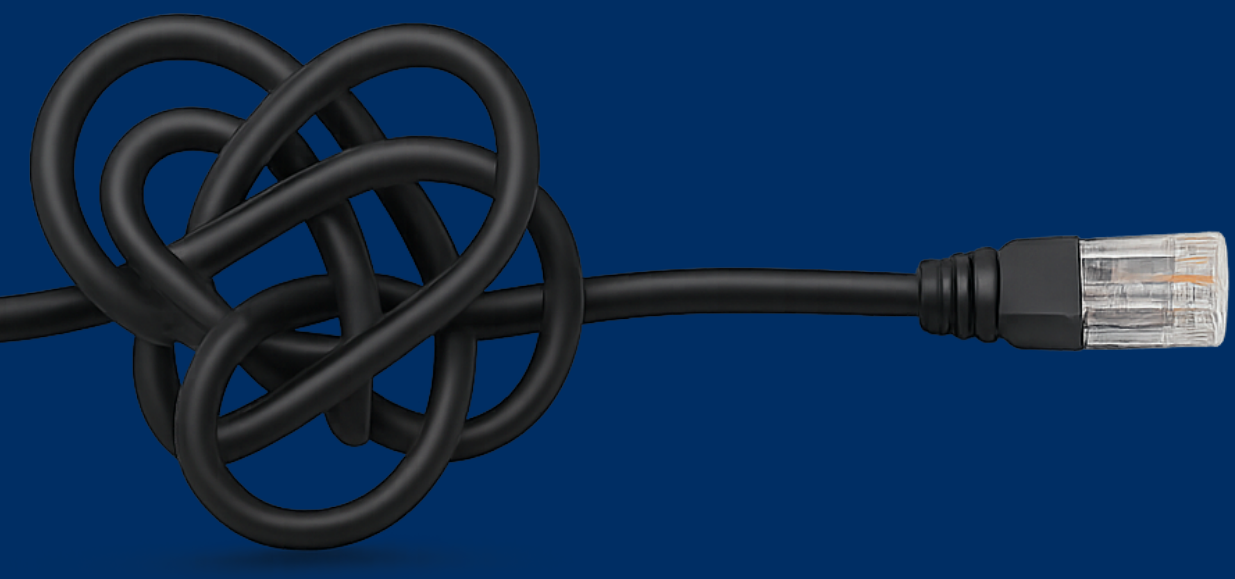
Unravelling the impact of cybercrime: Understanding victim experiences and implications for police practice

UNRAVELLING THE IMPACT OF CYBERCRIME

UNDERSTANDING VICTIM EXPERIENCES AND IMPLICATIONS FOR POLICE PRACTICE



JILDAU BORWELL

Unravelling the impact of cybercrime

Understanding victim experiences and implications for police practice

Jildau Borwell

Layout Renate Siebes | Proefschrift.nu
Printed by Proefschriftmaken | www.proefschriftmaken.nl
ISBN 978-94-6510-792-9

Unravelling the impact of cybercrime

Understanding victim experiences and
implications for police practice

PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Open Universiteit
op gezag van de rector magnificus
prof. dr. Th.J. Bastiaens
ten overstaan van een door het
College voor promoties ingestelde commissie
in het openbaar te verdedigen

op vrijdag 17 oktober 2025 te Heerlen
om 13.30 uur precies
door

Jildau Borwell
geboren op 16 september 1988 te Leeuwarden

Promotor:
Prof. dr. W.Ph. Stol, Open Universiteit

Copromotor:
Dr. J. Jansen, NHL Stenden Hogeschool; Politieacademie

Leden beoordelingscommissie:
Prof. dr. E. Giebels, Universiteit Twente
Prof. dr. S. de Kimpe, Vrije Universiteit Brussel
Prof. dr. mr. M.J.J. Kunst, Universiteit Leiden
Prof. dr. J.H.L.J. Janssen, Open Universiteit
Dr. ir. V. Niculescu-Dincă, Universiteit Leiden
Dr. R. Spithoven, Saxion Hogeschool

Contents

CHAPTER 1 – Toward an understanding of cybercrime victims' experiences **11**

1.1. Background and scope 12
1.1.1. Digitization and crime 13
1.1.2. Attention for victims 15
1.1.3. Impact and needs of cybercrime victims 16
1.1.4. The role of the police 18
1.2. Objectives and research questions 20
1.3. Overall contribution 22
1.3.1. Scientific contribution 22
1.3.2. Practical contribution 23
1.4. Outline of the dissertation 24
1.4.1. Guide to the reader 24
1.4.2. Chapter 2. Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions 24
1.4.3. Chapter 3. The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory 24
1.4.4. Chapter 4. The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors 25
1.4.5. Chapter 5. Exploring the impact of cybercrime and traditional crime victimization: Impact comparisons and explanatory factors 25

1.4.6. Chapter 6. The needs and experiences of cybercrime and traditional crime victims compared and explained: Implications for the role of the police 26
1.4.7. Intermezzo. Reporting cybercrime online versus in-person: A comparison of victim experiences 26
1.4.8. Chapter 7. Conclusion and discussion 26

CHAPTER 2 – Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions 29
2.1. Introduction 30
2.2. The relevance of comparing the impact of cybercrime and traditional crime 32
2.3. Methods 35
2.4. Studies comparing the victimization impact of cybercrime and traditional crime 36
2.5. Studies considering cybercrime from a victim perspective 38
2.6. Shortcoming in current literature on the impact of crime 39
2.7. Future research directions 41
2.7.1. Distinguishing between cybercrime and traditional crime 42
2.7.2. Classifying cybercrime and traditional crime 43
2.7.3. Measuring the victimization impact of cybercrime and traditional crime 44
2.8. Concluding remarks 47

CHAPTER 3 – The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory 49
3.1. Introduction 50
3.2. Literature review and expectations from the SAT 52
3.2.1. Victimization impact of cybercrime 52
3.2.2. Categorizing cybercrime and victimization impact 53
3.2.3. Theoretical explanations for cybercrime victimization impact 55
3.2.4. The SAT applied to cybercrime victimization impact 55
3.3. Materials and methods 59
3.3.1. Distributions and divisions 59
3.3.2. Operationalization 60
3.4. Results 64
3.5. Discussion and conclusion 69

3.5.1. Interpretation of findings 69
3.5.2. Limitations and future research directions 72
3.5.3. Policy recommendations 75

CHAPTER 4 – The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors **77**
4.1. Introduction 78
4.2. The democratization of victimization, coping, and personal factors 80
4.3. Cyborg theory and circumstantial factors 82
4.4. Current study 84
4.5. Materials and methods 84
4.5.1. Dataset and selection of respondents 84
4.5.2. Operationalization 85
4.5.3. Statistical tests 87
4.6. Results 88
4.7. Conclusion and discussion 93
4.7.1. Personal factors 93
4.7.2. Circumstantial factors 94
4.7.3. Theoretical reflection 95
4.7.4. Limitations and future research 95
4.7.5. Practical implications 96
4.7.6. Closing remarks 97

CHAPTER 5 – Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors **99**
5.1. Introduction 100
5.1.1. Background 100
5.1.2. Categories of victim impact 102
5.1.3. Determinants of victim impact 102
5.2. Crime types 102
5.2.1. Crime characteristics 104
5.2.2. Social factors 105
5.2.3. Personal factors 105
5.2.4. Demographics 106
5.3. Materials and methods 106
5.3.1. Ethical considerations 106
5.3.2. Victim selection 107

5.3.3. Data collection 107
5.3.4. Response 108
5.3.5. Operationalization 108
5.3.6. Descriptives 111
5.3.7. Analyses 111
5.4. Results 115
5.4.1. Impact comparisons of crime pairs 115
5.4.2. Explanatory factors for victim impact 117
5.5. Conclusion and discussion 123
5.5.1. Reflection and implications of the findings 123
5.5.2. Study limitations 125
5.5.3. Recommendations for future research 125
5.5.4. Closing statements 126

CHAPTER 6 – Doing justice to the needs of cybercrime victims: Reflections on the role of the police 129
6.1. Introduction 130
6.2. Victim needs 131
6.3. Reporting experiences 132
6.4. Methods 132
6.4.1. Survey, invitation letter and victim selection 133
6.4.2. Data collection 133
6.4.3. Response 134
6.4.4. Operationalizations 134
6.4.5. Analyses 135
6.5. Results 136
6.5.1. Needs of victims 136
6.5.2. Explanations for victim needs in property crime (burglary, scams) 139
6.5.3. Explanations for victim needs in person-centered crime (threat and violation of physical integrity) 142
6.5.4. Victims' reporting experiences 147
6.6. Conclusion and discussion 150
6.6.1. Needs 150
6.6.2. Reporting experiences 152
6.6.3. The role of the police 153
6.6.4. Limitations and future research 155

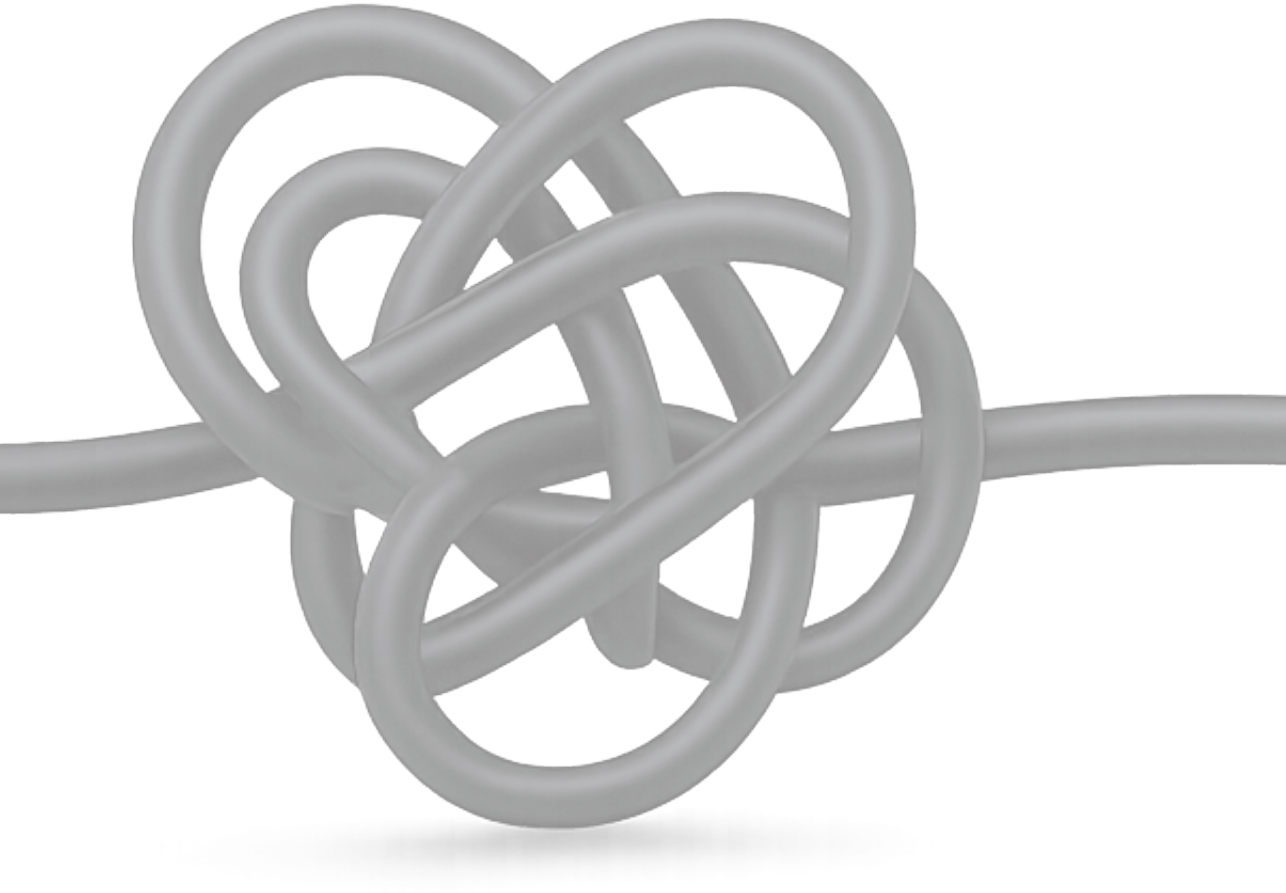
INTERMEZZO – Reporting cybercrime online versus in-person: A comparison of victim experiences **159**
I.1. Background 160
I.2. Methods 160
I.3. Results 160
I.4. Conclusion 162

CHAPTER 7 – General conclusion and discussion: The impact and needs of cybercrime victims and the implications for police practice **165**
7.1. Introduction 166
7.2. Victim impact of cybercrime and comparison to traditional crime 167
7.2.1. Explaining the victim impact of cybercrime 167
7.2.2. Comparing the impact of cybercrime and traditional crime 168
7.3. Implications for the role of the police 169
7.3.1. Needs and reporting experiences 169
7.3.2. Implications for the role of the police 171
7.4. Theoretical considerations and contributions 172
7.5. Recommendations for police and victim policies 176
7.6. Limitations and future research directions 180
7.7. What lies ahead in cybercrime and its impact on victims 183

REFERENCES **187**

APPENDICES **209**
Appendix 1. Variations in impact by cybercrime type – Chapter 4 210
Appendix 2. Survey design and data collection – Chapters 5 and 6 212
Appendix 3. Victim survey – Chapters 5 and 6 227
Appendix 4. Victim impact interactions – Chapter 5 265

SAMENVATTING (SUMMARY IN DUTCH) **273**
SUMMARY **283**
DANKWOORD (ACKNOWLEDGMENTS IN DUTCH) **291**
CURRICULUM VITAE **295**



Chapter 1

Toward an understanding of cybercrime victims' experiences

1.1. Background and scope

> "*I experienced insomnia and it haunted my mind all day. At first, you feel ashamed of your stupidity. It also took a few days before I could talk to others about it. But even now, there are very few people around me who know about it.*"[1]
>
> - Male bank helpdesk fraud victim, aged approximately[2] 67; 6-9 months post-incident.

> "*The threshold was very high to step into the police station, afraid of being judged, but I was received so incredibly well […], which made me leave much more confident.*"
>
> - Male image-based sexual abuse victim; aged approximately 70; up to 3 months post-incident.

These impact testimonies, drawn from the victim surveys conducted for this dissertation, illustrate the diverse and profound effects that cybercrime victims may endure, as well as the crucial role the police can play in the recovery process. They also underscore the damage to cybercrime victims' self-image and their reluctance to seek support. This dissertation shows that cybercrime victims experience severe effects, emphasizing the need for compassionate and effective support systems tailored to their needs. As a central point of contact and a primary stakeholder in the realm of cybercrime, the police play an important role in guiding victims toward recovery. This dissertation aims to shed light on the impact of cybercrime on victims and to explore its implications for the role of the police. It addresses a significant gap in the current literature, as research thus far has lacked a comprehensive view of the wide impact range experienced by victims across various cybercrimes, as well as a comparative approach by examining cybercrime alongside traditional crime (Button et al., 2021; Faubert et al., 2021; Leukfeldt et al., 2020; Riek, 2017; Sipma & Van Leijsen, 2019).

This chapter begins by providing an overview of the dissertation's background and scope, focusing on the relationship between digitization and crime, the attention for crime victims in academia and practice, the impact and needs of cybercrime victims, and the role of the police. Following this, the objectives and research questions of the dissertation are presented. The chapter then discusses the overall contributions of the dissertation, both scientific and practical. Finally, an outline of the dissertation

[1] Quotes have been translated from Dutch and retained as closely as possible to the original wording.
[2] Age estimated based on the respondent's year of birth.

is provided, including a guide for readers on how to navigate the dissertation and a brief outline of the chapters with the separate studies.

1.1.1. Digitization and crime

Computers and the internet have brought numerous advantages, such as easier personal communication and the ability to work more efficiently and from any location (Holt & Bossler, 2014; Wall, 2005). These developments have enhanced personal and professional lives. However, they have also introduced new opportunities for criminal activity. The concept of computer crime emerged in the 1960s, with initial instances of manipulation and sabotage by financially motivated offenders (Riek, 2017). At that time, limited connectivity and the specialized skills required to operate computers reduced the likelihood that offenses would be committed. The introduction of personal computers in households during the 1980s and their subsequent networking capabilities through the introduction of the internet in the 1990s paved the way for new cybercrime forms. In the Netherlands, hacking began to surface in the 1970s and 1980s, as noted by Stol and Strikwerda (2019). This marked the start of a new criminal landscape involving digital systems. A notable event occurred in 1992 with the arrests of two Dutch hackers, Harry W. (alias Wave) and Rob N. (alias Fidelio), which predated the enactment of the first Computer Crime Act (Wet Computercriminaliteit) in 1993. Over the following decades, computers have become integral to daily life. By 2024, 96% of the Dutch population aged 12 and older used the internet daily (Arends et al., 2025). As people have become increasingly dependent on the internet, they also find themselves inescapably confronted with its risks (Kerr et al., 2013).

In the early years of the internet, it operated under a self-regulatory approach, with proponents arguing against interference (Moitra, 2005). Barlow's (1996) influential manifesto "A declaration of the independence of cyberspace," advocated for 'cyberspace' to remain free from governmental control. The declaration begins with the statement "*Governments of the Industrial World […] I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*" (Barlow, 2019). It envisioned a humane and fair digital world, concluding with the assertion "*We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.*" This declaration has proven to be overly optimistic. Increasing rates of cybercrime victimization have underscored that relying solely on self-regulation of the internet is inadequate to ensure online

safety (Nieuwenhuizen & Van Huijstee, 2022). While self-regulation and social control do occur online (Berenblum et al., 2019; Stol & Strikwerda, 2019), they are not sufficient on their own to address cybercrime effectively. Consequently, there is now consensus that governments and law enforcement agencies have a crucial role to play in combatting cybercrime.

In the 21st century, cybercrime has surged due to several factors: the expanding potential of computer networks, increased internet usage, availability of personal information, legal ambiguities, the ability to target geographically dispersed victims, and the anonymity provided by online environments (Diamond & Bachmann, 2015; Reep-Van den Bergh & Junger, 2018; Riek, 2017). The development of online payment methods further fueled organized cybercrime, which escalated with the availability of cybercrime tools in underground markets (Leukfeldt, 2016; Riek, 2017). As a result, the digitization of society has transformed criminal methods significantly (Reep-Van den Bergh & Junger, 2018). Cybercrime has now become a substantial component of overall crime rates, while traditional crime has declined across North and West Europe as well as in Anglo-Saxon countries (Akkermans et al., 2024; Landman, 2023; Leukfeldt & Van 't Hoff-de Goede, 2023; Montoya et al., 2013; Reep-Van den Bergh & Junger, 2018). In the Netherlands, the cybercrime victimization rate in 2023 was approximately 16 percent compared to 20 percent for traditional crime, reflecting the pervasive impact of cybercrime in digitized societies (Akkermans et al., 2024). Since 2005, traditional crime victimization has dropped by 53 percent (Akkermans et al., 2024), indicating a significant shift in the crime landscape over an extended period.

Some authors, notably Grabosky (2001), have argued that cybercrime is merely 'old wine in new bottles;' suggesting that while the medium is new, the fundamental nature of cybercrime is essentially the same as traditional crime. They contend core criminal methods, such as fraud, have not significantly evolved; rather, these methods are simply applied in a digital context. From this perspective, the impact on victims might be expected to follow similar patterns to the impact of traditional crimes. For instance, whether fraud is executed through a digital platform or a physical interaction, the fundamental mechanisms of deceit and exploitation remain unchanged. Accordingly, Correia (2019) posits that victims' reactions to cybercrime are likely to be similar to their reactions to traditional crime. This perspective is debatable. Cybercrime exhibits unique characteristics that distinguish it from traditional crime and can lead to distinct victim responses. Factors such as the complexity of the technology involved, the anonymity of offenders, the intangibility and remote nature of the crime, and the potential permanence of cybercrimes (e.g., online images or personal

information that remain accessible) could contribute to different victim experiences and reactions (Agustina, 2015; Diamond & Bachmann, 2015; Hay & Ray, 2019; Kerr et al., 2013; Landman, 2023; Leukfeldt et al., 2018; Leukfeldt & Van 't Hoff-de Goede, 2023; Van der Wagen & Pieters, 2018). The unique characteristics translate into differences in a victimological sense (Moitra, 2005). The key question is whether these differences create unique impacts and needs for victims, thus requiring specific attention and tailored approaches to effectively address their experiences.

In this dissertation, cybercrime is defined as criminal activity in which information and communication technology (ICT) plays a crucial role in the execution of the offense (Domenie et al., 2013). There is no consensus on the precise definition or scope of cybercrime (Holt & Bossler, 2014; Leukfeldt & Van 't Hoff-de Goede, 2023; Riek & Böhme, 2018). Within the criminal justice system, cybercrime is typically categorized into two types: cybercrime in the narrow sense, also known as cyber-dependent crime, and cybercrime in the broad sense, also known as cyber-enabled crime. Cyber-dependent crime involves ICT as both the target and the means, consisting of offenses that are uniquely enabled by the digital realm and cannot occur outside of it (Domenie et al., 2013; Leukfeldt & Van 't Hoff-de Goede, 2023; Smit et al., 2018). On the other hand, cyber-enabled crime employs ICT as a means to facilitate already existing criminal activities. For the purpose of this dissertation, 'cybercrime' includes both types, sometimes also referred to as 'online crime', 'computer crime' or 'internet crime' (Henson et al., 2016). In this dissertation, traditional crime refers to criminal activities in which ICT does not play a crucial role in the execution of the offense. It should be noted that, in practice, the boundaries between cybercrime and traditional crime are often blurred. Many offenses involve both digital and physical elements, referred to as hybrid forms of crime (Leukfeldt et al., 2018; Montoya et al., 2013). For example, a case of stalking might involve both online harassment and in-person confrontation. In this dissertation, however, a clear operational distinction is applied by assessing whether ICT plays a crucial role in the execution of the offense.

1.1.2. Attention for victims

The attention for crime victims has steadily increased since the 1970s (Dunn, 2007; Shapland & Hall, 2007). In the Netherlands, the police have since enhanced victim services and support, particularly following the adoption of European Union's 2012 Victims' Rights Directive, which establishes the minimum standards on the rights, support, and protection of victims of crime (Van Bourgondien, 2017). These efforts aim to strengthen victims' positions by providing recognition, information, protec-

tion, and restoration. However, existing victim care frameworks are primarily based on traditional crime, while the landscape has changed with the rise in cybercrime rates (Notté et al., 2021). For example, current victim policies place considerable emphasis on participation in the judicial process. Yet, many cybercrime victims do not reach this stage due to the police's challenges in detecting cybercrime offenders (Ruiter et al., 2023). Moreover, considering the unique characteristics of cybercrime, cybercrime victims' experiences may differ significantly from those of traditional crime victims. Therefore, despite recent efforts to enhance victim support, there remains a notable gap in understanding the specific impact and needs of cybercrime victims. To effectively support these victims, it is essential to understand their experiences, which are not yet sufficiently understood (Button et al., 2021b; Notté et al., 2021).

In this dissertation, a victim is defined as "the person who has suffered financial damage or other harm as a direct result of a criminal offense" (Article 51a of the Dutch Code of Criminal Procedure). The focus is on direct victimization of individuals aged 18 and older, excluding companies, secondary victims (those indirectly affected by the crime) and tertiary victims (societal-level impact) (Aiken et al., 2015; Dinisman & Moroz, 2017; Vanderstraeten et al., 2012).

1.1.3. Impact and needs of cybercrime victims

Victim impact refers to the intensity and severity of the effects of crime as perceived by the victim (Dignan, 2005; Groenhuijsen, 1996). This experience is inherently subjective and thus the impact can vary widely among victims of the same crime type. For example, a person facing financial difficulties who loses a substantial amount of money may experience significant distress, whereas another individual in different circumstances might not perceive the impact as severely (Dignan, 2005; Jansen & Leukfeldt, 2018; Leukfeldt et al., 2018).

Previous research on victim impact (e.g., Dinisman & Moroz, 2017; Golladay & Holtfreter, 2017; Jansen & Leukfeldt, 2018; Lamet & Wittebrood, 2009; Leukfeldt et al., 2018; Shapland & Hall, 2007) suggests four main impact categories: psychological/emotional, financial/material, physical, and social/behavioral. The studies in this dissertation build upon this preliminary classification and also propose new categorizations based on factor analyses and a review of literature beyond crime victimization (see Chapter 3, 4 and 5). Furthermore, this dissertation explores explanatory factors for the impact experienced by victims. Previous research suggests that crime impact is influenced by crime characteristics, personal factors, and social factors (Aiken et al., 2015; Button et al., 2014; Cross et al., 2016a; Dinisman & Moroz,

2017; Golladay & Holtfreter, 2017; Jansen & Leukfeldt, 2018; Lamet & Wittebrood, 2009; Leukfeldt et al., 2018; Shapland & Hall, 2007). These factors are integrated into this dissertation to gain deeper insight into victim impact for cybercrime and traditional crime victims.

While it is widely acknowledged that crime can result in severe and long-lasting consequences for its victims, including impaired well-being, illness, and PTSD (Dinisman & Moroz, 2017; Janssen et al., 2021; Lamet & Wittebrood, 2009; Van de Ven, 2022), the specific effects of cybercrime have remained underexplored. Cybercrimes, particularly those with financial implications, are often perceived as having low impact due to the potential for financial compensation (Cross et al., 2016a; Graves et al., 2019; Jansen & Leukfeldt, 2018). However, this viewpoint overlooks the significant social, psychological, and sometimes physical effects that often can persist beyond financial losses (Button et al., 2021b; De Kimpe et al., 2020; Dunn, 2007; Henson et al., 2016; Leukfeldt & Van 't Hoff-de Goede, 2023; Riek & Böhme, 2018). The intangible nature of cybercrime may contribute to the underestimation of victim impact, as it lacks a direct physical component, leading some to believe that there is no 'real' harm involved (Palassis et al., 2021; Popham, 2021). Nevertheless, cybercrime victims often seem to experience profound effects, including financial losses alongside emotional distress, social disapproval, and even conditions such as PTSD or suicidal ideation (Leukfeldt et al., 2018; Palassis et al., 2021; Popham, 2021). The lack of recognition from law enforcement agencies and social environments, possibly due to the unfamiliarity with these crime types, can exacerbate these emotional consequences. This underscores the need for more targeted research into the impact and needs of cybercrime victims (Faubert et al., 2021; Leukfeldt et al., 2018).

Victim needs, while distinct from victim impact, are closely tied to the consequences of an experienced crime (Leukfeldt et al., 2020; Ten Boom et al., 2008). These needs typically encompass emotional, practical, financial, and informational aspects, although they can vary significantly depending on the type and severity of the crime, as well as individual characteristics, resources, and cultural factors (Dinisman & Moroz, 2017; Leukfeldt et al., 2018; Ten Boom et al., 2008). Cybercrime victims seem to experience needs in all of these categories, but empirical evidence on the subject is limited (Cross et al., 2016b; Leukfeldt et al., 2020). In this dissertation, victim needs are defined as those that arise after and because of the crime, which must be addressed to facilitate recovery and reduce the impact of victimization (Dinisman & Moroz, 2017). When these needs are not met, the negative emotional effects of victimization can intensify (Notté et al., 2021). The police often serve as an initial

point of contact for addressing victim needs, as victims may turn to them to report the crime and seek support, or at least see them as one of the parties that is going to help them (Leukfeldt et al., 2020). Victim support and broader victim-related policies within police forces are important as part of the police's commitment to addressing victim needs and to define their role in supporting cybercrime victims. However, current policies are primarily designed for traditional crime, with insufficient consideration of the specific experiences and needs of cybercrime victims. This underscores a significant area for further research (Leukfeldt et al., 2020; Notté et al., 2021).

1.1.4. The role of the police

Cybercrime presents unique challenges for police organizations, as it is not merely 'old wine in new bottles' but a fundamentally different realm that complicates traditional law enforcement approaches (Landman, 2023). While Stol and colleagues (1999) and Wall (2005) already recognized the internet as both a conduit for criminal activity and a potential opportunity for law enforcement efforts, the Dutch police continue to struggle with defining their role online (Landman, 2023). Although this is a contemporary challenge, it should be noted that the police have faced difficulties in addressing cybercrime since the early internet's days in the mid-1990s, largely due to a persistent lack of knowledge and resources (Domenie et al., 2009). The internet's relatively short existence of about 30 years (Nieuwenhuizen & Van Huijstee, 2022) partly explains why law enforcement agencies face difficulties adapting to this environment, where traditional, physical policing models do not easily apply. Cybercrime's distinct characteristics—such as anonymity, the irrelevance of national borders, and regulations that are influenced by sometimes powerful international (tech) entities—complicate the efforts of law enforcement agencies to keep pace with cybercrime (Bijleveld et al., 2021; Faubert et al., 2021). However, as criminal activities increasingly move online, it is crucial for law enforcement agencies to clearly define their role, maintain public trust, and adapt to rapid changes in the digital landscape to remain effective and legitimate (Bijleveld et al., 2021; Faubert et al., 2021; Van der Plas et al., 2022).

The difficulties police face in addressing cybercrime can significantly impact victims, since it can lead to inadequate handling of cases, support, and may lead to secondary victimization (Jansen & Leukfeldt, 2018; Notté et al., 2021). Cybercrime victims often feel that their emotional and practical needs are unmet (Button et al., 2020; Jansen & Leukfeldt, 2018; Leukfeldt et al., 2020; Notté et al., 2021). This can undermine trust in the legitimacy of law enforcement agencies (Nieuwenhuizen

& Van Huijstee, 2022). There are significant issues with the responsiveness of both police and other support organizations. Issues such as dismissive attitudes, reporting obstacles, and lack of follow-up are common, which seem to be driven by gaps in expertise and the perception of cybercrime as less serious (Akkermans et al., 2024; Button et al., 2022; Faubert et al., 2021; Graham et al., 2020; Jansen & Leukfeldt, 2018; Notté et al., 2021; Riek & Böhme, 2018; Ruiter et al., 2023). Victims may hesitate to report crimes due to the perceived inability of the police to help (Correia, 2019; Cross et al., 2016a; Kerr et al., 2013; Riek & Böhme, 2018; Toutenhoofd-Visser et al., 2009; Van de Weijer et al., 2018; Wall, 2005). In this dissertation, the exploration of the impact and needs of cybercrime victims, and what this implies for the role of the police, extends beyond the reporting and judicial process. The focus is on understanding the impact of cybercrime and the needs of victims in their own right. This independent examination aligns with the guiding consent paradigm, which implies that the police should adapt to meet the needs of crime victims as part of their mandate.

Since the 1960s, the Dutch police transitioned from the control paradigm to the consent paradigm. Under the control paradigm, the police primarily focused on maintaining order through a repressive approach, typically remaining distant from the public (Van Dijk & Hoogewoning, 2018). In contrast, the consent paradigm broadens the police mandate, emphasizing legitimacy derived from the public. This paradigm positions the police as community-centric, dedicated to enhancing both safety and citizen well-being, alongside traditional crime control measures (Van Dijk & Hoogewoning, 2018). Within this context, understanding the impact and needs of crime victims has become increasingly essential. The consent paradigm underscores the importance for the police to be aware of the impact of crime on well-being and to act accordingly. However, recent years have seen an increasing emphasis on scalability, rapid response, and enforcement, potentially reducing victim-oriented policing efforts (Terpstra et al., 2019). A critical consideration is whether these policing strategies effectively meet the needs of cybercrime victims. Aligning policing practices with the evolving online landscape is crucial, yet there remains insufficient understanding in this area. Gaining knowledge on the impact of (cyber)crimes is needed for the police to determine what their role is in the field of cybercrime, what priority they should give these crimes and how they should treat victims.

Based on the findings on victim impact and needs, this dissertation looks into the Dutch police's role in dealing with cybercrime victims, using it as a representative case study due to similar challenges faced by police forces in other countries in defining their online roles and effectively assisting victims (Button et al., 2022; Cross,

2018; Horsman, 2017). Insights from the Dutch experience can offer valuable lessons for those other jurisdictions. Furthermore, while addressing cybercrime undeniably extends beyond traditional law enforcement (Aiken et al., 2015; Domenie et al., 2013), this dissertation focuses on the police's role. Although the police alone cannot address all aspects of cybercrime effectively, also considering this era of 'plural policing' (Bijleveld et al., 2021; Staats et al., 2021), the police remain important to the initial response and support for victims and therefore also play a role in their coping process (Leukfeldt et al., 2018). The focus of this dissertation on the police is also driven by their multifaceted role, including being the first contact point, offering practical and emotional support, and initiating legal processes for cybercrime.

1.2. Objectives and research questions

The aim of this dissertation is to gain a comprehensive understanding of the victim impact of cybercrime and to clarify the role of the police based on these insights. The dissertation begins by identifying theoretical models and methods for measuring the impact of cybercrime victimization. Once these frameworks are established, the focus shifts to explaining the impact of cybercrime. Comparing cybercrime with traditional crime plays a crucial role in putting the impact of cybercrime into perspective, while the primary goal is to clarify the specific impact of cybercrime. Therefore, traditional crime is incorporated into the research questions to provide a comparative framework for understanding the impact of cybercrime. Additionally, the dissertation examines the needs and reporting experiences of cybercrime victims, using comparisons with traditional crime where relevant. Finally, the dissertation reflects on how the police's role in combatting cybercrime and supporting cybercrime victims should evolve considering the impact, needs, and reporting experiences of cybercrime victims.

The main research question is "*What is the victim impact of cybercrime, and what does this mean for the role of the police?*"

To answer the main research question, the following sub-questions were developed:

1. How can the victim impact of cybercrime and traditional crime be measured?
   a. Which theoretical models and measurement methods are most effective for determining victim impact?
   b. How can a meaningful and feasible comparison be made between the impact of cybercrimes and traditional crimes?

2. What is the victim impact of cybercrime, and how does it compare to the victim impact of traditional crime?
   a. What is the impact of cybercrime on victims, and how can this be explained?
   b. What is the impact of traditional crime on victims, and how can this be explained?
   c. How does the victim impact of cybercrime compare to that of traditional crime, and what factors explain the differences?

3. What implications does the victim impact of cybercrime have for the role of the police?
   a. What are the needs of cybercrime victims compared to those of traditional crime victims, and what factors explain these needs?
   b. How do the reporting experiences of cybercrime victims compare to those of traditional crime victims?
   c. Should the current role of the police be adjusted based on the impact, needs, and reporting experiences of cybercrime victims, and if so, how?

To address the main research question (RQ) and its sub-questions, a multi-method approach was adopted, as outlined in the method matrix in Table 1.1.

Table 1.1. Method matrix

RQs	Expert interviews	Systematic literature review	Secondary analyses data Statistics Netherlands (N = 2,415)	Survey cybercrime and traditional crime victims (N = 910)
1a	X	X		
1b	X	X		
2a			X	
2b				X
2c				X
3a				X
3b				X
3c	X			X

Initially, expert interviews and a systematic literature review were conducted to address RQ 1, focusing on identifying theoretical models and measurement methods for assessing victim impact. To explore the impact of cybercrime and its determinants (RQ 2a), a secondary analysis was carried out using data from Statistics Netherlands (CBS). Data collection from reporting crime victims was then conducted to compare the impact and needs of cybercrime victims versus those of traditional crime victims,

as well as to examine the role of the police (RQs 2 and 3). Throughout the research process, literature was consulted to contextualize the findings and guide the dissertation's focus.

1.3. Overall contribution

1.3.1. Scientific contribution

The answers to the central research question and sub-questions will advance both theoretical and empirical knowledge on the impact of cybercrime. This dissertation addresses a research gap by examining a broad spectrum of cybercrimes and of impact types. Previous research mostly focused on one or a few types of cybercrime or isolated impact forms, and often lacks a comprehensive theoretical and empirical framework (Jansen & Leukfeldt, 2018; Koning et al., 2024; Leukfeldt et al., 2018; Li et al., 2019; Reep-Van den Bergh & Junger, 2018; Riek, 2017). Additionally, the explanatory factors of cybercrime impact have remained largely unknown. Another notable gap is the absence of thorough comparisons between the impact on victims of cybercrime and traditional crime (Button et al., 2021b; Palassis et al., 2021), which provide crucial insights by highlighting contrasts with traditional crime impact. Lastly, this dissertation contributes to theoretical advancement (Bada & Nurse, 2020; Diamond & Bachmann, 2015; Hay & Ray, 2019) by applying aspects of theoretical frameworks such as the shattered assumptions theory (Janoff-Bulman, 1985), coping theory (Agnew, 1985; Jansen & Leukfeldt, 2018; Modic & Anderson, 2015), democratization of victimization (Jansen et al., 2013; Junger et al., 2017), online disinhibition effect (Agustina, 2015; Bada & Nurse, 2020; Suler, 2004) and cyborg theory (Longo, 2018) to the context of cybercrime victimization. These frameworks, along with additional theoretical perspectives, are elaborated upon in the following chapters.

The dissertation takes an exploratory approach covering a broad spectrum of cybercrimes and impact types. The research methodology is mainly quantitative, providing foundational insights into the impacts, needs, and reporting experiences of cybercrime victims. This involves first identifying the range of impact and crime types, determining the most effective measurement methods, and then applying these measurements. While the dissertation does not explore every topic in depth, it aims to establish a crucial foundation for future research, with each chapter contributing to this groundwork. It primarily relies on victim reports collected through surveys, which are effective in capturing individual experiences (Button et al., 2022). Instead

of assigning monetary values or considering sentencing implications—methods that often fail to accurately reflect the real impact (Button et al., 2022; Graves et al., 2019)—this dissertation focuses on understanding the diverse range of impact that crime can have on victims.

1.3.2. Practical contribution

Knowledge about victim impact is essential for policy-making and guiding resource allocation as law enforcement agencies define their role in the digital landscape (Domenie et al., 2013; Riek, 2017). The government's responsibility to act increases with the severity of a crime's impact, requiring that more serious offenses receive higher priority and resources (Button et al., 2022; Leukfeldt et al., 2018). The experiences of individual victims not only reveal personal consequences but also reflect the broader societal impact of cybercrime, making it essential to consider these (Button et al., 2022; Kerr et al., 2013). Understanding victim impact is important given the constraints of limited resources; not every case can be pursued with equal effort. This knowledge is especially critical for emerging crimes like cybercrime, where the full extent of the impact is not yet fully understood. By accurately assessing victim impact, law enforcement agencies can ensure that cybercrime receives appropriate attention and resources, while also upholding procedural justice for all crime victims (Graham et al., 2020).

This dissertation offers valuable insights into police policies related to cybercrime victims and provides recommendations for improvements. Each chapter emphasizes the practical implications of its findings for law enforcement agencies and other stakeholders, helping these organizations develop strategies that more effectively address the needs and experiences of cybercrime victims. This can contribute to a more effective and legitimate response to cybercrime and help refine the roles of the police and their partners in this evolving domain. The victim-centered approach adopted in this dissertation ensures that the actual experiences of victims can inform policy-making. Fully understanding the scope of victims' impacts and needs is crucial for ensuring fair treatment, addressing their primary concerns, and ensuring that victims feel genuinely heard, validated, and supported (Van der Vijver, 1993). By deepening insights into victims' emotional and behavioral responses to cybercrime, law enforcement agencies can better tailor their support strategies to facilitate recovery (Li et al., 2019). This, in turn, can strengthen the legitimacy of the police and increase public trust, as they may then be perceived as more attuned and responsive to the needs of the communities they serve (Faubert et al., 2021; Hageman & Loeffen, 2016).

1.4. Outline of the dissertation

1.4.1. Guide to the reader

In the following chapters, this dissertation presents the various studies in greater detail. Each chapter is designed to be read independently (except for the Intermezzo following Chapter 6), which has resulted in some repetition of method descriptions, theoretical discussions, and other content across the chapters. Additionally, as the research progressed, evolving insights led to differences in terminology and occasional contradictions within the text. To maintain visual consistency, all chapters have been uniformly formatted, while the content itself remains unchanged. The final chapter provides a comprehensive conclusion and discussion. An outline of the individual studies is provided below.

1.4.2. Chapter 2. Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions

The first study establishes the foundation for the dissertation by underscoring the need to build knowledge on the impact of cybercrime victimization. It also highlights the importance of comparing the impact of cybercrime and traditional crime from both academic and practical perspectives. Through a systematic literature review, the study provides an overview of the current state of research. It identifies key studies that consider the impact of cybercrime and the characteristics of cybercrime that could be associated with that impact, such as its intangibility, permanence, and the prevalence of victim blaming. The study reveals a limited understanding of the impact of cybercrime and the differences with the impact of traditional crime. Several directions for further research are suggested to address this.

1.4.3. Chapter 3. The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory

The second study seeks to predict and explain the impact of cybercrime on victims using the shattered assumptions theory (SAT) as a framework. The SAT suggests that victimization disrupts some of the fundamental, positive assumptions people hold about themselves and the world, such as being invulnerable and autonomous, and the world's controllability and comprehensibility. The study applies the SAT to develop hypotheses about the impact of different crime types, namely hacking, financial cybercrime, and person-centered cybercrime. It distinguishes between the psychological impact on emotional well-being and the impact on victims' sense of

security in the digital environment. A secondary analysis was conducted on a dataset from Statistics Netherlands (CBS) involving 2,415 cybercrime victims. The findings reveal variations in psychological impact across explanatory factors and provide insights into the relevance of the SAT for understanding the psychological impact of cybercrime. The theory was found to be less effective in explaining cybercrime-related sense of security than in explaining emotional well-being.

1.4.4. Chapter 4. The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors

The third study builds on the same dataset from Statistics Netherlands (CBS) (N = 2,415) to further explore the impact of cybercrime on victims' emotional well-being and cybercrime-related sense of security, focusing on the influence of personal (mostly demographic) and circumstantial (offense-related) factors. It employs the democratization of victimization, coping theory, and cyborg theory as theoretical frameworks, while also drawing on empirical studies of traditional and cybercrime victim impact to develop hypotheses. The findings shed light on how various personal and circumstantial factors shape the psychological impact of cybercrime, emphasizing the differences between the impact on emotional well-being and cybercrime-related sense of security. The study reflects on these findings through the lenses of the aforementioned theoretical frameworks, while also taking into account the concept of online disinhibition.

1.4.5. Chapter 5. Exploring the impact of cybercrime and traditional crime victimization: Impact comparisons and explanatory factors

In the fourth study, the victim impact of cybercrime and traditional crime is compared. Furthermore, the study measures determinants of victim impact and whether these differ for cybercrime and traditional crime, including crime characteristics, as well as social, personal and demographic factors. A survey was completed by 910 crime victims who reported to the police, covering both cybercrime and traditional crime forms of burglary, scams, threat and violation of physical integrity. The data revealed an unanticipated categorization of impact into internalizing problems, externalizing problems, financial impact and damaged self-image. The findings offer conclusions about how the impact of cybercrime differs from that of traditional crime. Additionally, the study identifies significant determinants of victim impact, with variations observed between cybercrime and traditional crimes.

1.4.6. Chapter 6. Doing justice to the needs of cybercrime victims: reflections on the role of the police

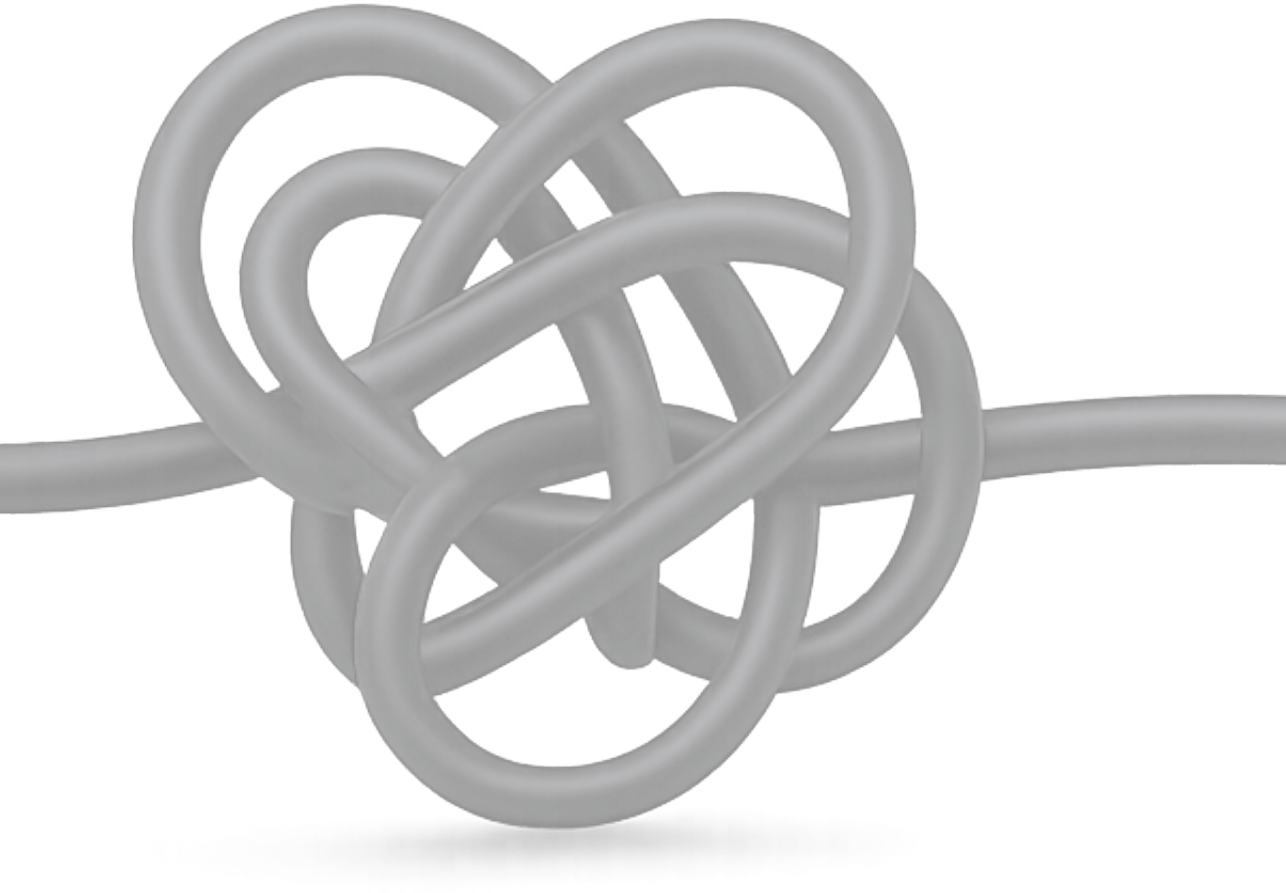
The final study explores the needs and reporting experiences of cybercrime victims in comparison to traditional crime victims, with a focus on the implications for the role of the police, utilizing the same victim survey data (N = 910) and crime categories as in Chapter 5. The study also assesses the explanatory value of victim impact, crime characteristics, and various demographic, personal and social factors for victims' needs. The differences in the explanatory value for these factors between cybercrime and traditional crimes are considered. The findings reveal differences in needs, reporting experiences, and the significance of explanatory value for cybercrime versus traditional crime victims. The study discusses the implications of the findings for the role of the police, highlighting the importance of responsiveness to cybercrime victims needs for upholding police legitimacy.

1.4.7. Intermezzo. Reporting cybercrime online versus in-person: A comparison of victim experiences

Following Chapter 6, an intermezzo presents a focused analysis conducted as part of the broader study on victim reporting experiences. It examines whether the method of reporting—online versus in-person—shapes how cybercrime victims experience the police reporting process. The findings show that online reporting is linked to significantly lower satisfaction across multiple dimensions of the experience. The intermezzo reflects on the challenges of ensuring adequate victim support at a time when police services are increasingly shifting to digital platforms.

1.4.8. Chapter 7. General conclusion and discussion: The impact and needs of cybercrime victims and the implications for police practice

Chapter 7 concludes the dissertation by addressing the central research questions and synthesizing the key findings in a comprehensive manner. It further discusses the theoretical contributions and practical implications of the dissertation, particularly regarding policy development and intervention strategies aimed at supporting cybercrime victims. The chapter also considers the main limitations of the studies and offers suggestions for future research, identifying concrete directions for building on the insights gained. It concludes with a forward-looking reflection on emerging developments in cybercrime and their potential implications for victim impact.



Chapter 2

Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions

Jildau Borwell, Jurjen Jansen, Wouter Stol

Originally published in Journal of Digital Social Research 2021, 3(3), 85-110.

2.1. Introduction

This chapter 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 chapter, cybercrime is defined as crime for which information and communication technology (ICT) plays an essential role in the execution of the offense (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 offense (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 (CBS), 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 (CBS), 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 chapter 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 cyber-

crime from a victim's perspective. Thereafter, shortcomings in current literature are discussed and future research directions are proposed. The focus of this chapter 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.

2.2. The relevance of comparing the impact of cybercrime and traditional 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 (Council of Europe, 2001; 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 & Sharma, 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.

2.3. 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[3]. 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,

[3] 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*")).

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.

2.4. 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 and colleagues (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 offense, 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.

2.5. 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 offense 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., 2016b; 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.

2.6. Shortcoming 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 offense-centered instead of victim-centered and in a lack of focus on the impact for individual victims. Most studies focus on the committed offenses 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., 2016b; 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.

2.7. 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.

2.7.1. 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 offense, 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 (Council 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 offense. 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.

2.7.2. 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 et al., 2015; Neufeld, 2010; Sabillon et al., 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 offense—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 offense (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 offense 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.

2.7.3. 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 offense 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., 2021b; Van der Wagen & Pieters, 2018). Furthermore, determinants influencing the impact can be specific to cybercrimes, such as the anonymity, perma-

nence 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 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., 2021b; 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.

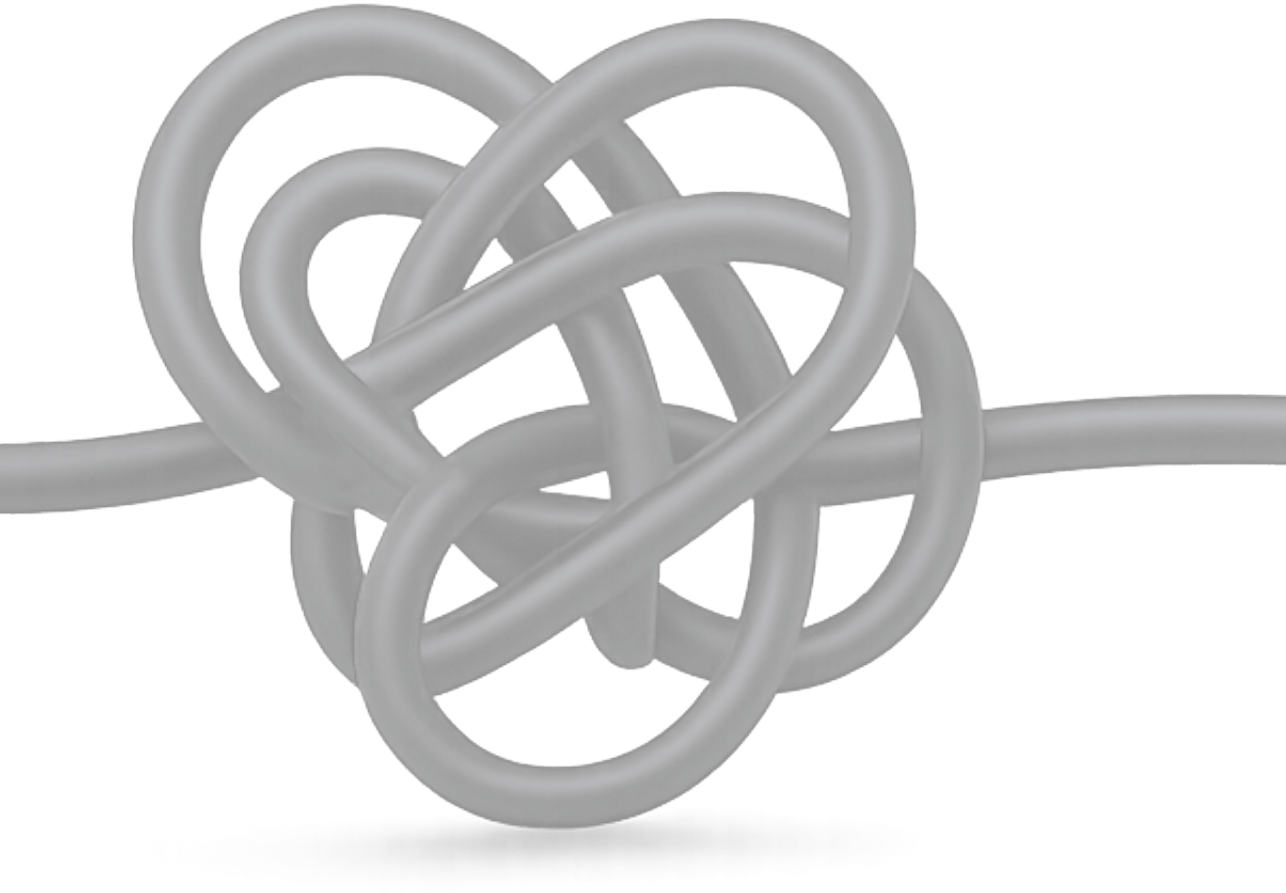
Personal and social factors are also related to victimization impact, and therefore need to be controlled for when measuring the impact of crime. Firstly, personal factors such as demographic and socio-economic factors, coping skills, personality, but also important life events such as previous victimization might influence victimiza-

tion impact (Borwell et al., 2021b; 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 offense 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., 2016b; Kerr et al., 2013; Leukfeldt et al., 2018; Whitty & Buchanan, 2016).

2.8. Concluding remarks

This chapter 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.



Chapter 3

The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory

Jildau Borwell, Jurjen Jansen, Wouter Stol

Originally published in Social Science Computer Review 2021, 40(4), 933-954.

3.1. Introduction

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 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 (CBS), 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 con-

tributes 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).

3.2. Literature review and expectations from the SAT

3.2.1. 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 victimiza-

tion. '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.

3.2.2. 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 (CBS), 2019). Later in this chapter, 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[4] (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

[4] 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).

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).

3.2.3. 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.

3.2.4. 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 suggests 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.*

3.3. 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.

3.3.1. 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.

3.3.2. 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 (CBS), 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 a 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) housefather 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%.

3.4. 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 3.1. 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).

Table 3.1. 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 (.94)	502
Financial cybercrime[b]			
Online banking fraud	1.42 (.71)	1.85 (.88)	212
Identity fraud (orders)	1.46 (.76)	1.91 (.92)	178
Consumer fraud	1.53 (.70)	1.64 (.77)	856
Fake fine/bill/campaign	1.67 (.98)	1.87 (.92)	75
Microsoft fraud	1.52 (.89)	1.62 (.79)	42
Wangiri fraud	1.38 (.55)	2.01 (1.08)	119
Person-centered cybercrime			
Stalking	1.68 (.90)	1.50 (.79)	119
Libel/slander	1.61 (.85)	1.44 (.70)	273
Violent threat	1.54 (.76)	1.05 (.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 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 3.2. 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 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

Table 3.2. 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.
*$p < .05$; **$p < .01$.

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 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 (H3). No significant differences in emotional well-being means were found $F(3, 259) = 2.08$, $p = .1$. Although the 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 to compare the mean impact scores on sense of security showed no significant difference between the means: $F2(3, 132.19) = 1.65$; $p = .18$. H3, therefore, was not supported.

To test whether the psychological impact of cybercrime victims who experienced financial loss is lower when that loss was compensated (H4), 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; 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 H4. 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, H4 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 cybercrime victims who did not actively contribute to the crime (H5). 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). H5 was therefore rejected.

To test whether the psychological impact of cybercrime is higher for victims with a higher SES (H6), two two-way between groups ANOVA tests were conducted. Respondents were grouped according to income level (group 1: lowest 20 percent to group 5: highest 20 percent) 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 group 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 p-value of .04; $F(3, 2296) = 2.83$, 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, H6 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 3.3 summarizes the findings for all hypotheses.

Table 3.3. 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.

3.5. Discussion and conclusion

3.5.1. 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 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.

3.5.2. 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 compensa-

tion, 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).

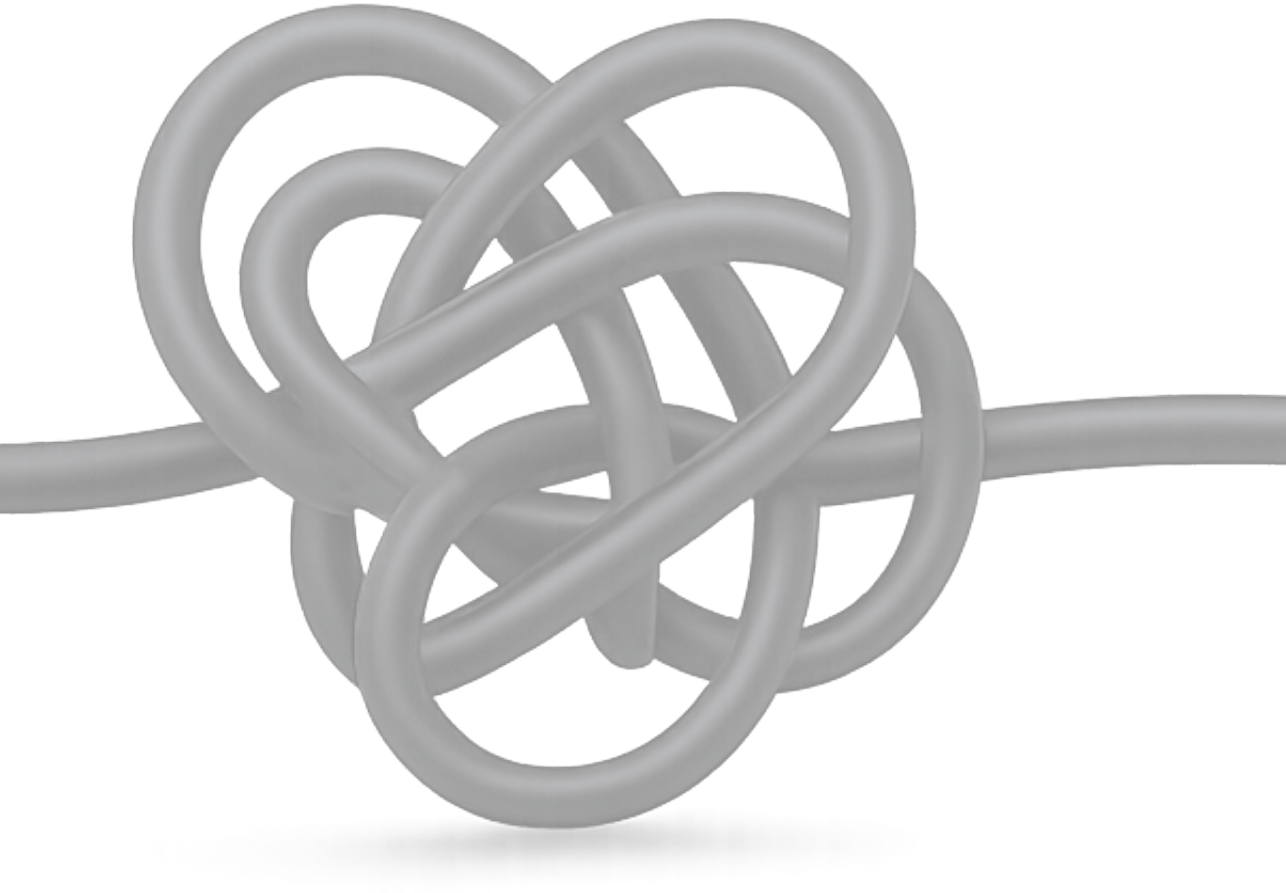
In future work, the applicability of the SAT on cybercrime victimization could be explored further. This study demonstrated that the SAT is suitable for developing expectations about the psychological impact of cybercrime and thus might help to understand the impact of cybercrime, even though the SAT 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.

3.5.3. 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 3.2. 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.



Chapter 4

The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors

Jildau Borwell, Jurjen Jansen, Wouter Stol

Originally published in European Journal of Criminology 2025, 22(4), 603-624.

4.1. Introduction

The prevalence of cybercrime has risen in recent years (Akkermans et al., 2024; Button et al., 2022; Reep-Van den Bergh and Junger, 2018). According to the Crime Survey for England and Wales, 45% of all crime involves fraud or computer misuse, making it comparable in scale to traditional crime (Office for National Statistics, 2021). In the Netherlands, 16% of citizens were victims of cybercrime in 2023, close to the 20% who experienced traditional crime (Akkermans et al., 2024). As society becomes more digitized and reliant on technology, opportunities for cybercrime offenders continue to expand, likely leading to further increases in cybercrime rates (Diamond and Bachmann, 2015; Holt and Bossler, 2014; Riek, 2017). For cybercrime victims, the psychological and emotional impact can be similar to that of traditional crime, often resulting in stress, anxiety, and, in severe cases, depression or suicidal thoughts (Button et al., 2020; Kerr et al., 2013; Leukfeldt et al., 2018). Many victims report feelings of intrusion, physical violation, and danger (Button et al., 2020; Kerr et al., 2013). Understanding these implications for victims is crucial, given the ongoing shift toward the digitization of crime (De Kimpe et al., 2020).

The impact of cybercrime has received less attention in research and practice compared to traditional crime (Diamond and Bachmann, 2015; Van der Wagen and Pieters, 2018). This study enhances the body of literature by exploring the psychological impact of cybercrime on victims and exploring factors influencing that impact. Research indicates that the effects of victimization can vary widely (Dunn, 2007; Janoff-Bulman and Frieze, 1983; Shapland and Hall, 2007; Vanderstraeten et al., 2012). Beyond the type of crime (Agnew, 1985; Dinisman and Moroz, 2017; Lamet and Wittebrood, 2009; Shapland and Hall, 2007), personal factors (e.g., demographic and socioeconomic characteristics) and circumstantial factors concerning the crime (e.g., direct consequences and duration of the crime) (Button et al., 2014; Dinisman and Moroz, 2017; Jansen and Leukfeldt, 2018; Lamet and Wittebrood, 2009; Li et al., 2019; Shapland and Hall, 2007) can shape these effects. However, how such factors relate to the impact of cybercrime victimization remains largely unclear. Cybercrime introduces unique victimological and criminological elements (Moitra, 2005; Van der Wagen and Pieters, 2018; Wall, 2005). Differences reside in technological aspects, intangible tools, anonymity, and a lack of spatial-temporal boundaries (Diamond and Bachmann, 2015; Moitra, 2005). Thus, theories and empirical results from traditional crime may not always be applicable to cybercrime (Van der Wagen and Pieters, 2018).

This study aims to clarify how personal and circumstantial factors influence the psychological impact of cybercrime, building on Borwell et al.'s (2021) work

using the same dataset. That study, applying the shattered assumptions theory as a framework (Janoff-Bulman, 1985), found that person-centered cybercrime had a greater negative effect on victims' emotional well-being, while financial cybercrime and hacking had a more negative impact on victims' cybercrime-related sense of security (how secure victims feel in the digital world and how distrustful or fearful they are of it because of the crime). As in the previous study, we define cybercrime as crime for which information and communication technology plays an essential role in the execution of the offense (Domenie et al., 2013). We distinguish (1) hacking (i.e., breaking into a device or account); (2) financial cybercrime (i.e., cybercrime with a financial motive, such as online banking fraud, identity fraud, and consumer fraud); and (3) person-centered cybercrime (i.e., cybercrime with a personal motive, such as stalking, threat, and libel/slander). Psychological impact is defined as the psychological or emotional seriousness or severity of the effects of crime as perceived by victims (Groenhuijsen, 1996; Jansen and Leukfeldt, 2018).

In the current study, we aim to further explore the determinants of cybercrime victimization impact by incorporating new measures, namely personal and circumstantial factors. We address a research gap by primarily drawing on the democratization of victimization theory, which suggests that cybercrime victimization may be more evenly distributed across the population (Jansen et al., 2013). To explore potential nuances and exceptions to this theory when it comes to victimization *impact*, we incorporate coping and cyborg theory, which help explain the patterns of psychological impact and why those may not be as randomly distributed as the democratization of victimization suggests. Coping mechanisms affect how individuals handle the psychological effects of cybercrime and are dependent on personal factors. Cyborg theory, exploring the fusion of humans and technology, helps us understand the subjective experience of cybercrime and how this depends on the crime circumstances.

Our goal is to enhance academic understanding and inform effective prevention and support strategies. Current regulations, such as the EU Minimum Standards on Victims' Rights, focus on emotional recovery (Kunst and Koster, 2016), but often fall short because of the focus on legal proceedings, while these phases are often not reached for cybercrime victims due to the low number of solved cases (Leukfeldt et al., 2018; Veenstra et al., 2013). By identifying factors influencing the psychological impact of cybercrime, our findings can help refine prevention and support efforts for victims, benefiting law enforcement, victim support services, and financial institutions (Aiken et al., 2015; De Kimpe et al., 2020; Leukfeldt et al., 2018). The research question

guiding this study is: 'What is the relationship between personal and circumstantial factors and the psychological impact of cybercrime victimization?'

4.2. The democratization of victimization, coping, and personal factors

In a digitized society, the risk of victimization appears more evenly distributed across various groups, a phenomenon referred to as the 'democratization of victimization' (or 'normalization of victimization'), previously described in the cybercrime literature by Jansen et al. (2013) and Junger et al. (2017). Unlike traditional crime, where victims are typically young, male, less educated, and lower income, digitalization seems to have made cybercrime victims more representative of the general population (Jansen et al., 2013; Junger et al., 2017). This shift suggests that online behaviors—such as sharing personal information or clicking on suspicious links—may influence victimization risk more than immutable characteristics such as age or gender. However, it remains uncertain whether this distribution is truly random, or if new patterns are emerging. For example, younger individuals may still be at higher risk of cybercrime, potentially due to their online activity (Brands and Van Wilsem, 2019; Jansen et al., 2013; Oksanen & Keipi, 2013; Virtanen, 2017).

Additionally, while older individuals and women may report greater fear of cybercrime (Virtanen, 2017), the relationship between personal factors and victimization *impact* remains less understood. This study extends the democratization of victimization concept by questioning whether cybercrime affects everyone equally or if new patterns of vulnerability are emerging. A person's vulnerability can be influenced by their coping abilities and resilience (Button et al., 2014; Janssen et al., 2021). Coping strategies, which aid recovery from fear, stress, or danger, are shaped by personal factors and may apply equally to both traditional and cybercrime victimization (Janoff-Bulman and Frieze, 1983; Jansen and Leukfeldt, 2018). Neutralization techniques such as rationalizing the crime as less harmful are examples of coping mechanisms that can mitigate the impact (Agnew, 1985; Modic and Anderson, 2015).

Below, we will develop hypotheses on how personal factors (namely age, household situation, gender, socioeconomic status [SES], origin, and religion) might influence victimization impact, drawing on both traditional crime (coping) literature and relevant insights from cybercrime literature where available. The democratization of victimization impact would suggest that there are no differences between the groups.

Age. Age can influence the psychological impact of crime victimization. Older individuals are more likely to report emotional distress following such events (Lamet and Wittebrood, 2009). Agnew (1985) found that both younger and older individuals tend to use fewer neutralization techniques, possibly due to their heightened vulnerability and that they are usually more severely injured, making denial or rationalization of the event more challenging. Also, the impact of hacking or identity fraud seems to be more pronounced for older people than for younger people (Golladay and Holtfreter, 2017; Van de Weijer et al., 2018). This could be attributed to limited resources and coping skills among the elderly (Cross, 2015). Therefore, we arrive at the following hypothesis:

Hypothesis 1: The psychological impact of cybercrime increases with age

Household situation. Social support seems important for coping with online and offline crime victimization (Button et al., 2020; De Kimpe et al., 2020; Dinisman and Moroz, 2017; Ten Boom et al., 2008). Prior research indicates that having a social support network or being married can reduce the negative impact of crime (Golladay and Holtfreter, 2017). Conversely, individuals who are divorced or live alone are more likely to experience emotional challenges following victimization, likely due to weaker social support systems (Lamet and Wittebrood, 2009). For cybercrime victims, the frequent lack of support from authorities can make reliance on personal networks even more critical (Cross, 2018; Leukfeldt et al., 2018). It is therefore expected that living alone is associated with a higher psychological impact. Thus, we hypothesize:

Hypothesis 2: People who live alone experience more psychological impact from cybercrime than people who do not live alone

Gender. Research indicates that gender affects the impact of crime victimization, with women typically experiencing more severe emotional effects from cybercrime and traditional crime (Dinisman and Moroz, 2017; Lamet and Wittebrood, 2009; Rosoff et al., 2014; Ten Boom et al., 2008). For instance, female victims seem to experience higher distress and more distrust compared to men (Norris & Kaniasty, 1991). Consequently, we hypothesize:

Hypothesis 3: Women experience more psychological impact from cybercrime than men

Socioeconomic status. SES might significantly influence the impact of crime on victims as well (Bonanno et al., 2011; Borwell et al., 2021; Lamet and Wittebrood, 2009).

Victims with higher SES generally experience less severe psychological impact due to better access to coping resources and support, which aids in managing both online and offline crime (Agnew, 1985; Bonanno et al., 2011; Brands and Van Wilsem, 2019). Previous research shows that individuals with low SES experience stronger emotional effects from identity fraud (Golladay and Holtfreter, 2017) and are more likely to develop mental health problems after victimization (Dinisman and Moroz, 2017). Therefore, we expect the following:

> *Hypothesis 4: The psychological impact of cybercrime decreases with increasing socio-economic status*

Origin. Research indicates that ethnic origin can influence the psychological impact of crime. Ethnic minorities often face greater challenges in meeting their needs after victimization (needed for effective coping) and tend to have higher safety-related concerns (Ten Boom et al., 2008). They are also more prone to developing mental health issues following victimization and experience more intense emotional effects from identity fraud (Dinisman and Moroz, 2017; Golladay and Holtfreter, 2017). We developed the following hypothesis:

> *Hypothesis 5: Ethnic minorities experience more psychological impact from cybercrime than ethnic majorities*

Religion. Religion may influence the psychological impact of crime. Religious individuals often hold beliefs in 'ultimate justice' or 'immanent justice', where they trust that wrongdoers will be punished and they themselves will ultimately receive what they deserve (Pemberton, 2011). This belief can aid in coping by helping individuals redefine or neutralize their victimization experience (Agnew, 1985; Janoff-Bulman, 1985). We therefore come to our next hypothesis:

> *Hypothesis 6: Religious people experience less psychological impact from cybercrime than non-religious people*

4.3. Cyborg theory and circumstantial factors

Cyborg theory helps explain the impact of cybercrime by viewing computers as extensions of our bodies rather than mere tools (Van der Wagen and Pieters, 2018). Humans can nowadays be seen as 'cyborgs': hybrid forms of human and machine (Haraway, 1985; Van der Wagen and Pieters, 2018). People may experience their devices as extensions of themselves, making attacks on these devices feel like physical

invasions (Haraway, 1985; Longo, 2018; Van der Wagen and Pieters, 2018). This theory suggests that cybercrime can have a similar emotional impact as traditional crime, as both often involve violations of something closely tied to the self, be it a computer, body, or home (Button et al., 2020; Leukfeldt et al., 2018; Van der Wagen and Pieters, 2018). If people are experientially connected to their devices, the nature of a cyber-offense—what device was targeted, what happened to it, and the duration of the incident—likely influences victimization impact. Below, we will explore how this theory informs our hypotheses about that impact. To the best of our knowledge, this theory has not been previously tested in the context of cybercrime victimization impact. Again, the democratization of victimization impact would suggest that there are no differences between groups.

Hacked device or account. Hacking can be seen as a direct intrusion into devices to which people feel connected, as suggested by cyborg theory (Longo, 2018). While hacking victims do not seem to report higher impact than other cybercrime victims (Borwell et al., 2021), the specific target of the hack might influence the psychological effect. Hacking an entire device (e.g., phone or PC) may cause greater psychological distress than hacking a single account (e.g., social media or email account) not tied to a specific device. This leads to the following hypothesis:

> *Hypothesis 7: Hacking victims experience more psychological impact when their devices are hacked than when their accounts are hacked*

Hacking consequences. The consequences of a hacking incident can also influence the psychological impact on the victim. Previous research indicates that victims often react more strongly to the aftermath of a cyberattack than to the attack itself (Bada and Nurse, 2020). In line with cyborg theory, we expect that the severity of the impact may vary depending on whether an entire device was compromised or if 'only' an account was misused. The psychological impact could be more severe if the hacking leads to a malware infection—rendering the device inoperable, causing the loss of important files, or requiring software reinstallation—compared to situations where a social media or email account was misused or nothing noticeable happened. This leads to the following hypothesis:

> *Hypothesis 8: Hacking victims experience more psychological impact when a malware infection took place than when their accounts were misused or nothing noticeable happened*

Duration of person-centered crime. The psychological impact of a crime may also be more severe if it occurs over an extended period (Lamet and Wittebrood, 2009). From the cyborg theory, the impact is expected to intensify the longer the incident lasts, as it involves devices to which victims feel connected. Digital victimization relatively often persists over time without a clear beginning or end (Jahankhani et al., 2014; Van der Wagen and Pieters, 2018). In our dataset, the duration of the crime is measured for person-centered cybercrime, where the ongoing interaction between victim and offender may prolong the experience. Therefore, we hypothesize:

> *Hypothesis 9: The psychological impact of person-centered cybercrime increases with the duration of the crime*

4.4. Current study

In this study, we examine how various personal and circumstantial factors affect the psychological impact experienced by cybercrime victims. Current literature reveals a gap in understanding this. To address that gap, we developed the above hypotheses guided by the concepts of democratization of victimization, coping theory, and cyborg theory, which will be tested with data from a large survey described in the following section. While the democratization theory would suggest no significant effects of personal and circumstantial factors, both coping and cyborg theories predict certain victimization impact differences between groups. Although our study does not test these theories in their entirety, the results may provide insights into their relevance for understanding victimization impact. In the discussion section, we will evaluate how our findings relate to these theoretical concepts, helping to guide future research on cybercrime victimization.

4.5. Materials and methods

4.5.1. Dataset and selection of respondents

We conducted a secondary analysis using survey data from Statistics Netherlands (2019) among Dutch citizens (N = 33,702), collected between October and November 2018. The survey topics included cybercrime victimization and its psychological impact. We selected victims (aged 18 years and older) of hacking, financial cybercrimes, and person-centered cybercrimes. Hacking was characterized as breaking into a device (N = 502). Financial cybercrime was divided into six subcategories, namely

(1) online banking fraud (N = 212); (2) identity fraud (N = 178); (3) consumer fraud (N = 856); (4) fake fine/bill/campaign (N = 75); (5) Microsoft scam (where offenders approach victims about so-called problems with their computer and offer to resolve them against payment; N = 42); and (6) Wangiri fraud (where offenders call victims to redirect them to an expensive pay phone number; N = 119). Person-centered cybercrime was divided into three subcategories, namely (1) stalking (N = 119), (2) violent threat (N = 273), and (3) libel/slander (N = 39). For further details on the dataset, selection process, and measures, refer to the original publication on this dataset by Statistics Netherlands (2019) and the study by Borwell et al. (2021).

4.5.2. Operationalization

Cybercrime victimization. Respondents were asked if they had been victimized by any of the specified cybercrimes in the past 12 months. If affirmative, further questions were asked about the most recent incident. Statistics Netherlands excluded respondents who were compensated partially for consumer fraud, as partial compensation was deemed atypical for this crime type. Financial crime victims without financial loss were excluded, except for victims of payment fraud and identity fraud, given that their accounts were accessed. Hacking incidents that were part of another crime type were included under that primary category. We also excluded 364 respondents who experienced multiple crime types, as this could confound the impact assessment. The final sample consisted of 2415 victims: 502 from hacking, 1482 from financial cybercrime, and 431 from person-centered cybercrime.

Psychological impact. Respondents reported if they experienced any of the following consequences after the crime (yes = 1 or no = 0): (1) reduced trust in digital safety; (2) reduced trust in their own digital skills; (3) fear of repeat victimization; (4) persistent thoughts about the incident; (5) anger; (6) sleep deprivation; (7) other effects, namely…; or (8) none of the above. Using principal component analysis and mean interim correlations, two psychological impact scales were developed: (1) emotional well-being—this scale, including options 4–6, includes the direct impact on the victim's emotional state; (2) cybercrime-related sense of security—this includes options 1–3, assesses how secure victims feel in the digital world and how distrustful or fearful they are of it because of the crime. Options 7 and 8 were excluded. The Cronbach's alpha coefficients for the two scales were relatively low (0.48 for emotional well-being and 0.44 for sense of security). However, the mean inter-item correlations fell mostly within the acceptable range of 0.2–0.4, supporting the use of these scales for further analysis.

Age. Age was categorized into four groups: 18–35, 36–50, 51–65, and 66 and over, based on administrative records linked to the respondent by Statistics Netherlands.

Household situation. Household situation was also based on administrative records from Statistics Netherlands, categorized as single-person households, couples without children, couples with children, and single-parent households. Single-person and single-parent households were grouped as 'living alone' due to typically lower social support.

Gender. Gender was recorded as male or female, linked to the respondents by registered data from Statistics Netherlands.

Socioeconomic status. Respondents were asked to select their employment status: (1) working/self-employed; (2) unemployed; (3) volunteer; (4) incapacitated; (5) student; (6) housefather or househusband/housemother or housewife; (7) pensioner; (8) none of the above; and (9) refusal. Options 8 and 9 were excluded, and options 2, 3, 4, and 6 were grouped as 'unemployed.' Furthermore, respondents were categorized into five income quintiles based on registered data and the standard classification method of Statistics Netherlands, starting from the lowest 20% of standardized incomes in the first quintile until the highest 20% in the fifth quintile.

Origin. Origin was added from registered Statistics Netherlands data and categorized as follows: (1) Dutch origin; (2) Western origin; (3) Moroccan origin; (4) Turkish origin; (5) Surinam origin; (6) Antillean origin; and (7) other non-Western origin. We considered category 1 as Dutch origin (ethnic majorities), 2 as other Western origin (ethnic minorities), and 3–7 as non-Western origin (ethnic minorities). A person is considered of foreign origin by Statistics Netherlands if they or at least one of their parents were born outside the Netherlands (Van Andel & Joosten, 2017).

Religion. Respondents' religiousness was assessed with the following options: (1) no church affiliation or ideological group; (2) Roman Catholic; (3) Dutch Reformed; (4) Reformed Churches; (5) Protestant Church of the Netherlands; (6) Islam; (7) Jewish; (8) Hindu; (9) Buddhist; (10) other church affiliation or ideological group. Option 1 was classified as 'non-religious', and options 2–10 were classified as 'religious'.

Hacked device or account. Hacking victims were asked what happened during that incident with the following choices: (1) my computer (desktop/laptop/tablet)/network has been broken/logged into without authorization; (2) my e-mail account has been broken/logged into without authorization; (3) my mobile phone has been broken/

logged into without authorization; (4) my social media account has been broken/logged into without authorization; (5) my household appliances such as security equipment or baby monitor has been broken/logged into without authorization; (6) something else has been broken/logged into without authorization; (7) do not know/unknown. Options 1 and 3 were categorized as 'device'. Options 2 and 4 were categorized as 'account'. Option 5 did not occur in the data, and options 6 and 7 were excluded.

Hacking consequences. Hacking victims were asked to specify the consequences of the incident, choosing from the following options: (1) suffered from viruses that made me lose my data; (2) misuse of my (personal) data on the internet (spyware); (3) blocking, disrupting, or hostage-taking of my computer data, which could be restored for a fee (ransomware); (4) stealing of my data via a trojan horse; (5) encryption of my computer data (cryptoware); (6) suffered from other malicious software (malware); (7) misuse of my computer system, for instance in a botnet, for distributed denial of service (DDoS) attacks or crypto mining; (8) misuse of my e-mail account or profile page; (9) transferring my internet traffic to an illegal website (pharming); (10) other consequences, namely…; or (11) no noticed consequences. Options 1–7 and option 9 were categorized as 'malware infection', option 8 as 'misuse of e-mail account or profile page', and option 11 as 'no further consequences'. Option 10 was excluded.

Duration person-centered cybercrime. Respondents who experienced person-centered cybercrimes (stalking, violent threat, and libel/slander) were asked about the duration of the crime with the following options: (1) one-off incident; (2) less than 1 week; (3) longer than 1 week but less than 1 month; (4) longer than 1 month but less than 3 months; (5) 3–6 months; (6) 6 months to a year; (7) longer than a year; or (8) do not want to say. We grouped these into four categories: option 1 (once); options 2 and 3 (less than a month); options 4 and 5 (1–6 months); and options 6 and 7 (longer than 6 months). Option 8 was excluded.

4.5.3. Statistical tests

To test the hypotheses, we used *t* tests for comparisons between two groups and ANOVA (analysis of variance) tests for comparisons between more than two groups. Welch tests were applied where variances differed. Despite some deviations from normality, the large sample size justified this approach. We opted for two-sided tests due to the exploratory nature of the study, and because prior research and theories do not consistently align. The utilization of ANOVA and *t* tests in our study also aligns

with its exploratory nature. Instead of regression analysis, which assesses variables in relation to one another, we explored individual effects. This reflects our intent to examine distinct impacts and address practical concerns, as individual effects are often more relevant to practitioners.

4.6. Results

Hypothesis 1. To test whether the psychological impact of cybercrime increases with age, we conducted two one-way ANOVA tests (see Table 4.1). For emotional well-being, a Welch test was performed due to unequal variances indicated by Levene's test. The results showed no statistically significant difference between age groups: $F2(3, 884.09) = 2.34$, $p = .07$. The second ANOVA test on sense of security revealed a difference: $F(3, 2069) = 3.01$, $p < .05$. Post hoc comparisons using the Tukey's honestly significant difference (HSD) test showed that the youngest group ($M = 1.66$; $SD = .82$) experienced a significantly lower impact on sense of security than the oldest group ($M = 1.83$; $SD = .85$) with $p < .05$. The second and third age groups did not differ significantly from the others. Hypothesis 1 was therefore confirmed for sense of security but not for emotional well-being.

Table 4.1. ANOVA and *t* tests of differences in mean psychological impact

	Mean psychological impact — emotional well-being (*SD*)	Mean psychological impact — sense of security (*SD*)	*N*
Age group			
18–35	1.43 (.69)	1.66 (.82)	667
36–50	1.48 (.75)	1.75 (.90)	616
51–65	1.46 (.71)	1.68 (.82)	536
>66	1.58 (.79)	1.83 (.85)	254
ANOVA *F*	2.34[a]	3.01*	
Household situation			
Living alone	1.54 (.79)	1.68 (.82)	595
Not living alone	1.45 (.71)	1.68 (.85)	1809
t	2.51*[b]	0.15	
Gender			
Female	1.51 (.76)	1.71 (.86)	1148
Male	1.44 (.70)	1.65 (.82)	1267
t	–2.43*[b]	–1.92	

Table 4.1 continues on next page.

Table 4.1. ***Continued***

Variables and statistical tests	Mean psychological impact — emotional well-being (*SD*)	Mean psychological impact — sense of security (*SD*)	*N*
Socioeconomic status			
Income level			
First 20%	1.53 (.80)	1.66 (.82)	288
Second 20%	1.50 (.76)	1.73 (.84)	309
Third 20%	1.56 (.79)	1.72 (.86)	454
Fourth 20%	1.49 (.74)	1.69 (.87)	566
Fifth 20%	1.36 (.63)	1.67 (.81)	699
ANOVA *F*	3.98**[b]	0.22	
Employment situation			
Paid job/self-employed	1.43 (.70)	1.69 (.84)	1366
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**	
Origin			
Dutch	1.47 (.73)	1.68 (.84)	1976
Western other	1.43 (.71)	1.70 (.88)	239
Non-Western	1.53 (.76)	1.64 (.82)	200
ANOVA *F*	0.99	0.35	
Religion			
Non-religious	1.45 (.72)	1.66 (.84)	1463
Religious	1.52 (.74)	1.70 (.83)	952
t	–2.31*[b]	–1.07	
Hacked device or account			
Device	1.51 (.82)	2.06 (1.01)	49
Account	1.24 (.53)	1.76 (.91)	384
t	3.13*[b]	2.25*	
Hacking consequences			
Malware infection	1.41 (.70)	2.05 (1.04)	76
Misuse of e-mail/profile	1.30 (.64)	1.93 (.94)	120
No further consequences	1.17 (.43)	1.72 (.91)	214
ANOVA *F*	4.98**[a]	4.39*	
Duration person-centered crime			
Once	1.47 (.73)	1.35 (.62)	172
<1 month	1.71 (.86)	1.38 (.75)	99
1–6 months	1.82 (.99)	1.52 (.77)	66
>6 months	1.83 (1.04)	1.72 (.86)	46
ANOVA *F*	4.21**[a]	2.84*[a]	

[a]Welch test; [b]Equal variances not assumed.
*$p < .05$; **$p < .01$.

Hypothesis 2. To determine whether victims who live alone experience more psychological impact from cybercrime compared to those who do not live alone, we conducted two *t* tests. The mean impact score on emotional well-being for people living alone (M = 1.54; SD = .79) was significantly higher than that for people not living alone (M = 1.45; SD = .71): $t(932.33) = 2.51$, $p < .05$ (two-tailed, equal variances not assumed). For sense of security, there was no statistically significant difference between people who live alone and those who do not: $t(2402) = .15$, $p = .89$ (two-tailed, equal variances assumed). Therefore, Hypothesis 2 was confirmed for emotional well-being but rejected for sense of security.

Hypothesis 3. To evaluate if women experience more psychological impact from cybercrime compared to men, two *t* tests were conducted. The mean impact scores on emotional well-being were higher for women (M = 1.51; SD = .76) than for men (M = 1.44; SD = .70): $t(2342.87) = -2.43$, $p < .05$ (two-tailed, equal variances not assumed). No significant differences were found in sense of security for women and men: $t(2413) = -1.92$, $p = .06$ (two-tailed, equal variances assumed). Hypothesis 3 was therefore confirmed for emotional well-being but not for sense of security.

Hypothesis 4. To determine whether the psychological impact of cybercrime decreases with increasing SES, two between-groups ANOVA tests were conducted with employment status and the five income groups. There was no significant interaction effect between income and employment situation for emotional well-being, $F(12, 2296) = .70$, $p = .75$. There was, however, a significant main effect of income group, $F(4, 2296) = 3.98$, $p < .01$. Post hoc comparisons with the Tukey's HSD test showed a lower mean impact score on emotional well-being for income group 5 (the highest income group) (M = 1.36, SD = .63) than for income group 1 (the lowest income group; M = 1.53, SD = .80), 2 (M = 1.50, SD = .76), 3 (M = 1.56, SD = .79) and 4 (M = 1.49, SD = .74). A main effect of employment situation had a *p*-value of .04 and $F(3, 2296) = 2.83$, but it was not deemed significant due to variances in error terms. For sense of security, we found no significant interaction effect of income group and employment situation, $F(12, 2296) = 1.13$, $p = .33$, and no significant main effect of income group, $F(4, 2296) = .22$, $p = .93$. However, there was a significant main effect of employment situation, $F(3, 2296), 4.25$, $p < .01$. Post hoc tests showed that students experienced a lower impact on sense of security (M = 1.57) than those who were employed or self-employed (M = 1.69, SD = .84), unemployed (M = 1.76, SD = .86) or pensioners (M = 1.84, SD = .86). Hypothesis 6 was thus confirmed regarding income for emotional well-being but not for sense of security.

Hypothesis 5. To evaluate whether the psychological impact scores for victims from ethnic minorities were higher than those for ethnic majorities, we conducted one-way ANOVA tests. There were no significant differences between the groups in emotional well-being: $F(2, 2414) = .99$, $p = .37$; or sense of security: $F(2, 2414) = .35$, $p = .71$. Hypothesis 5 was not confirmed.

Hypothesis 6. To determine if religious people experience less psychological impact from cybercrime than non-religious people, we conducted *t* tests. Contrary to our expectations, the mean impact score on emotional well-being for religious people ($M = 1.52$; $SD = .74$) was higher than for non-religious people ($M = 1.45$; $SD = .72$): $t(1995.93) = -2.31$, $p < .05$ (two-tailed, equal variances not assumed). There was no significant difference in the impact on sense of security: $t(2413) = -1.07$, $p = .29$ (two-tailed, equal variances assumed). Hypothesis 6 was therefore not confirmed for either psychological impact scale.

Hypothesis 7. We examined whether it mattered if a victim's device or account was hacked with *t* tests. As expected, victims whose devices were hacked reported a higher impact on emotional well-being ($M = 1.51$; $SD = .82$) compared to those whose e-mail or social media account were hacked ($M = 1.24$; $SD = .53$): $t(53.26) = 2.25$, $p < .05$ (two-tailed, equal variances not assumed). Victims whose devices were hacked also experienced a higher mean impact score on sense of security ($M = 2.06$; $SD = 1.01$) compared to those whose accounts were hacked ($M = 1.76$; $SD = .91$): $t(431) = 2.13$, $p = .03$ (two-tailed, equal variances assumed). Hypothesis 7 was confirmed.

Hypothesis 8. To determine if the consequences of hacking—whether it led to malware infection, misuse of an account or profile page, or no further consequences—affected the psychological impact, we conducted one-way ANOVA tests. A Welch test due to differing variances revealed a statistically significant difference in mean impact on emotional well-being across the three groups: $F(2, 157.64) = 4.98$, $p < .01$. Post hoc comparisons using the Tukey's HSD test showed that victims who experienced a malware infection experienced a significantly higher mean impact on emotional well-being ($M = 1.41$; $SD = .70$) compared to those who experienced no further consequences ($M = 1.17$; $SD = .43$), with $p < .01$. However, there was no significant difference between the malware group and those whose account or profile page was misused ($M = 1.30$; $SD = .64$). Similarly, the ANOVA test showed a significant difference in mean impact on sense of security: $F(2, 407) = 4.39$, $p < .05$. Post hoc comparisons indicated that the mean impact on sense of security was higher for victims who experienced a malware infection ($M = 2.05$; $SD = 1.04$) than for those

who experienced no further consequences (M = 1.72; SD = .91) at the level of p < .05. The mean impact score of hacking victims whose account or profile page was misused (M = 1.93; SD = .94) did not deviate significantly from the other groups. Hypothesis 8 was not confirmed for either emotional well-being or sense of security.

Hypothesis 9. To test whether the psychological impact scores were higher for victims who experienced longer durations of person-centered cybercrime, we conducted two one-way ANOVA tests. A Welch test indicated significant differences in the mean impact scores on emotional well-being for victims for whom the crime was a one-off incident (M = 1.47; SD = .73), took less than a month (M = 1.71; SD = .86), 1–6 months (M = 1.82; SD = .99), and longer than 6 months (M = 1.83; SD = 1.04): $F2$(3, 131.56) = 4.21, p < .01. Post hoc comparisons using the Tukey's HSD test revealed a difference between the first group (once) and the third group (1–6 months) at the level of p < .05. The mean scores of the fourth group were higher, but apparently, the smaller N accounted for non-significant results. For sense of security, a Welch test also revealed differences between the impact scores when the crime took place once (M = 1.35; SD = .62), less than a month (M = 1.38; SD = .75), 1–6 months (M = 1.52; SD = .86) or longer than 6 months (M = 1.72; SD = .86): $F2$(3, 132.89) = 2.84, p < .05. A post hoc Tukey's HSD test revealed a difference between the first group (once) and the fourth group (longer than 6 months) at p < .05. Groups 2 and 3 did not significantly differ from the other groups. Hypothesis 9 was confirmed, since for both sense of security and emotional well-being, the mean impact scores were higher when the crime duration was longer.

To summarize, our study identified several personal and circumstantial factors that are associated with the psychological impact experienced by cybercrime victims. Differences emerged regarding the explanatory factors affecting emotional well-being versus sense of security. Table 4.2 provides an overview of all these results.

Table 4.2. Results summary

	Emotional well-being	Cybercrime-related sense of security
H1: The psychological impact of cybercrime increases with age	FALSE	**TRUE**
H2: People who live alone experience greater psychological impact from cybercrime than people who do not live alone	**TRUE**	FALSE
H3: Women experience more psychological impact from cybercrime than men	**TRUE**	FALSE
H4: The psychological impact of cybercrime decreases with increasing socio-economic status	**TRUE**	FALSE
H5: Ethnic minorities experience more psychological impact from cybercrime than ethnic majorities	FALSE	FALSE
H6: Religious people experience less psychological impact from cybercrime than non-religious people	FALSE (reversed)	FALSE
H7: Hacking victims experience more psychological impact when their devices are hacked than when their accounts are hacked	**TRUE**	**TRUE**
H8: Hacking victims experience more psychological impact when a malware infection took place than when their accounts were misused or nothing noticeable happened	FALSE	FALSE
H9: The psychological impact of person-centered cybercrime increases with the duration of the crime	**TRUE**	**TRUE**

4.7. Conclusion and discussion

This study examined the role of personal and circumstantial factors in explaining the psychological impact of cybercrime on victims.[5] We will give a brief overview of the most important results and relate this to previous research, after which we will go through a theoretical reflection, limitations, and recommendations for future research, as well as practical implications.

4.7.1. Personal factors

The results indicate that age, household situation, gender, SES, and religion are significant in determining the psychological impact of cybercrime. Older individuals experienced a greater impact on their sense of security, likely due to relative unfamiliarity with digital environments (Virtanen, 2017). Living alone increased the impact on

[5] See Appendix 1 for supplementary analyses indicating some variations in results across cybercrime types (hacking, financial, and person-centered).

emotional well-being, confirming the role of social support in mitigating victimization impact (Golladay and Holtfreter, 2017). Women reported higher impact on emotional well-being, a finding consistent with traditional crime literature (Dinisman and Moroz, 2017; Lamet and Wittebrood, 2009; Ten Boom et al., 2008). However, the lack of gender differences in sense of security suggests that cybercrime-specific impact is less tied to emotional reactions, highlighting a distinct type of victim response with possibly less gender differences. Higher SES individuals experienced less impact on emotional well-being, possibly due to greater resources for coping (Agnew, 1985; Brands and Van Wilsem, 2019). However, for sense of security, students were less affected than others, which might be due to their stronger digital skills and familiarity with the Internet. Religious individuals experienced more impact on emotional well-being than non-religious people, potentially due to a disrupted belief in a 'just world' which is more common among religious people (Janoff-Bulman, 1985; Pemberton, 2011). These findings partly support coping theory, which suggests that individuals who might be more vulnerable — due to factors such as age, lower social support, or SES — tend to experience a greater psychological impact following victimization.

4.7.2. Circumstantial factors

The study confirmed that hacking a device led to higher psychological impact than hacking an account. This supports the idea derived from the cyborg theory about deeper personal connections felt to devices than to separate accounts, thus amplifying the sense of violation (Longo, 2018; Van der Wagen and Pieters, 2018). The expected differences between malware infections, account misuse, and no noticeable consequences were not confirmed. Although malware infections had more impact than experiencing no further consequences of a hack, there were no significant differences between malware and account misuse. This does not refute the cyborg theory, as victims may struggle to differentiate between attack types (Bada and Nurse, 2020). Moreover, the reduced impact when no noticeable consequences occurred still suggests that the invasiveness of the attack matters. The duration of victimization of person-centered cybercrime was a significant factor, with longer incidents leading to greater psychological distress. This finding can also be interpreted through the lens of the cyborg theory, from which prolonged digital disruptions can be expected to lead to more severe psychological impact, but also due to the potential absence of a clear beginning or end of the crime (Jahankhani et al., 2014; Van der Wagen and Pieters, 2018).

4.7.3. Theoretical reflection

The democratization of victimization theory is largely unsupported by our findings. According to this theory, victimization risks and their impact would be distributed equally across different groups. However, our results reveal that significant differences in the impact of cybercrime persist between groups, showing that the distribution is not as uniform as the theory would suggest. These differences may be attributed to coping mechanisms, resulting in more vulnerable individuals experiencing greater impact. Regarding circumstantial factors, the cyborg theory was effective in predicting psychological impact, with most hypotheses being supported.

The results also indicate that personal factors are more effective in predicting the impact on emotional well-being compared to cybercrime-related sense of security. This finding highlights that traditional crime research, which informed most of the personal factor hypotheses, seems less effective in predicting cybercrime-specific impact. Emotional well-being may be regarded as a more universal impact type. Age is an exception, as it showed a significant relationship with cybercrime-related sense of security, likely due to older individuals' lower familiarity with technology, leading to a greater impact on their sense of security (Virtanen, 2017). The findings suggest the need for theories specifically tailored to cybercrime for explaining cybercrime-specific impact, as evidenced by the cyborg theory's success in predicting most of the observed effects related to cybercrime-related sense of security.

Reflecting on the theories used, it is notable that both the democratization of victimization and the cyborg theory connect with another cyber-theoretical concept: the online disinhibition effect (Suler, 2004). The democratization of victimization parallels the online disinhibition effect's idea of status minimization, where everyone starts from an equal footing online (Agustina, 2015; Suler, 2004). The cyborg theory aligns with the concept of dissociative imagination, where online and offline lives blur. The online disinhibition effect can help explain both perpetrator behavior and victim responses (Agustina, 2015; Bada and Nurse, 2020). Future research should explore other facets of this, such as the asynchronicity between perpetrators and victims. This would facilitate the explicit testing of these potentially relevant theories to better explain the impact of cybercrime on victims.

4.7.4. Limitations and future research

This study has several limitations, which also inform our recommendations for future research. First, we only examined a few circumstantial factors, specifically related to hacking and certain person-centered cybercrimes. Future studies should

include a broader range of factors (such as the time and effort spent on incidents and the further consequences for affected devices) and cover more cybercrime types. Second, exploring additional personal factors, such as personality traits and life events, could provide deeper insights. Third, broader theory testing should be a priority in future research. While the theories we used helped guide hypothesis formulation and result interpretation, we did not fully test these theories. Future studies could focus on testing the online disinhibition effect and the cyborg theory. Fourth, using a secondary dataset has several limitations, such as the exclusion of certain relevant concepts and crime types (Borwell et al., 2021), as well as potential over- or under-representation. The latter means that specific crime types—in this study, consumer fraud within financial cybercrime and threat within person-centered cybercrime—may dominate the results for these broader categories, potentially influencing the overall findings for these groups. Furthermore, the sample sizes might not always have been sufficient when comparing different groups for different types of cybercrime, thus the findings should be interpreted with some caution. Sixth, the data was collected in 2018, and an update would be beneficial due to the ongoing digitization, the impact of the COVID-19 pandemic, advancements in victim policies, and the rising cybercrime rates. Seventh, we focused on group differences rather than developing a comprehensive model. While this allowed us to explore specific relationships, it did not assess the relative importance of personal and circumstantial factors through regression analysis or test effect sizes. Future research should address these aspects.

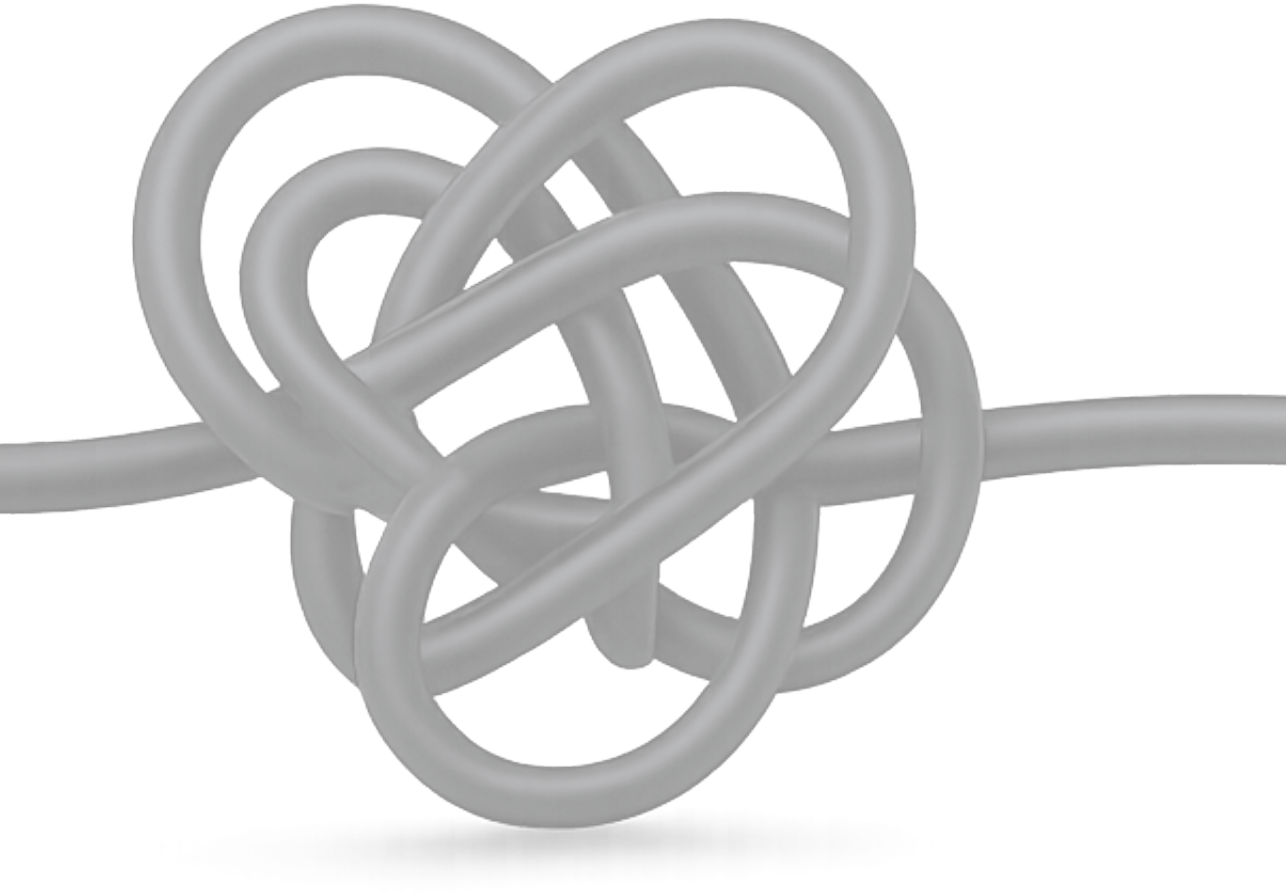
4.7.5. Practical implications

Despite its limitations, this study advances our understanding of the psychological impact of cybercrime on victims by exploring the relationship between personal and circumstantial factors on victim's emotional well-being and cybercrime-related sense of security. The study's alignment with theoretical frameworks and its exploration of various cybercrime aspects contribute to the field's knowledge. Moreover, it offers practical insights about the need for tailored interventions and support measures for different victim groups. First, the study shows that the psychological impact of cybercrime, particularly on emotional well-being, varies according to personal factors. Prevention and support measures could be more effective if they target potential and actual victims with specific characteristics. For example, prevention campaigns and support services should be directed toward individuals living alone (and/or lacking social support systems), women, and those with lower SES, offering them additional emotional support and resources when they report a crime. Second, mitigating the

psychological impact of cybercrime also requires addressing circumstantial factors. Efforts should focus on preventing more invasive types of cybercrime, such as hacking entire devices and reducing the duration of victimization. These practical measures are crucial for organizations involved in dealing with cybercrime victims, including the police, local governments, internet service providers, victim support agencies, and banks. These entities must collaborate to adequately support victims, prevent victimization among vulnerable groups, and combat cybercrime. For instance, early notification of account misuse by service providers can help minimize the potential damage to victims (Jhaveri et al., 2017).

4.7.6. Closing remarks

This study explored how personal and circumstantial factors influence the psychological impact of cybercrime victimization. Our findings challenge the democratization of victimization theory, which suggests that victimization risks and impacts would be evenly distributed across various groups. Instead, we observed significant variations in impact among different groups, which can be partially explained by coping mechanisms and cyborg theory. Future research could build on this foundation with a broader theoretical framework and focus on establishing causality. Expanding this research to include other European countries would enhance the generalizability of the findings across the European context. The relevance of this study has only increased since the data collection by Statistics Netherlands in 2018, as more aspects of our lives have shifted online. Follow-up research should aim to address the limitations identified in this study and further investigate the factors that shape the psychological impact of cybercrime. This study provides a starting point for such efforts.



Chapter 5

Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors

Jildau Borwell, Jurjen Jansen, Wouter Stol

Originally published in International Review of Victimology 2025, 31(1), 156-181.

5.1. Introduction

5.1.1. Background

The societal consequences of digitization have emerged as a popular academic topic in recent years. Cybercrime is one of the most recognized negative consequences (Button et al., 2020; Domenie et al., 2013; Reep-Van den Bergh & Junger, 2018; Wall, 2005). In the Netherlands, cybercrime victimization rates stood at 16% in 2023, which is probably an underestimation (Akkermans et al., 2024). With technology advancing rapidly, cybercrime victimization rates are not expected to decline (Palassis et al., 2021). However, our understanding of the impact on cybercrime victims remains incomplete (Button et al., 2021b). Furthermore, a comprehensive comparative analysis of the impact of cybercrime and traditional crime is lacking (Borwell et al., 2021a). Given the unique nature of cybercrimes, closer examinations and comparisons are warranted.

Since the 1970s/1980s, there has been a notable shift toward recognizing victims alongside offenders, prompting criminal justice reforms and increased support by victim assistance organizations (Janssen et al., 2021; Van der Vijver, 1993). This shift has fueled scholarly interest in understanding victims' challenges (Janssen et al., 2021). However, understanding these challenges is a complex and ongoing process, particularly in the area of cybercrime where research remains limited. The unique characteristics of cybercrime, including its technological nature, intangibility, large scale, remoteness, permanence, anonymity, and global reach (Agustina, 2015; Gini et al., 2018; Leukfeldt et al., 2018; Moitra, 2005; Nadim & Fladmoe, 2021; Stol, 2022; Wall, 2005; Walrave & Van de Heyning, 2022), introduce new dimensions to victim experiences, necessitating further investigation. Comprehensive understanding of these experiences is essential for developing effective victim policies and support in our digitized society (Li et al., 2019).

Decades of research on the impact of traditional crime such as robbery, assault, and burglary has provided insights into the physical, psychological, financial, and behavioral consequences experienced by victims (Bonanno et al., 2011; Janssen et al., 2021; Lamet & Wittebrood, 2009; Mumtaz, 2019; Palassis et al., 2021; Shapland & Hall, 2007). Our understanding of the impact of cybercrime is comparatively limited (Jansen & Leukfeldt, 2018; Leukfeldt et al., 2018; Li et al., 2019; Reep-Van den Bergh & Junger, 2018), despite its potential for severe harm. Prior studies indicate parallels between cybercrime and traditional victim impact, including financial consequences, serious psychological damage and health implications (Button et al., 2020, 2021a; De Kimpe et al., 2020; Kerr et al., 2013; Leukfeldt et al., 2018; Notté et al., 2021;

Palassis et al., 2021). Victims might experience feelings of violation when their digital space is invaded (Agustina, 2015; Kerr et al., 2013; Van der Wagen & Pieters, 2018). Social disapproval and a lack of recognition from their social environment and law enforcement agencies (victim blaming or secondary victimization) might exacerbate the impact of cybercrime on victims (Leukfeldt et al., 2018). Yet, although questions about the comparative impact of cybercrime and traditional crime have been raised (Button et al., 2022; Kerr et al., 2013), research in this area is lacking (Borwell et al., 2021a).

In addition to the existing research gap, the significance of the social, behavioral, and psychological impact of cybercrime on individual victims is often underestimated or overlooked (Bada & Nurse, 2020; (Button et al., 2021a); De Kimpe et al., 2020; Henson et al., 2016; Li et al., 2019; Reep-Van den Bergh & Junger, 2018). Serious offenses should receive higher priority and allocated resources within law enforcement compared to less serious offenses, thus it is important to assess the severity of relatively new crime forms (Button et al., 2022; Domenie et al., 2013). Until now, cybercrime has received limited attention, resources, and priority within law enforcement (Button et al., 2022). Crimes without physical interaction, such as cybercrime, are often perceived as less significant (Button et al., 2021a; Dinisman & Moroz, 2017; Golladay & Holtfreter, 2017; Henson et al., 2016; Jansen & Leukfeldt, 2018; Kerr et al., 2013). To clarify the validity of these notions and to address the academic knowledge gap, our main goal is comparing the impact of cybercrime and traditional crime. In addition, we aim to identify factors explaining victim impact and compare their relevance between cybercrime and traditional crimes. While prior research on traditional crime shows that causal mechanisms for victim impact apply across crime types (Golladay & Holtfreter, 2017), their applicability to cybercrime remains largely unexplored.

The comparison of victim impact between cybercrime and traditional crime, alongside understanding contributing impact factors, holds significant implications for policymakers and law enforcement. Beyond bridging an academic knowledge gap, we therefore aim to inform strategies to address cybercrime, enhancing support and justice for its victims. We define cybercrime as crime in which information and communication technology (ICT) plays an essential role in the execution of the offense (Domenie et al., 2013), and victim impact as the severity of crime effects perceived by the victim (Dignan, 2005; Groenhuijsen, 1996). Next, we will discuss identified victim impact categories, potential determinants, and research design, including survey development and sample acquisition (910 crime victims).

5.1.2. Categories of victim impact

Drawing on previous research, we distinguished four types of crime impact: psychological/emotional, physical, financial/material, and social/behavioral (Button et al., 2021b; Lamet & Wittebrood, 2009; Mawby & Walklate, 1994; Shapland & Hall, 2007). However, during factor analysis and as outlined in the methodology section, we found a different pattern, resulting in the following dimensions: internalizing problems, externalizing problems, damaged self-image (selfblame and shame), and financial impact. Internalizing and externalizing problems are established concepts in psychopathology, supported by extensive literature (Achenbach et al., 2016). 'Internalizing' pertains to inward-focused problems such as anxiety, depression, social withdrawal and psychosomatic complaints, while 'externalizing' refers to outward-focused problems such as anger, disruptiveness, dishonesty and impulsivity (Achenbach et al., 2016; Budimir et al., 2021; Gini et al., 2018). Although describing victim impact in terms of internalizing and externalizing problems is less common, previous research has used these concepts around victimization of peer aggression or harassment and security breach situations (Budimir et al., 2021; Gini et al., 2018).

5.1.3. Determinants of victim impact

The main objective of this study is to compare the victim impact of cybercrime and traditional crime. However, it is important to acknowledge that individuals respond differently to crime, even in similar situations (Bonanno et al., 2011; Button et al., 2021a; Janoff-Bulman & Frieze, 1983; Jansen & Leukfeldt, 2018; Mawby & Walklate, 1994; Shapland & Hall, 2007). Victim impact is influenced by various other factors than crime type, including crime characteristics, and social, personal, and demographic factors (Janoff-Bulman & Frieze, 1983; Palassis et al., 2021). We aim to explore if these factors have differing relationships with impact depending on the crime type (cyber or traditional crime). In the following section, we will discuss the crime types being compared and other factors potentially influencing victim impact, drawing from previous literature. All mentioned factors are included in our study.

5.2. Crime types

Previous victimization studies often either grouped diverse crime forms or focused narrowly on specific offenses, limiting our understanding of victim impact (De Kimpe et al., 2020; Dinisman & Moroz, 2017; Li et al., 2019; Nieuwenhuizen & Van Huijstee, 2022; Wall, 2005). Leukfeldt et al. (2018) emphasized the importance

of examining specific cybercrimes in detail. Determining which cybercrime and traditional crimes to compare is essential for a fair and comprehensive comparison. Existing studies commonly classify crime into three main categories: property crime, person-centered crime, and violent/sexual crime (see Furnell, 2001; Jansen & Leukfeldt, 2018; Lamet & Wittebrood, 2009). We refined the main classification into: burglary, scam, threat, and violation of physical integrity (see Table 5.1). In addition to encompassing a wide range of offenses, our selection of underlying crime pairs was influenced by similarities in the methods and motives employed by offenders. We consulted experts to assess the meaningfulness and feasibility of various comparisons, and we took into account the prevalence of these crime types, drawing from information in police databases and the latest Dutch victims statistics at the time of data collection (Akkermans et al., 2022).

Table 5.1. Categorization of included offense types

Category	Subcategory	Traditional crime	Cybercrime
Property crime	*Burglary*	Residential burglary	Hacking of online bank account
	Scam	Doorstep deception	Bank helpdesk fraud
Person-centered crime	*Threat*	Offline threat	Online threat
Violent/sexual crime	*Violation of physical integrity*	Sexual assault	Image-based sexual abuse

For traditional crime, the specific offenses that we distinguish are: (1) residential burglary (theft inside a home, by someone who is there without the knowledge or against the will of the entitled party); (2) doorstep deception (also referred to as confidence scams—using an excuse, distracting or lying with the aim of committing theft from a home or elsewhere—'doorstep' should not be interpreted literally); (3) offline threat (face-to-face threat of murder, rape, openly committing violence against persons or property, aggravated assault, hostage-taking, or arson); and (4) sexual assault (forcing someone to commit or tolerate sexual or sexually oriented acts). For cybercrime, the offenses, respectively, consist of (1) hacking of online bank accounts (logging into a victim's digital banking environment to transfer money, usually preceded by phishing); (2) bank helpdesk fraud (impersonating a bank or the government to convince victims that their money should be transferred to a 'safe' bank account); (3) online threat (online threat of murder, rape, openly committing violence against persons or property, aggravated assault, hostage-taking, or arson); and (4) image-based sexual abuse (the unwanted online dissemination and/or creation

of sexual imagery, mainly encompassing (a) sextortion—the demand for money or additional explicit images to avert dissemination of the images; (b) escalated/unwanted sexting—the involuntary dissemination of previously consensually shared images; and (c) revenge porn—the non-consensual sharing of sexual imagery, driven by motives such as revenge, defamation, or libel.

In the following sections, we will explore the factors that might influence victim impact beyond crime type, namely, (1) crime characteristics, (2) social factors, personal factors, and (3) demographics. Our classification is based on a comprehensive analysis of the existing literature on contributors to victim impact, encompassing both cyber and traditional crime domains. The factors under consideration hold significance in both domains, ensuring their potential applicability to the discerned crime types.

5.2.1. Crime characteristics

Victimization moment. While recovery timelines differ, most crime victims either experience minimal disruptions or return to baseline functioning within 1 or 2 years (Bonanno et al., 2011; Kunst & Koster, 2016; Lamet & Wittebrood, 2009). It is important to distinguish peritraumatic stress, which encompasses specific reactions during and immediately after the crime, from other aspects of victim impact (Kunst & Koster, 2016). According to Frieze et al. (1987), individuals go through three stages: immediate (hours to days), medium-term (3 to 8 months), and successful coping. Lamet & Wittebrood (2009) also identify short-term (up to 3 months), medium-term (3 to 12 months), and long-term (12 or more months) phases.

Crime duration. Prolonged victimization can heighten victim impact (Lamet & Wittebrood, 2009), due to longer exposure and factors such as increasing financial losses and ongoing contact with the offender (Leukfeldt et al., 2018), significantly affecting psychological well-being (Gini et al., 2018).

Financial damage. Beyond its financial consequences, financial damage can also have emotional and social impact (Lamet & Wittebrood, 2009), resulting in effects such as anxiety, isolation, stress, and depression (Bada & Nurse, 2020; Kerr et al., 2013).

Damage compensation. Obviously, damage compensation can lead to less financial impact of a crime (Borwell et al., 2021b; Dinisman & Moroz, 2017), facilitating recovery, while insufficient compensation can hinder this process (Button et al., 2021b; Kerr et al., 2013). Symbolically, compensation acknowledges the crime and the victim's experience, potentially restoring their sense of justice (Pemberton, 2011; Van der Vijver, 1993).

Known offender. Victim–offender relationships can affect crime impact (Lamet & Wittebrood, 2009). Offenses by acquaintances may result in heightened impact due to breached trust, dependency, and potential for recurrence (Agnew, 1985; Borwell et al., 2021b; Janoff-Bulman, 1985; Lamet & Wittebrood, 2009; Mawby & Walklate, 1994).

Misleading offender. Victims of crimes involving misleading behavior by offenders tend to experience heightened impact, including feelings of guilt, shame, and self-blame (Button et al., 2020; Notté et al., 2021). Victims may perceive themselves as responsible for their victimization, potentially intensifying the negative effects (Agnew, 1985; Burgard & Schlembach, 2013; Notté et al., 2021).

Avoidance possibility. The belief that a crime could have been avoided affects how victims cope (Janoff-Bulman, 1985). Restoring a sense of agency is vital for emotional recovery (Kunst & Koster, 2016). The knowledge that the crime could have been avoided may enhance their perceived ability to take preventive measures in the future, potentially facilitating their overall recovery (De Kimpe et al., 2020; Janoff-Bulman, 1985). However, similar to cases involving misleading offenders, it can also trigger shame and self-blame (Button et al., 2020; Notté et al., 2021).

5.2.2. Social factors

Support/understanding. Positive social support from partners, friends, and family aids victim recovery (Bonanno et al., 2011; Cross, 2015; Golladay & Holtfreter, 2017; Janoff-Bulman, 1985; Leukfeldt et al., 2018; Mumtaz, 2019; Notté et al., 2021; Whitty & Buchanan, 2016). Conversely, avoidance, distancing, and negative reactions can worsen impact, amplifying feelings of isolation and shame (Kerr et al., 2013; Pemberton, 2012).

Victim blaming. Victim blaming, often observed in crime cases, can exacerbate the impact of victimization and hinders recovery (Cross, 2015; Janoff-Bulman, 1985; Leukfeldt et al., 2018; Pemberton, 2011). It can lead to 'secondary victimization', causing distress beyond the experienced crime (Janoff-Bulman, 1985).

5.2.3. Personal factors

Neutralization/denial. Denial of the crime, considered a neutralization technique, can affect victim impact (Li et al., 2019). While denying reality may hinder emotional processing and prolong negative effects (Li et al., 2019), it can also serve as a defense mechanism for victims to distance themselves from the incident and its consequences (De Kimpe et al., 2020; Van der Vijver, 1993).

Self-efficacy. Crime victimization can undermine one's sense of agency, leading to psychological challenges (Kunst & Koster, 2016; Moore, 2016). Self-efficacy, defined as an individual's belief in their own abilities (Ajzen, 2002; Benight & Bandura, 2004), plays a crucial role. Perceived control over post-victimization challenges can alleviate stress by fostering a perception of reduced threat in the outside world (Benight & Bandura, 2004).

Psychological problems. Pre-existing psychological issues may amplify the negative consequences of crime victimization and hinder the process of recovery (Dinisman & Moroz, 2017; Maercker & Horn, 2012).

Repeat victim. Previous victimization can amplify the impact of subsequent incidents (Shapland & Hall, 2007). This 'cumulative dose' of victimization may induce trauma symptoms (Hamby et al., 2018; Van der Vijver, 1993), yet individuals with prior negative experiences may also develop coping mechanisms (Agnew, 1985).

5.2.4. Demographics

Demographic factors such as age, gender, and socioeconomic status (SES) can influence victimization experiences (Janssen et al., 2021; Mumtaz, 2019). Lower SES is associated with higher victim impact, possibly due to limited coping resources (Agnew, 1985; Borwell et al., 2021b; Brands & Van Wilsem, 2019; Lamet & Wittebrood, 2009). Women generally experience more serious emotional problems after victimization than men (Bonanno et al., 2011; Dinisman & Moroz, 2017; Lamet & Wittebrood, 2009; Mawby & Walklate, 1994; Rosoff et al., 2014). The effect of age varies across studies (Bonanno et al., 2011; Cross, 2015; Golladay & Holtfreter, 2017; Lamet & Wittebrood, 2009; Mawby & Walklate, 1994).

5.3. Materials and methods

5.3.1. Ethical considerations

The procedure of this study was approved by the Ethical Research Board of the Open University of the Netherlands (cETO)[6] and by the Netherlands Public Prosecution Service (PaG).[7]

[6] Reference U20220.086.
[7] Reference PaG/BJZ/56421.

5.3.2. Victim selection

Our study included victims of the discerned crime types who reported to the Dutch police and experienced victimization up to 3; 6 to 9; or 12 to 15 months ago, allowing us to consider time of victimization as an explanatory variable. The chosen time periods align with existing literature that identifies different phases of victim impact, as outlined in our description of crime characteristics in Section 5.2.1. The shortest distinguished time of hours to days (Frieze et al., 1987), and peritraumatic stress during the offense (Kunst & Koster, 2016), cannot be obtained from our survey design. We addressed this issue by asking victims about their experiences at the time.

To select victims of the discerned offense types, we utilized police categorization, and queries. We excluded 'hybrid' crime forms with physical and online aspects, such as bank helpdesk fraud involving house visits. A detailed description is available in the first section of Appendix 2. The first author reviewed the reports and assessed their conformity to the criteria, definition, and operationalization specific to each offense. Reports of the offenses were randomly ordered and reviewed to ensure they corresponded to the intended offense until the desired number of reports was reached. Individuals were excluded if they did not have a Citizen Service Number, reported on behalf of someone else, were not the direct victim, represented a company, were under 18, were non-Dutch speakers, or resided abroad. In the main category 'violation of physical integrity', individuals without a registered phone number were excluded.

5.3.3. Data collection

To ensure an adequate sample size, 167 victims were selected for each offense type within the discerned time groups. This was based on an expected minimum response rate of 20%, discerned from similar methods (Borwell et al., 2018). Invitation letters and emails adhered to the Dutch police's house style and were signed by the portfolio holder of Victim Care. We used survey software 'Questback', which is commonly employed by the Dutch Police.[8] A total of 3,006 invitation letters were sent between 7 June 2022 and 11 August 2022. From returned letters, we assume that at least 24 victims did not receive the invitation. Each respondent received a reminder letter after 1.5 weeks. For the violation of physical integrity category, 1,002 victims were contacted by telephone to request permission to send an invitation email. This approach was chosen to address the sensitivity of these offenses. Phone calls and subsequent email invitations were conducted between 5 October 2022 and 30 January 2023. Of those victims, 791 were successfully reached (392 for sexual assault, 399 for image-based sexual abuse), and 648

[8] The full survey text is provided in Appendix 3.

victims agreed to receive the invitation email (332 for sexual assault, 316 for image-based sexual abuse). A detailed description of the procedure is available in Appendix 2.

5.3.4. Response

The total response rate from victims reached through letters or telephone contact was 24.7% (933 respondents). We deleted cases in which respondents failed our screening questions: they indicated that they had not experienced the specific offense in the intended time frame (6 cases), or they did not file a police report for themselves (8 cases), resulting in 919 respondents. Furthermore, we excluded four victims selected for online threat who reported offline threats, two victims who reported being threatened by phone, and two victims selected for offline threat who reported being threatened by phone. One respondent was deleted because of regression assumptions, see below. This resulted in a remaining sample of 910 victims for further analysis.

To assess potential selective non-response, we compared the characteristics of the respondents with the total of selected victims. A complete description is given in Appendix 2. Respondents had a significantly higher approximate mean age compared to the approximate mean age of selected victims, except for the violation of physical integrity crimes. The male proportion did not differ significantly between the respondents and the selected victims, except for offline threat, where the male proportion within the respondents was lower. This suggests that some caution should be exercised when generalizing to the total victim population, while the differences do not seem substantial enough to cause significant issues. Moreover, the values for the total victim population are unknown, since we only selected victims who reported to the police.

5.3.5. Operationalization

To our knowledge, there are no validated surveys to measure experienced victim impact. Therefore, we conducted a comprehensive literature review to identify relevant aspects of impact. We made a distinction between studies focusing on (1) cybercrime (e.g. Button et al., 2020; Kerr et al., 2013; Leukfeldt et al., 2018; Li et al., 2019; Notté et al., 2021), (2) traditional crime (e.g. Dinisman & Moroz, 2017; Kunst, 2010; Norris & Kaniasty, 1991; Van der Vijver, 1993; Vanderstraeten et al., 2012), and (3) studies considered more 'neutral' or 'hybrid' in nature (e.g. Bonanno et al., 2011; Hay & Ray, 2019; Janssen et al., 2021; Lamet & Wittebrood, 2009; Shapland & Hall, 2007). Prominent topics and questions aligning with our study objectives were selected and adapted from this review. In this section, we discuss the operationalizations used to measure impact, crime characteristics, and personal, social, and demographic factors.

Impact

Participants rated the current consequences of the crime using a Likert-type scale (1–5) for impact statements. A principal components analysis (PCA) was conducted on 29 impact items, with six double-loading items removed. The final solution, presented in Table 5.2, contains four components: internalizing problems, externalizing problems, financial impact, and damaged self-image. A more detailed description of the PCA and the first four factor solution can be found in Appendix 2. Cronbach's alpha for the four impact dimensions ranged from 0.81 to 0.94. We used five items for peritraumatic stress: shock, denial, despair, helplessness, and physical reactions. A PCA yielded a single factor, explaining 64% of the variance. The scale demonstrated high internal consistency (Cronbach's alpha = 0.85).

Table 5.2. PCA pattern coefficients with Oblimin rotation of final four factor solution

Item	Pattern coefficients				Communalities
	Factor 1	Factor 2	Factor 3	Factor 4	
Concentration difficulties[a]	**0.87**				0.78
Nausea[a]	**0.82**				0.61
Weight change[a]	**0.78**				0.58
Impaired work/study functioning[b]	**0.78**				0.72
Suicidal ideation[a]	**0.77**				0.52
Headache[a]	**0.77**				0.71
Reduced social interaction[b]	**0.72**				0.57
Relationship issues[b]	**0.72**				0.54
Sleep disturbances[a]	**0.67**				0.71
Fear/panic[c]	**0.67**	0.31			0.69
Depression/sadness[c]	**0.65**				0.75
Anger[c]		**0.80**			0.65
Frustration/irritation[c]		**0.77**			0.68
Sense of privacy violation[c]		**0.74**			0.55
Persistent thoughts of the crime[c]		**0.64**			0.65
Applying protective measures[b]		**0.62**			0.35
Desire for retaliation[b]		**0.59**			0.48
Fear of recurrence[c]	0.33	**0.56**			0.53
Financial hardships[d]			**0.88**		0.75
Substantial loss[d]			**0.84**		0.74
Decreased income[d]			**0.84**		0.77
Self-blame[c]				**0.94**	0.86
Feelings of shame[c]				**0.86**	0.84

Note. Items per factor are bolded.
Initial impact classification: [a]physical; [b]social/behavioral; [c]psychological/emotional; [d]financial material.

Crime characteristics

Victimization moment. Respondents were grouped into recent (0–3 months ago) and non-recent (6–9 or 12–15 months ago) victimization categories. This choice was made because impact differences between the two non-recent groups were non-significant (see Appendix 2).

Crime duration. Respondents indicated if the crime was one-off (1) or lasted from less than a week (2) to over a year (7). Due to infrequent longer durations, we categorized crimes as one-off or longer.

Financial damage. Respondents reported direct financial damage on a scale from no damage (1) to over €50,000 (9). Given the extensive range of categories, we treated this variable as continuous.

Damage compensation. Respondents reported whether they requested and received full or partial reimbursement, categorized into fully/mostly compensated or not.

Known offender. Respondents indicated the extent of familiarity with the offender(s), which was categorized into unknown or known.

Misleading offender. Respondents indicated if the offender convinced them to do or not do something (yes/no).

Avoidance possibility. Respondents rated on a scale of 1 to 5 their ability to prevent the offense at the time.

Social factors

Support/understanding. Respondents rated two statements on a scale of 1 to 5: 'I received sufficient support from those around me' and 'My environment understands what I have been through'. Since the Pearson correlation coefficient was sufficiently high ($r = 0.53$), we decided to combine the variables.

Victim blaming. Respondents rated whether the statement 'My environment blames me for the offense' applied to them on a scale of 1 to 5.

Personal factors

Neutralization/denial. Respondents rated whether the statement 'I prefer to pretend the offense did not happen' applied to them on a scale of 1 to 5.

Self-efficacy. Respondents rated the extent to which the statement 'I can deal with the offense and its consequences myself' applied to them on a scale of 1 to 5.

Psychological problems. Respondents rated whether the statement 'I was experiencing psychological problems before the offense took place' applied to them on a scale of 1 to 5.

Repeat victim. Respondents were asked if they had been a victim of the same or another crime within the past 2 years (yes/no).

Demographics

Gender. Respondents indicated their gender identity as male, female, or non-binary, with two respondents identifying as non-binary. Their responses were excluded from gender analysis.

Age. Respondents' ages were calculated by subtracting their year of birth from the survey completion year.

Education level. Respondents' education levels were categorized into low, medium, and high based on 10 options. Analysis, provided in Appendix 2, revealed no significant impact differences for cyber and traditional crime victims with lower or medium education levels. Therefore, we distinguished between those with a high education level and those with a low or medium education level.

5.3.6. Descriptives

Table 5.3 presents descriptive statistics for all variables, including the total sample and separate statistics for victims of traditional crimes and cybercrimes. Although mean centering was used for regression analysis, we display the non-centered variables to facilitate interpretation.

5.3.7. Analyses

SPSS v28 was used for analyses, employing two-sided tests with significance levels of $p < 0.01$ and $p < 0.001$ due to the study's exploratory nature and the relatively high number of respondents. To assess mean impact score differences across crime pairs, *t* tests were conducted. Results led to aggregating all online and all offline crimes for subsequent regression analyses. Linear regression analyses were performed for each predictor. Interaction effects between crime type and predictors were examined to assess differences between traditional and cybercrime. A brief interpretation of the results will be provided in the results section.

Table 5.3. Description of variables included in the analyses (before mean centering)

Variables	*M* total *(SD)*	*M* traditional crime *(SD)*	*M* cybercrime *(SD)*	Min.	Max.	% total	% traditional crime	% cybercrime	*N* traditional crime	*N* cybercrime	*N* total
Internalizing problems (low-high)	0.54 (0.85)	0.62 (0.93)	0.46 (0.77)	0	4				414	496	910
Externalizing problems (low-high)	2.03 (1.10)	2.07 (1.12)	2.00 (1.09)	0	4				414	496	910
Financial impact (low-high)	0.30 (0.73)	0.29 (0.64)	0.31 (0.80)	0	4				414	496	910
Damaged self-image (low-high)	1.59 (1.47)	0.95 (1.27)	2.13 (1.42)	0	4				414	496	910
Peritraumatic stress (low-high)	2.03 (1.23)	1.93 (1.24)	2.12 (1.21)	0	4				414	496	910
Type of traditional crime											413
Residential burglary							31.4%				
Doorstep deception							22.7%				
Offline threat							12.6%				
Sexual assault							33.3%				
Type of cybercrime											496
Hacking of online bank								28.8%			
account								42.7%			
Bank helpdesk fraud								11.3%			
Online threat								17.1%			
Image-based sexual abuse											
Victimization moment									414	496	910
6-9 or 12-15 months ago						64.2%	63.0%	65.1%			
0-3 months ago						35.8%	37.0%	34.9%			
Crime duration									402	486	888
One-off experience						83.2%	91.8%	76.1%			
Not one-off experience						16.8%	8.2%	23.9%			

Table 5.3. ***Continued***

Variables	*M* total *(SD)*	*M* traditional crime *(SD)*	*M* cybercrime *(SD)*	Min.	Max.	% total	% traditional crime	% cybercrime	*N* traditional crime	*N* cybercrime	*N* total
Financial damage (low-high)	2.93 (2.51)	2.36 (2.52)	3.39 (2.40)	0	8				387	484	871
No financial damage						30.8%	42.9%	21.1%			
< €100						4.2%	5.2%	3.5%			
€100 - €500						13.1%	10.3%	15.3%			
€501 - €1.000						9.0%	7.2%	10.3%			
€1.001 - €2.000						9.4%	8.5%	10.1%			
€2.001 - €5.000						13.7%	9.3%	17.1%			
€5.001 - €10.000						10.6%	9.6%	11.4%			
€10.001 - €50.000						7.8%	5.4%	9.7%			
> €50.000						1.5%	1.6%	1.4%			
Damage compensated									179	357	536
Not fully or mostly compensated						33.2%	54.7%	22.4%			
Fully or mostly compensated						66.8%	45.3%	77.6%			
Known offender									373	487	860
No						82.8%	75.9%	88.1%			
Yes						17.2%	24.1%	11.9%			
Misleading offender									414	496	910
No						41.9%	72.0%	16.7%			
Yes						58.1%	28.0%	83.3%			
Avoidance possibility (low-high)	1.82 (1.66)	1.09 (1.41)	2.44 (1.60)	0	4				414	496	910
Support/understanding (low-high)	3.06 (1.07)	3.13 (1.03)	3.00 (1.10)	0	4				414	496	910
Victim blaming (low-high)	0.41 (0.92)	0.26 (0.75)	0.54 (1.02)	0	4				414	496	910
Neutralization/denial (low-high)	1.26 (1.47)	1.11 (1.41)	1.38 (1.51)	0	4				414	496	910
Self-efficacy (low-high)	1.87 (1.53)	1.79 (1.53)	1.94 (1.54)	0	4				414	496	910
Psychological problems (low-high)	0.44 (1.07)	0.53 (1.13)	0.36 (1.00)	0	4				414	496	910

Table 5.3 continues on next page.

Table 5.3. ***Continued***

Variables	*M* total *(SD)*	*M* traditional crime *(SD)*	*M* cybercrime *(SD)*	Min.	Max.	% total	% traditional crime	% cybercrime	*N* traditional crime	*N* cybercrime	*N* total
Repeat victim									402	474	876
No						79.7%	79.6%	79.7%			
Yes						20.3%	20.4%	20.3%			
Gender									411	495	906
Male						45.8%	32.4%	57.0%			
Female						54.2%	67.6%	43.0%			
Age	55.93 (21.08)	52.82 (23.25)	58.53 (18.70)	18	92				409	491	900
Education level									403	485	888
Low or medium						61.4%	53.3%	68.0%			
High						38.6%	46.7%	32.0%			

SD: standard deviation.

$^{*}p < .01$; $^{**}p < .001$ (two-sided).

[a]Scale 0 to 4; [b]Equal variances not assumed.

5.4. Results

5.4.1. Impact comparisons of crime pairs

Table 5.4 presents the results of the *t* tests comparing the mean impact scores of the four crime pairs. In this section, we focus on reporting the significant findings ($p < 0.01$). Regarding internalizing and externalizing problems, there were no statistically significant differences between the cyber and traditional variants of crime. This indicates that the impact on internalizing and externalizing problems, which may be referred to as psychological, behavioral/social, and psychosomatic impact in other studies, is comparable for both cybercrime and traditional crime, in line with prior studies (Bluhm et al., 2022; Button et al., 2020, 2021a; Gini et al., 2018; Kerr et al., 2013; Leukfeldt et al., 2018; Notté et al., 2021; Palassis et al., 2021).

Experienced financial impact was higher for residential burglary victims compared to hacking of online bank account victims, while no significant differences were found among other crime pairs. When evaluating the impact on victims' self-image, cybercrime variants generally resulted in greater damage, except for the threat category where no significant difference was observed. Specifically, damage to self-image was higher for hacking of online bank accounts than for residential burglary; higher for bank helpdesk fraud than for doorstep deception; and higher for image-based sexual abuse than for sexual assault. These findings align with prior research suggesting that cybercrime victims often feel responsible for their victimization, experiencing feelings of embarrassment, shame, and self-blame (Button et al., 2020; Kerr et al., 2013; Notté et al., 2021). While victim blaming and self-blame are also relevant in cases of sexual assault, burglary, and doorstep deception (Agnew, 1985; Littleton, 2010; Notté et al., 2021; Vanderstraeten et al., 2012), damaged self-image was more prominent in the cybercrime variants. The absence of a significant effect in the threat category may be related to misleading tactics not commonly being employed.

Our findings reveal higher peritraumatic stress for hacking of online bank accounts compared to residential burglary, and bank helpdesk fraud compared to doorstep deception. Symptoms of acute stress, such as panic, trembling, and severe shock are commonly associated with the discovery of a residential burglary (Dinisman & Moroz, 2017; Vanderstraeten et al., 2012). Our findings suggest that the peritraumatic stress experienced for hacking of online bank accounts was even higher. The stress in cyber property crimes may stem from the technical complexities of the digital environment, creating uncertainty about appropriate actions and ongoing threats from invisible intruders (Stol, 2022). Interestingly, no significant differences were found in the threat and violation of physical integrity categories between cyber

Table 5.4. T tests of differences in mean impact for four crime pairs

	Burglary		Scam		Threat		Violation of physical integrity	
	Residential burglary (*N* = 130)	Hacking of online bank account (*N* = 143)	Doorstep deception (*N* = 94)	Bank helpdesk fraud (*N* = 212)	Offline threat (*N* = 52)	Online threat (*N* = 56)	Sexual assault (*N* = 138)	Image-based sexual abuse (*N* = 85)
Dependent variables[1]	*M (SD)*	*M (SD)*	*M (SD)*	*M (SD)*	*M (SD)*	*M (SD)*	*M (SD)*	*M (SD)*
Internalizing problems	0.34 (0.62)	0.22 (0.59)	0.24 (0.49)	0.34 (0.56)	1.12 (1.25)	1.00 (1.20)	0.97 (1.04)	0.80 (0.88)
t	1.54		-1.60[2]		0.50		1.31[2]	
p	.124		.111		.620		.191	
Externalizing problems	1.90 (1.08)	1.68 (1.07)	1.94 (1.03)	2.15 (1.04)	2.12 (1.39)	1.94 (1.19)	2.30 (1.06)	2.18 (1.06)
t	1.68		-1.67		0.70		0.81	
p	.094		.096		.486		.419	
Financial impact	0.34 (0.66)	0.14 (0.55)	.29 (.56)	0.33 (0.83)	0.40 (0.90)	0.55 (1.01)	0.19 (0.55)	0.40 (0.86)
t	2.76[2]		-0.44		-0.81		-2.04[2]	
p	.006*		.660		.419		.043	
Damaged self-image	0.26 (0.56)	1.77 (1.28)	1.64 (1.37)	2.59 (1.24)	0.26 (0.68)	0.61 (1.16)	1.40 (1.40)	2.59 (1.34)
t	-12.77[2]		-5.98		-1.92[2]		-6.30	
p	<.001**		<.001**		.059		<.001**	
Peritraumatic stress	1.31 (1.20)	1.72 (1.24)	1.81 (1.20)	2.30 (1.13)	2.32 (1.35)	1.81 (1.39)	2.44 (0.98)	2.55 (0.99)
t	-2.79		-3.41		1.89		-0.81	
p	.006*		<.001**		.061		.420	

SD: standard deviation.

*$p < .01$; ** $p < .001$ (two-sided).

[a]Scale 0 to 4; [b]Equal variances not assumed.

and traditional variants, while offenses with a physical component and direct contact between victim and offender are often considered more impactful than cybercrimes (Button et al., 2021a; Dinisman & Moroz, 2017; Golladay & Holtfreter, 2017; Henson et al., 2016; Jansen & Leukfeldt, 2018).

5.4.2. Explanatory factors for victim impact

Based on the consistent patterns in the impact comparisons between the crime pairs, where there were no significant differences or differences in the same direction, we decided to aggregate all the cybercrime and traditional crime variants. This allowed us to identify the determinants of overall victim impact and examine potential differences between cyber and traditional crime. We excluded peritraumatic stress as a dependent variable. Mean centering was applied to continuous variables in the regression analysis. Despite some deviation from normality in the dependent variables, this was deemed acceptable due to the large sample size (over 200 cases; see Tabachnick et al., 2013). We found no evidence of non-linear relationships. Multicollinearity was assessed using Pearson correlations, showing no significant issues. Some outliers were identified, after which one case was removed. Others were retained after careful examination.

Table 5.5 presents the relationship between all independent variables and the four impact variables. Separate models were used to explore the effects and potential differences for cyber and traditional crime. A distinct model was used to examine the effect of crime type (cybercrime or traditional crime). Subsequently, for each independent variable, three models per impact type were used to assess the main effects and potential interactions. Model 1 included crime type; Model 2 included the main effect of an additional independent variable, while Model 3 examined the interaction effect between crime type and the other independent variable. This approach was chosen to address the exploratory nature of this study, focusing on understanding the main effects of the independent variables and their potential differences between cybercrime and traditional crime. Due to the large amount of results, we predominantly discuss the significant effects.

Crime types and characteristics. As we expected from the *t* tests, cybercrime victims experienced higher damage to self-image than traditional crime victims, explaining 16% of the variance in the impact variable. Contrary to our expectations based on the *t* tests, cybercrime victims reported lower levels of internalizing problems compared to traditional crime victims. The effect size wassmall. In the models where the main effect of another independent variable was added, the significant effect of crime type disappeared for 9 out of 16 independent variables.

Table 5.5. Linear regression analyses for predicting four impact types: main effects and interactions

	Dependent variables															
	Internalizing problems				Externalizing problems				Financial impact				Damaged self-image			
Independent variables (*N* sample[a])	*b*	*F* change	*p*	R^2 (adj)	*b*	*F* change	*p*	R^2 (adj)	*b*	*F* change	*p*	R^2 (adj)	*b*	*F* change	*p*	R^2 (adj)
Crime type (cybercrime) (910)	-.16	8.47	.004*	.01	-.07	0.96	.327	.00	.03	0.27	.605	.00	1.18	170.88	<.001**	.16
Victimization moment (recent) (910)	.24	16.48	<.001**	.03	.38	26.10	<.001**	.03	.24	23.69	<.001**	.02	.25	7.43	.007*	.16
Crime type x victimization moment	-.03	0.07	.796	.02	.01	0.00	.972	.03	.12	1.32	.251	.02	.22	1.40	.237	.16
Crime duration (not one-off) (888)	.73	96.50	<.001**	.11	.32	10.19	.001*	.01	.27	16.67	<.001**	.02	-.10	0.65	.422	.16
Crime type x crime duration	-.90	28.44	<.001**	.13	-.76	10.82	.001*	.02	-.21	1.92	.166	.02	-.18	0.41	.522	.16
Financial damage (871)	-.01	1.09	.296[b]	.01	.08	25.64	<.001**	.03	.08	62.34	<.001**	.07	.07	14.34	<.001**	.17
Crime type x financial damage	.00	0.01	.930	.01	.04	1.60	.206	.03	-.04	4.76	.029	.07	.22	34.51	<.001**	.20
Damage compensated (fully or mostly) (536)	-.57	51.84	<.001**[b]	.09	-.45	18.47	<.001**	.03	-.76	143.94	<.001**	.21	-.19	2.19	.139	.16
Crime type x damage compensated	-.61	7.36	.007*	.10	.07	0.06	.815	.03	-.56	9.65	.002*	.22	1.29	11.93	<.001**	.18
Known offender (yes) (861)	.84	135.94	<.001**[b]	.14	.31	9.29	.002*	.01	.24	13.20	<.001**	.01	-.21	2.81	.094	.16
Crime type x known offender	-.31	4.29	.039	.15	-.35	2.80	.095	.01	.11	0.63	.426	.01	-0.99	15.15	<.001**	.17
Misleading offender (yes) (910)	-.18	7.15	.008*[b]	.02	.15	2.81	.094	.00	.00	0.00	.974	.00	1.35	181.56	<.001**	.30
Crime type x misleading offender	-.39	7.15	.004*	.02	-.02	0.01	.919	.00	-.28	5.56	.019	.00	.19	0.91	.339	.30
Avoidance possibility (910)	-.09	26.36	<.001**[b]	.04	-.05	3.85	.050	.00	-.04	7.23	.007*	.01	.33	143.44	<.001**	.27
Crime type x avoidance possibility	-.02	0.29	.589	.03	.03	0.31	.576	.00	-.07	4.59	.032	.01	-.04	0.52	.470	.27
Support/understanding (910)	-.13	24.55	<.001**	.03	.03	0.72	.396	.00	-.05	4.69	.031	.00	-.11	6.34	.012	.16
Crime type x support/understanding	.03	0.26	.608	.03	.04	0.32	.574	.00	-.05	0.94	.332	.00	.18	4.62	.032	.17
Victim blaming (910)	.12	15.80	<.001**	.03	.16	15.92	<.001**	.02	.07	6.79	.009*	.01	.35	54.13	<.001**	.20
Crime type x victim blaming	-.06	0.70	.402	.03	.08	0.93	.335	.02	.03	0.26	.608	.01	-.23	5.05	.025	.21

Table 5.5. ***Continued***

	Dependent variables															
	Internalizing problems				Externalizing problems				Financial impact				Damaged self-image			
Independent variables (*N* sample[a])	*b*	*F* change	*p*	R^2 (adj)	*b*	*F* change	*p*	R^2 (adj)	*b*	*F* change	*p*	R^2 (adj)	*b*	*F* change	*p*	R^2 (adj)
Neutralization/denial (910)	.14	57.70	<.001**	.07	.18	53.84	<.001**	.06	.05	9.31	.002*	.01	.33	136.10	<.001**	.27
Crime type x neutralization/denial	-.02	0.39	.531	.07	-.01	0.08	.776	.06	.05	2.17	.141	.01	-.12	4.07	.044	.27
Self-efficacy (910)	-.17	93.96	<.001**[b]	.10	-.24	110.90	<.001**	.11	-.11	47.10	<.001**	.05	-.10	10.62	.001*	.17
Crime type x self-efficacy	.09	6.79	.009*	.11	.08	2.99	.084	.11	-.03	1.01	.314	.05	.04	0.55	.460	.17
Psychological problems (910)	.30	143.80	<.001**[b]	.14	.21	39.55	<.001**	.04	.06	6.98	.008*	.01	.24	33.41	<.001**	.19
Crime type x psychological problems	.01	0.02	.879	.14	.01	0.04	.852	.04	.13	7.63	.006*	.01	-.32	15.26	<.001**	.20
Repeat victim (yes) (876)	.47	45.52	<.001**	.06	.31	10.98	<.001**	.01	.16	7.11	.008*	.01	-.05	0.20	.656	.16
Crime type x repeat victim	-.27	3.58	.059	.06	-.20	1.19	.275	.01	.04	0.12	.725	.01	-.58	6.40	.012	.16
Gender (female) (906)	.19	10.80	.001*[b]	.02	.39	27.22	<.001**	.03	-.04	0.52	.470	.00	.31	11.43	<.001**	.17
Crime type x gender	-.16	1.87	.172	.02	.06	0.14	.709	.03	.22	4.60	.032	.00	-.28	2.19	.140	.17
Age (900)	-.01	62.50	<.001**[b]	.07	.00	0.65	.421	.00	.00	0.06	.815	.00	.00	0.47	.494	.16
Crime type x age	.00	1.38	.240	.07	.00	0.01	.910	.00	-.01	8.53	.004*	.01	.01	10.27	.001*	.17
Education level (high) (888)	-.40	47.21	<.001**	.06	-.55	54.74	<.001**	.06	-.15	8.36	.004*	.01	-.54	34.39	<.001**	.19
Crime type x education level	.19	2.74	.098	.06	-.10	0.42	.518	.06	-.09	0.58	.3445	.01	-.27	2.01	.156	.19
Total of independent variables[c] (excluding interaction terms) (480)		20.43	<.001**	.40		12.86	<.001**	.29		17.52	<.001**	.36		27.84	<.001**	.48

Note. Table contains separate regression analyses, each encompassing three models: (1) main effect crime type; (2) main effect one additional independent variable (value reported in table); (3) interaction effect crime type and additional independent variable (value reported in table).

*$p < .01$; **$p < .001$ (two-sided).

[a]Discrepancies in *N* may arise due to specific response options or questionnaire routing; consult descriptives in Table 5.4 and operationalizations; [b]Crime type not significant in the model where this independent variable was included (not reported for the interaction terms); [c]All independent variables included in a single model.

Victimization moment (recent) had a positive and significant effect on all four dependent variables, suggesting that more recent victimization is associated with higher levels of impact, as we expected. Crime duration (not one-off) had a significant positive effect on internalizing problems, externalizing problems and financial impact. This suggests that individuals who experienced crimes of longer duration tended to report higher levels of these impact types. Notably, there were significant interaction effects between crime type and crime duration for internalizing problems and externalizing problems. Figures A.4.1 and A.4.2 in Appendix 4 show that the effect of crime duration is more pronounced for traditional crime than for cybercrime. It should be noted that 8.2% of traditional crime victims experienced a longer crime duration, whereas 23.9% of cybercrime victims did, as is shown in the descriptives in Table 5.3.

Financial damage significantly influenced externalizing problems, financial impact, and damaged self-image, in line with prior research (Bada & Nurse, 2020; Kerr et al., 2013; Lamet & Wittebrood, 2009). The interaction effect between crime type and financial damage was significant for damaged self-image. Figure A.4.3 in Appendix 4 shows that while cybercrime victims experienced a stronger damaged self-image with increasing financial harm, the impact seemed to slightly decrease for traditional crime victims. Damage compensation negatively affected internalizing problems, externalizing problems, and financial impact, indicating reduced impact for compensated victims, consistent with prior studies (Button et al., 2021b; Dinisman & Moroz, 2017; Kerr et al., 2013; Pemberton, 2012; Van der Vijver, 1993). The interaction effect between crime type and damage compensation was significant for internalizing problems, financial impact, and damaged self-image. Figures A.4.4 and A.4.5 in Appendix 4 illustrate a stronger negative effect of compensation on internalizing problems and financial impact for cybercrime victims, possibly due to higher initial financial damage. However, Figure A.4.6 shows that cybercrime victims who received compensation have a weaker decrease in damaged self-image compared to traditional crime victims.

The presence of a known offender is positively associated with internalizing problems, externalizing problems, and financial impact, consistent with existing research (Janoff-Bulman, 1985). Although the main effect of a known offender was not significant for damaged self-image, a significant interaction effect with crime type was observed. Figure A.4.7 in Appendix 4 shows lower damaged self-image for cybercrime victims when the offender was known, while traditional crime victims experienced slightly more damage. The presence of a misleading offender was negatively linked to internalizing problems but positively to damaged self-image. Appar-

ently, the self-image is more damaged when misleading takes place, aligning with prior research (Agnew, 1985; Burgard & Schlembach, 2013; Button et al., 2020; Notté et al., 2021). The interaction effect between crime type and a misleading offender's presence was significant for internalizing problems. Figure A.4.8 in Appendix 4 shows that cybercrime victims experience reduced internalizing problems when faced with a misleading offender. One possible explanation is that when the misleading involves an offender hiding their identity, it creates a sense of distance or detachment from the offender, leading to reduced impact on internalizing problems.

Higher perceived avoidance possibility is linked to reduced internalizing problems and financial impact but increased damaged self-image. This suggests that individuals who feel they could have avoided the crime experience fewer negative internalizing problems, potentially due to a sense of agency and control over their circumstances, which may serve as a protective factor (Ajzen, 2002; Borwell et al., 2021b). In terms of financial impact, that same sense of agency and control might have engaged people to actively seek support and resources. The positive association between avoidance possibility and damaged self-image can be explained by victims blaming themselves for becoming victimized (Borwell et al., 2021b; Cross, 2015; Kerr et al., 2013).

Social factors. More support and understanding from the victims' environment was negatively related to internalizing problems, potentially due to enhanced coping abilities, as expected from prior research (Cross, 2015; Dinisman & Moroz, 2017; Golladay & Holtfreter, 2017; Kerr et al., 2013; Leukfeldt et al., 2018; Mumtaz, 2019; Whitty & Buchanan, 2016). On the contrary, victim blaming positively influenced all impact types, also aligning with previous studies (Cross, 2015; Janoff-Bulman, 1985; Leukfeldt et al., 2018; Pemberton, 2011). However, the positive association with financial impact was not necessarily expected. It is possible that victims who are blamed for the crime receive less financial support, a form of secondary victimization (Janoff-Bulman, 1985). Another possibility is that financial impact or the absence of financial compensation is interpreted by the victim's surroundings as implying their culpability, thus victim blaming might actually be the result and not the cause of financial impact (Pemberton, 2012). Importantly, victim blaming appears to occur more frequently for cybercrime victims, see the descriptive statistics in Table 5.3.

Personal factors. Neutralization/denial was positively linked to all impact types, suggesting higher impact levels for victims who deny or neutralize the crime, aligning with prior research on maladaptive coping response (Li et al., 2019). However, individuals might resort to neutralization or denial when the crime's impact is substantial and the

crime itself is severe, thereby complicating the exact causal relationship. Conversely, self-efficacy had a negative association with all impact types. Apparently, victims who believe in their ability to handle the offense and its consequences themselves experience less impact, as expected from previous research (Ajzen, 2002; Bada & Nurse, 2020; Benight & Bandura, 2004). The interaction effect between crime type and selfefficacy was significant for internalizing problems. As shown in Figure A.4.9 in Appendix 4, the decrease in internalizing impact with increasing self-efficacy is stronger for traditional crime victims compared to cybercrime victims.

Psychological problems were positively associated with all impact types, indicating higher impact levels for individuals with pre-existing psychological issues. Significant interaction effects between crime type and psychological impact were found for financial impact and damaged self-image, see Figures A.4.10 and A.4.11 in Appendix 4. For cybercrime victims, the financial impact increases with pre-existing psychological problems, while there seems to be no such effect for traditional crime victims. This may be attributed to the relative uncertainty surrounding available help and resources for cybercrime victims (Cross et al., 2016b; Kerr et al., 2013; Stol, 2022). When the route to seek help is unclear, having pre-existing psychological problems might decrease the likelihood of help-seeking, resulting in higher financial impact. On the contrary, for traditional crime victims, there is a clear positive link between pre-existing psychological problems and damage to self-image, whereas no clear relationship is observed for cybercrime victims.

Repeat victimization was positively related to internalizing problems, externalizing problems, and financial impact. This aligns with previous literature indicating that repeat victimization leads to increased psychological impact (Hamby et al., 2018; Van der Vijver, 1993). The relationship between repeat victimization and financial impact seems less obvious and may be attributed to the additional financial burden repeat victims might experience.

Demographics. Gender (female) positively influenced internalizing problems, externalizing problems, and damaged self-image, aligning with prior research on psychological victim impact (Bonanno et al., 2011; Dinisman & Moroz, 2017; Lamet & Wittebrood, 2009; Mawby & Walklate, 1994; Rosoff et al., 2014). Age was negatively associated with internalizing problems, aligning with some earlier research (Bonanno et al., 2011; Rosoff et al., 2014), although contradicting other (Cross, 2015; Golladay & Holtfreter, 2017; Lamet & Wittebrood, 2009; Mawby & Walklate, 1994). Significant interaction effects were found for financial impact and damaged self-image. Figure A.4.12 in Appendix 4 illustrates that financial impact increases with age for

traditional crime victims, while it decreases with age for cybercrime victims. Figure A.4.13 shows that damaged self-image decreases with age for traditional crime victims, while it increases for cybercrime victims. Regarding education, a negative effect was found across all impact types, indicating potentially quicker recovery for higher SES individuals due to better coping skills and navigating resources for assistance (Agnew, 1985; Van Wilsem et al., 2021).

Independent variables combined. Combining independent variables (excluding the interaction terms) into one model, 40% of variance in internalizing problems, 29% in externalizing problems, 36% in financial impact, and 48% in damaged self-image were explained. This suggests that the included factors were meaningful predictors of victim impact, explaining a substantial portion of the variance in the dependent variables.

5.5. Conclusion and discussion

5.5.1. Reflection and implications of the findings

In this study, we compared the victim impact of cyber and traditional variants of burglary, scam, threat and violation of physical integrity. We identified an alternative categorization of impact types, diverging from the more traditional classification of psychological/emotional, physical, financial/material, and social/behavioral impact, encompassing internalizing problems, externalizing problems, financial impact and damaged self-image. Our findings revealed no significant differences between the cyber and traditional crime pairs in terms of internalizing and externalizing problems, suggesting similar emotional, physical, and social impact. However, residential burglary had a higher financial impact compared to hacking of online bank accounts. In addition, cybercrimes caused more damage to self-image, except in the threat category.

Considering peritraumatic stress—the impact during the crime or discovery thereof—online variants of burglary and scams showed higher impact than their traditional counterparts. This may be attributed to the absence of experienced boundaries between people and their devices, intensifying feelings of violation (Agustina, 2015; Kerr et al., 2013; Van der Wagen & Pieters, 2018). Moreover, the characteristics of cybercrime, including its technological complexity and intangibility, may exacerbate peritraumatic stress by complicating victims' ability to comprehend what happened and respond effectively (Agustina, 2015; Gini et al., 2018; Leukfeldt et al., 2018; Moitra, 2005; Nadim & Fladmoe, 2021; Stol, 2022; Wall, 2005; Walrave & Van de Heyning, 2022). Interestingly, there were no significant differences in peritraumatic

stress for threats or physical integrity violations, while physical crimes with direct victim–offender contact are typically deemed more impactful than cybercrimes (Button et al., 2021a; Henson et al., 2016; Jansen & Leukfeldt, 2018).

The impact of cybercrime on individual victims has been overlooked in the past, particularly in terms of its social and psychological consequences (Bada & Nurse, 2020). Our findings highlight the significant impact of cybercrime, which appears to be comparable to or surpassing that of traditional crimes. The damage to the self-image was higher for image-based sexual abuse than for sexual assault, challenging the notion that crimes with physical components are more severe (Button et al., 2021a; Dinisman & Moroz, 2017; Golladay & Holtfreter, 2017; Henson et al., 2016; Jansen & Leukfeldt, 2018; Kerr et al., 2013). Furthermore, the psychological impact of hacking into online bank accounts appears to be similar to and partly more severe than that of residential burglaries, while the latter are often considered among the most impactful crimes (Mawby & Walklate, 1994; Vanderstraeten et al., 2012). For instance, residential burglary is classified as a 'High Impact Crime' by the Dutch police, shaping their priorities (Van Dijk et al., 2021). Based on our findings, not classifying cybercrime as a High-Impact Crime could be reconsidered. In general, practitioners and policymakers should recognize the seriousness of cybercrime, dedicating resources to its investigation, prevention, and providing support to its victims (Button et al., 2021b).

In contrast to the other crime categories, the threat category showed no differences between the cybercrime and traditional variants across impact types. This could be due to the victim's passive role and lower technological complexity associated with online threats (Notté et al., 2021). Consequently, factors such as difficulty in comprehending the crime, limited oversight, and victim blaming seem of lesser importance. For other types of cybercrimes where these factors are more pronounced, it seems crucial to provide practical and reassuring support to assist victims in coping with these challenges. Various entities, including law enforcement agencies, victim support services, insurance companies, private security firms, and the victim's direct social surroundings, could provide such assistance. This might safeguard cybercrime victims from losing their trust in themselves and the digital environment (Kunst & Koster, 2016).

We explored factors influencing victim impact across cyber and traditional crime. Some notable differences between cyber and traditional crime emerged. First, while greater direct financial damage led to a clear increase in damaged self-image for cybercrime victims, this was not true for traditional crime victims. In addition, damage compensation reduced internalizing problems and financial impact more for

cybercrime victims, but had a lesser effect on self-image. Given that not all cybercrime victims receive compensation, establishing a dedicated compensation program could alleviate the negative consequences of victimization and aid in their recovery, as has been suggested before (Borwell et al., 2021b; Piquero, 2018). Second, damaged self-image appeared particularly pronounced among cybercrime victims, and was most strongly associated with misleading by the offender, avoidance possibility, neutralization/denial, and victim blaming. These issues, prevalent among cybercrime victims, underscore the need to place responsibility onto offenders rather than blaming victims (Cross, 2015; Powell et al., 2019). Addressing these challenges requires increased awareness and empathy from family, friends, and law enforcement agencies, to avoid secondary victimization and support victims' recovery process (Agnew, 1985). Professional organizations, including law enforcement agencies, should prioritize efforts aimed at restoring and affirming the self-image of cybercrime victims.

5.5.2. Study limitations

Our study has several limitations. First, our sample consists solely of victims who reported to the police. Previous research indicate relatively low reporting levels of cybercrime (Agustina, 2015; Riek & Böhme, 2018; Van Wilsem et al., 2021). According to the general victim study conducted by Statistics Netherlands, 29% of traditional crime victims filed an official police report, whereas 19% of cybercrime victims did so (Akkermans et al., 2022). However, the reporting rates for specific cybercrimes, such as phishing, are relatively higher, suggesting comparability between traditional and cybercrime reporting. As has been made clear earlier, our respondents also did not perfectly represent the total group of victims we selected. Second, our study focused on specific impact types of specific crimes on individuals, capturing only a portion of the overall societal impact. Thereby, we neglected the potential impact on the victims' surrounding environment and members of the general public who might experience concerns and anxiety due to victimization of others (Mawby & Walklate, 1994). Third, our sample was limited to Dutch-speaking adults from the Netherlands, limiting generalizability to other populations and age groups. Fourth, although we included a broad spectrum of offenses, our study did not cover all forms of crime.

5.5.3. Recommendations for future research

For future research, we recommend further exploration of the impact dimensions uncovered in our study. Internalizing and externalizing problems, particularly, as well as damaged self-image, are often overlooked in crime victimization research, while

they play a significant role in victim experiences (Budimir et al., 2021; Gini et al., 2018). Conducting interviews with victims could provide insights into the processes underlying their experiences. In addition, there is a need for deeper investigation into factors contributing to damaged self-image in cybercrime contexts. Misleading offenders, avoidance possibility, neutralization/denial, and victim blaming contribute most to that damage and appear more prevalent among cybercrime victims, warranting further study.

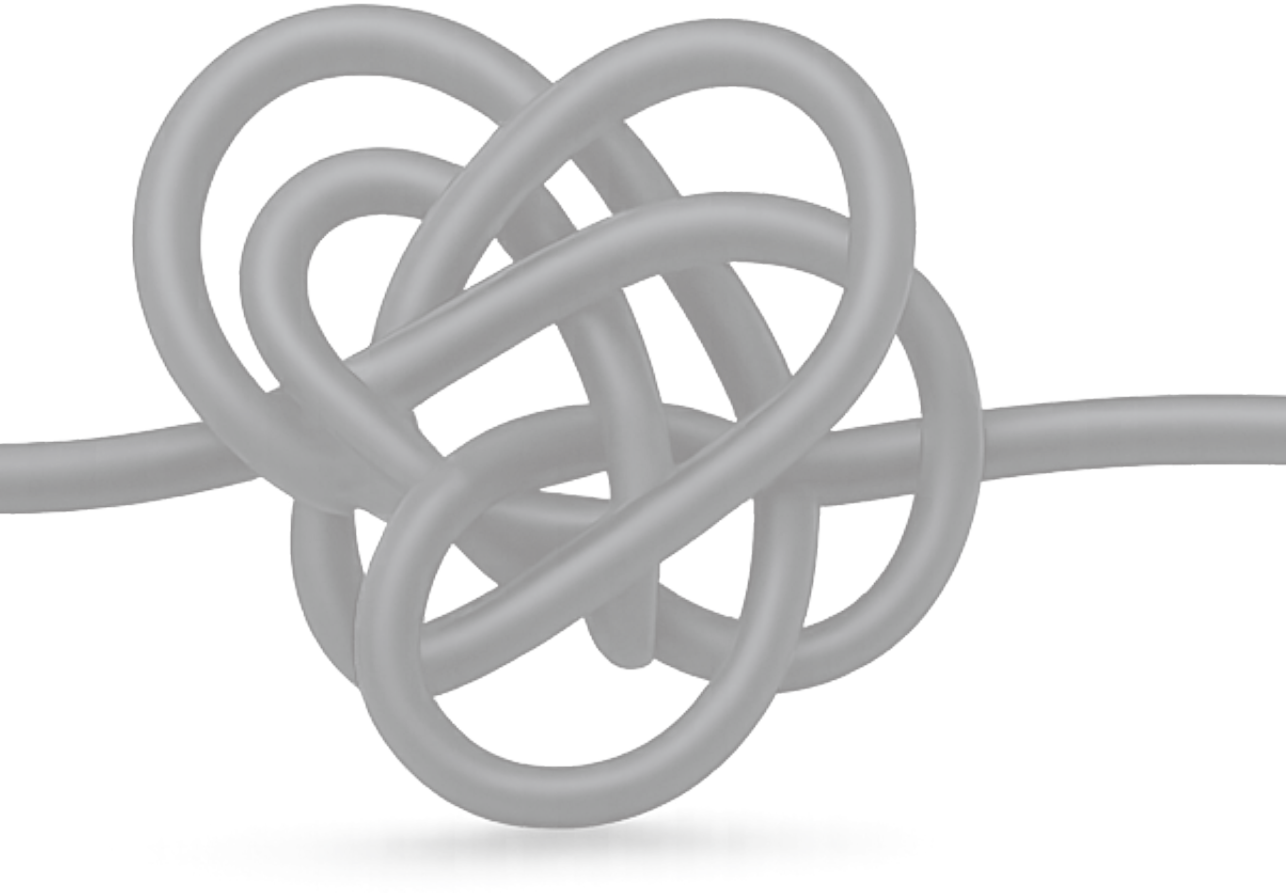
Furthermore, in addition to conducting comparisons, future research should independently assess the severity of impact across different crime types and also take the prevalence of those crimes into account. Crime comparisons offer valuable insights but may limit our understanding of actual victimization experiences and the overall societal impact. Also, explanatory factors specific to different crime types should be studied further, as our study grouped all cybercrimes and traditional crimes with diverse characteristics. For example, previous research showed that burglary victims who have a stronger attachment to their homes are more strongly affected than others (Vanderstraeten et al., 2012). Investigating whether hacking victims with a strong attachment to their devices experience heightened impact could provide valuable insights related to experienced attachment to devices (Agustina, 2015; Borwell et al., 2021a; Van der Wagen & Pieters, 2018).

While our study incorporated respondents victimized at different time points, actual longitudinal studies could significantly enhance the field of research (Brands & Van Wilsem, 2019). Currently, most victimization research relies on cross-sectional data (Janssen et al., 2021), limiting our ability to establish causal relationships (Hay & Ray, 2019). Longitudinal research can reveal nuanced patterns and identify potential long-term consequences, which is particularly relevant since we did not find significant impact differences between individuals victimized 6–9 months ago and those victimized 12–15 months ago. Previous research, for example, has shown that 1 year after a residential burglary, 41% of victims reported post-traumatic stress disorder (PTSD) symptoms (Dinisman & Moroz, 2017). Given that the impact of hacking of online bank accounts appears at least similar, examining the long-term consequences can further inform our understanding of the impact of cybercrime.

5.5.4. Closing statements

The dynamic cybercrime landscape suggests that the crime types we examined may evolve over time (Hamby et al., 2018; Riek, 2017). The reliance on technology is expected to grow even more in the future, and this will have consequences for

new and existing crimes to emerge. With advancements in technologies such as AI and virtual worlds, our engagement with the online world is becoming even more profound, necessitating ongoing research on the impact of cybercrime. Moreover, the growing overlap between cyber and traditional victimization can amplify the impact of crime, as victims may, for instance, experience harassment through multiple channels (Leukfeldt et al., 2018; Notté et al., 2021). Future research should continue to explore the nuanced consequences of cybercrime and expand our understanding of victim experiences, enabling the development of effective strategies to support and protect victims in the digital era.



Chapter 6

Doing justice to the needs of cybercrime victims: Reflections on the role of the police

Jildau Borwell, Jurjen Jansen, Wouter Stol

Originally published in Tijdschrift voor Veiligheid 2024, (23)3, 47-78.[9]

[9] Translated from Dutch for this dissertation.

6.1. Introduction

Digitization presents the police[10] with challenges in carrying out their work. Traditional, physical police work does not easily translate into a digital version (Bijleveld et al., 2021; Landman, 2023). For example, offenders and victims are less visible, and constraints of time and space are blurred (Bijleveld et al., 2021). Despite intensive efforts in this area, the police are still exploring how to perform their work in a digital world. This also applies to how the police engage with victims of online crime. That is what this chapter is about.

Previous research shows that cybercrime victims are sometimes not taken seriously or even turned away when reporting to the police (Leukfeldt et al., 2020; Notté et al., 2021). Moreover, relatively little is invested in cybercrime cases, for example because the police expect that the perpetrator will not be found, may not recognize the seriousness of the offense, or the investigation process seems too complex (Bijleveld et al., 2021; Button et al., 2022; Leukfeldt et al., 2018; Nieuwenhuizen & Van Huijstee, 2022; Notté et al., 2021). This can lead to frustration and dissatisfaction among victims (Button et al., 2020; Leukfeldt et al., 2018).

We define cybercrime as crime in which ICT plays an essential role in the execution of the crime (Domenie et al., 2013). Current police victim policies are primarily designed in the context of traditional crime, which raises questions about their suitability for addressing the needs of the large group of cybercrime victims (Leukfeldt et al., 2018). The unique characteristics of cybercrime, such as anonymity and technical complexity, may create different victim needs (Borwell et al., 2021a; Nieuwenhuizen & Van Huijstee, 2022). Moreover, current victim policies are fairly offender-oriented, which may not align with cybercrime victims who never have to deal with the criminal process, since in cybercrime cases offenders are identified less often than in cases of traditional crime (Ruiter et al., 2023). The way the police handle a case can shape how victims experience the reporting process. These experiences, in turn, are part of victims' process of coping with the offense (Van der Vijver, 1993).

Understanding victim needs and experiences is important because of the 'consent paradigm' that has prevailed since 1977, as introduced in the policy document *Politie in Verandering* ("Police in Transition") (Van Dijk & Hoogewoning, 2018). This paradigm focuses on promoting safety and well-being, in service of the community. It replaced the 'control paradigm,' which was focused on crime control, maintaining

[10] This chapter focuses on the Dutch police. Although this is not explicitly stated throughout the text, it was evident in the original publication's context, which appeared in a Dutch-language journal intended for a national audience.

order, and repression, with greater distance from the public. The reorganization into the National Police in 2013 did not signify a departure from the consent paradigm. However, austerity measures, among others, led to a more control-like approach to police tasks, such as treating reports as the start of a criminal justice process rather than starting from the expectations and needs of citizens (Van Caem & Hageman, 2018; Van Dijk & Hoogewoning, 2018).

In this chapter, we investigate the extent to which the needs and experiences of cybercrime victims differ from those of victims of traditional offenses when reporting—an explicit comparison that, to our knowledge, has not yet been made in prior research. The nature of this study is therefore exploratory. Furthermore, we aim to explain victim needs, examine whether explanations differ for victims of cybercrime and traditional crime, and reflect on the implications of the findings for the role of the police. We investigated the needs and experiences for victims of four crime pairs, namely the cybercrime and traditional variants of (for a more detailed description and justification of the study, see Chapter 5 and Appendix 2): *burglary*: residential burglary versus hacking of online bank accounts; *scams*: doorstep deception versus bank helpdesk fraud; *threat*: offline versus online threat; and *violation of physical integrity*: sexual assault versus image-based sexual abuse (including sextortion and revenge porn).

6.2. Victim needs

Victim needs are generally divided into the needs for information and for practical and emotional support. The extent to which these needs manifest themselves can differ depending on the type of crime (Dunn, 2007; Ten Boom et al., 2008). In this study, based on earlier studies, we focused on a number of victim needs that often emerge in the period shortly after the offense. Regarding informational and practical support, we focus on the following: *known support routes* (Button et al., 2020; Cross et al., 2016b); *practical help with problems arising from the offense* (Button et al., 2020; Leukfeldt et al., 2020; Ten Boom et al, 2008); *information about the offense* (Button et al., 2020; Leukfeldt et al., 2018; Van der Vijver, 1993); *financial compensation* (Leukfeldt et al., 2020; Notté et al., 2021; Ten Boom et al., 2008); and *advice on how to prevent recurrence* (De Kimpe et al., 2020; Dinisman & Moroz, 2017; Ten Boom et al., 2008). When it comes to emotional needs, we focus on the following: *acknowledgment of the offense* (Leukfeldt et al., 2020; Ten Boom et al., 2008); *being taken seriously as a victim* (Ten Boom et al., 2008; Van der Vijver, 1993); and *someone to talk to* (De Kimpe et al., 2020; Notté et al., 2021; Terpstra et al., 2019; Van der Vijver, 1993). In addition, we include two needs that fit less clearly into one of the

categories, namely: *detection, arrest and prosecution of the offender* (Button et al., 2020; Kerr et al., 2013; Leukfeldt et al., 2020; Notté et al., 2021; Van der Vijver, 1993) and *prevention for others* (Cross et al., 2016b; Leukfeldt et al., 2018).

In this study, we also explore explanatory factors for victim needs. These may include various circumstantial and personal factors, as we encountered in previous studies: *peritraumatic stress*: impact during the crime or its discovery (Leukfeldt et al., 2020; Ten Boom et al., 2008; Van Caem & Hageman, 2018; Van der Vijver, 1993); *characteristics of the crime*: financial damage and avoidability (De Kimpe et al., 2020; Dinisman & Moroz, 2017; Leukfeldt et al, 2018); *demographic characteristics*: gender and age (Dinisman & Moroz, 2017; Ten Boom et al., 2008; Van Caem & Hageman, 2018); *personal and social characteristics*: self-efficacy (confidence in one's own ability to solve problems caused by the offense); and *victim blaming by the social environment* (De Kimpe et al., 2020; Leukfeldt et al., 2020; Ten Boom et al., 2008; Van der Vijver, 1993).

6.3. Reporting experiences

For the experiences of victims when reporting to the police, we focus—again based on previous research—on factors that may determine whether the experience is positive or negative. In doing so, we consider the following aspects: *sufficient information about the crime and how it could have happened* (Leukfeldt et al., 2020; Van der Vijver, 1993); *sufficient advice on preventing recurrence* (Ten Boom et al., 2008); *insufficient knowledge of the police* (Leukfeldt et al, 2020); *underestimation of impact by police* (Ten Boom et al., 2008); *victim blaming by police* (De Kimpe et al., 2020; Van der Vijver, 1993); *report treated with urgency* (Van Caem & Hageman, 2018); *sufficient effort made by police* (Kerr et al, 2013; Van Caem & Hageman, 2018; Van der Vijver, 1993); *sufficient information about procedure* (Dinisman & Moroz, 2017; Leukfeldt et al., 2020; Van Caem & Hageman, 2018; Van der Vijver, 1993); *impact decreased due to treatment by police* (Ten Boom et al., 2008; Van der Vijver, 1993); and *impact increased due to treatment by police* (De Kimpe et al., 2020; Notté et al., 2021; Van der Vijver, 1993).

6.4. Methods

The research design was approved by the Ethics Committee of the Open University (cETO)[11] and the Public Prosecutor's Office (PaG)[12]. Below we describe the survey,

[11] Reference U20220.086.
[12] Reference PaG/BJZ/56421.

invitation letter, victim selection, data collection, response and operationalizations. We describe in more detail the design, setup and methods in Chapter 5, and in Appendix 2 and 3.

6.4.1. Survey, invitation letter and victim selection

We selected individuals who had reported to the police and who had been victimized by one of the eight discerned offenses within the past 15 months. In order to select victims of the correct crime types, we used police categories and additional search queries within the police registration system "*Basisvoorziening Informatie*" (BVI) (Basic Provision of Information) using the software platforms Cognos and BlueIntel.[13] We manually assessed the registrations for the definition, criteria and operationalizations of the specific crime. Hybrid forms were excluded (e.g., bank helpdesk fraud in which the victim was visited at home). Addresses of victims were selected through the "*Basisregistratie Personen*" (Basic Registration of Persons) based on Citizen Service Number (BSN). We excluded victims without a BSN, who did not report on their own behalf, were under the age of 18, did not speak Dutch, or lived abroad. We also excluded victims of physical integrity offenses if no phone number was recorded in the police systems, as these victims would only receive an invitation email after obtaining their permission by phone (see Section 6.4.2).

6.4.2. Data collection

The invitation letters and emails followed the police house style and were signed by the national portfolio holder for Police Service and Victim Care. The invitations contained links to the survey related to the specific offense reported. We sent 3,006 invitation letters to victims of the offense pairs within scams, burglary and threat (501 per offense). For the offense pair within violation of physical integrity, due to the sensitivity of the offenses, we approached 1002 victims (501 per offense) by phone to request permission to send the invitation email.

We sent the letters between June 7, 2022 and August 11, 2022. Respondents received a reminder letter after a week and a half. Phone calls and subsequent invitations took place between October 5, 2022, and January 30, 2023. Respondents were granted three weeks to complete the survey, and victims reached by phone and

[13] Cognos enables searches within the BVI, which we used to filter by, for instance, date and police categories, and to perform search queries to select the distinguished crime types. BlueIntel is an online crime categorization system that uses the "National Cybercrime Query" to identify online crime within the BVI (Borwell et al., 2020). The resulting police registrations are then classified by the National Police's cyber intelligence organization. We used some of these classifications for the current study.

e-mail were granted two weeks. Judging by returned letters, at least 24 of the 3,006 victims did not receive the letters. By phone, 791 of the 1002 victims were successfully reached; the others had non-existent or disabled phone numbers or did not answer four call attempts. Of the victims who were successfully reached, 648 received the invitation email.

6.4.3. Response

The gross response rate of the 3,630 victims who received an invitation was 25.7% (933 respondents). For fourteen respondents, the survey was terminated because they indicated during the screening questions that they had not experienced the offense in question during the intended period, or that the report had not been filed on their own behalf. In addition, eight respondents were excluded who indicated that they had been victims of a form of threat other than the one intended. One respondent was excluded during the checking of assumptions for regression analysis, see section 6.5.1. This left 910 victims for analysis. The final response by offense is the displayed *N* in Table 6.1.

To assess selective non-response, we compared the characteristics of the respondents with those of the total group of selected victims. Respondents had a significantly higher estimated mean age than the group of selected victims, except for physical integrity offenses. In terms of gender, the two groups did not differ, except for offline threats, where the proportion of males was lower among respondents. Some caution should be exercised when generalizing to the total victim population.

6.4.4. Operationalizations

Needs. Respondents could indicate on a Likert scale from 1 (I did not have this need) to 5 (I had this need very strongly) the extent to which they had certain needs in the period shortly after the offense, e.g., "Being taken seriously as a victim".

Reporting experience. On a Likert scale from 1 (definitely not) to 5 (definitely yes), respondents could indicate the extent to which statements applied to their experience of reporting, e.g., "I was able to share my story with the police".

Peritraumatic stress. Respondents could indicate on a Likert scale from 1 (then not experienced) to 5 (then experienced very strongly) to what extent they experienced certain consequences when the crime took place or they found out that it had taken place, e.g. "It made me feel helpless". We constructed the scale "peritraumatic stress" using five items (Cronbach's alpha = 0.85), based on a principal component analysis (PCA) which indicated a single factor.

Age. We asked for respondents' year of birth, and to estimate age we calculated the difference with the year in which the survey was completed.

Gender. Respondents could indicate their gender (male, female, or non-binary). Two respondents selected the latter category; their answers were excluded from analyses involving gender.

Financial loss. We asked respondents what the direct financial loss from the offense was. The response categories ranged from no loss (1) to more than €50,000 (9).

Avoidability. Respondents could indicate on a Likert scale from 1 (definitely not) to 5 (definitely yes) the extent to which the following statement applied to them: "Looking back on the experience, I could have prevented the offense from happening at the time."

Self-efficacy. Respondents could indicate on a Likert scale from 1 (definitely not) to 5 (definitely yes) the extent to which the statement "I can solve the offense and its consequences myself" applied to them.

Victim blaming. Respondents could indicate on a Likert scale from 1 (definitely not) 5 (definitely yes) the extent to which the statement "Those around me (e.g. partner, friends or family) blame me for the offense" applied to them.

6.4.5. Analyses

We used SPSS version 28 for the analyses. Given the exploratory nature of this study, we conducted two-sided tests with a significance level of $p < .01$. For differences in means, we used *t* tests. Explanations for needs were tested using separate linear regression analyses for each predictor variable. In doing so, we included interaction terms between the type of offense (cybercrime or traditional crime) and each predictor variable to examine any differences in the explanation of needs between cybercrime and traditional crime.

Using Mahalanobis distance, we detected several univariate and multivariate outliers, based on which we removed one case (a victim of image-based sexual abuse with extreme, inconsistent values). Using Cook's distance, we found no outliers. We considered some violations of the normalcy assumption in the dependent variables (positive or negative skewed distributions) to be minor because of the large sample size (more than 200 cases, see Tabachnick et al., 2013). We checked for multicollinearity among the dependent and independent variables using Pearson correlations.

All correlations remained below 0.8, indicating no significant multicollinearity. We also found no evidence of non-linear relationships. Specific output is available from the authors upon request.

6.5. Results

6.5.1. Needs of victims

Table 6.1 shows the *t* tests we used to compare the mean need scores among victims of the four crime pairs. We found twelve significant differences, ten of which occurred in the offense pairs of burglary and scams, and two in violation of physical integrity. Victims of the online variants of burglary and fraud reported a greater need for "known support routes," "information about the crime," and "financial compensation". In addition, victims of online bank account hacking, compared to victims of residential burglary reported a greater need for "acknowledgment of the crime" and "prevention for others". Victims of bank helpdesk fraud, compared to victims of doorstep deception, expressed a greater need for "practical help with problems caused by the crime" and "advice on preventing repetition". Finally, victims of image-based sexual abuse, compared to victims of sexual assault, reported a *lower* need for "someone to talk to" and "prevention for others".

Differences between the cyber and traditional property crimes (burglary and scams), and the cyber and traditional person-centered crimes (threat and violation of physical integrity), were in the same direction or absent. The needs of cybercrime property victims were stronger than or equal to the needs of traditional property crime victims. For person-centered crimes, the opposite was true: there were no differences, or the needs of victims of traditional person-centered crimes were higher. Therefore, for the explanatory analyses of victim needs described in Section 6.5.2, we decided to group the cyber and traditional property crimes on the one hand, and the cyber and traditional person-centered crimes on the other.

Table 6.1. T tests of differences in mean needs for four crime pairs

	Burglary		Scam		Threat		Violation physical integrity	
	Residential burglary (*N* = 130)	Online bank account hacking (*N* = 143)	Doorstep deception (*N* = 94)	Bank helpdesk fraud (*N* = 212)	Offline threat (*N* = 52)	Online threat (*N* = 56)	Sexual assault (*N* = 138)	Image-based sexual abuse (*N* = 85)
Needs[a]	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)
Known support routes	1.12 (1.34)	1.59 (1.58)	1.64 (1.54)	2.26 (1.59)	2.37 (1.60)	1.82 (1.61)	2.44 (1.34)	2.21 (1.38)
t	-2.71[b]		-3.18		1.76		1.23	
p	.007*		.002*		.081		.219	
Acknowledgment offense	1.45 (1.48)	1.94 (1.56)	2.29 (1.44)	2.63 (1.48)	2.90 (1.45)	2.36 (1.54)	2.79 (1.29)	2.40 (1.39)
t	-2.70		-1.90		1.90		2.13	
p	.007*		.059		.061		.034	
Taken seriously as a victim	1.72 (1.53)	2.20 (1.60)	2.57 (1.51)	2.72 (1.51)	3.10 (1.30)	2.70 (1.48)	3.08 (1.27)	2.62 (1.38)
t	-2.53		-0.76		1.49		2.52	
p	.012		.446		.140		.013	
Practical support	1.64 (1.50)	1.97 (1.66)	1.62 (1.59)	2.20 (1.64)	2.00 (1.75)	1.25 (1.43)	1.76 (1.50)	1.67 (1.48)
t	-1.70		-2.89		2.43[b]		0.44	
p	.091		.004*		.017		.661	
Information about the crime	1.35 (1.40)	2.20 (1.48)	1.69 (1.58)	2.27 (1.51)	1.87 (1.68)	1.11 (1.34)	1.74 (1.38)	1.61 (1.35)
t	-4.86		-3.04		2.58[b]		0.67	
p	<.001**		.003*		.011		.501	
Financial compensation	1.64 (1.55)	2.22 (1.70)	1.38 (1.63)	2.18 (1.72)	1.27 (1.68)	0.73 (1.30)	0.63 (1.24)	0.87 (1.35)
t	-2.93		-3.82		1.85[b]		-1.35	
p	.004*		<.001**		.068		.177	

Table 6.1 continues on next page.

Table 6.1. ***Continued***

	Burglary		Scam		Threat		Violation physical integrity	
	Residential burglary (*N* = 130)	Online bank account hacking (*N* = 143)	Doorstep deception (*N* = 94)	Bank helpdesk fraud (*N* = 212)	Offline threat (*N* = 52)	Online threat (*N* = 56)	Sexual assault (*N* = 138)	Image-based sexual abuse (*N* = 85)
Needs[a]	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)
Detection, arrest, prosecution	2.43 (1.59)	2.53 (1.59)	2.83 (1.49)	3.02 (1.43)	2.73 (1.62)	2.16 (1.79)	2.28 (1.67)	1.73 (1.68)
t	-0.53		-1.08		1.73		2.36	
p	.602		.281		.086		.019	
Someone to talk to	1.23 (1.42)	1.41 (1.53)	1.93 (1.59)	2.00 (1.61)	2.15 (1.60)	1.89 (1.53)	2.69 (1.34)	2.13 (1.49)
t	-0.98		-0.40		0.87		2.90	
p	.330		.690		.389		.004*	
Prevention advice	1.57 (1.45)	1.86 (1.48)	1.61 (1.48)	2.26 (1.50)	1.44 (1.71)	1.09 (1.40)	1.41 (1.45)	1.62 (1.47)
t	-1.64		-3.53		1.17[b]		-1.08	
p	.103		<.001**		.246		.281	
Prevention for others	1.35 (1.36)	2.04 (1.51)	2.55 (1.40)	2.46 (1.47)	2.06 (1.69)	1.64 (1.70)	2.68 (1.59)	2.00 (1.66)
t	-3.95		0.53		1.27		3.06	
p	<.001**		.595		.206		.003*	

*$p < .01$; **$p < .001$ (two-sided).

[a]Scale 0 to 4; [b]Equal variances not assumed.

6.5.2. Explanations for victim needs in property crime (burglary, scams)

In the previous section, we identified differences between the needs of cyber and traditional property crime victims. We now examine the explanations for victim needs and whether they are different for cybercrime and traditional crime, see Table 6.2. We used a separate explanatory model for the effect of crime type (cybercrime or traditional crime) on victim needs. This model is reported once in the table. We then used three models for each independent variable: model 1 includes only the type of crime, model 2 includes the main effect of the other independent variable, and model 3 includes the interaction effect between type of crime and that other independent variable. With this approach, we do justice to the exploratory and practice-oriented nature of the study, in which we aim to identify the effects of each individual independent variable on victim needs, as well as potential differences therein between cybercrime and traditional crime.

As expected from the *t* tests, victims of property cybercrime had higher needs for known support routes, acknowledgment of the offense, practical support, information about the crime, financial compensation for losses, advice on preventing recurrence, and prevention for others. Victims who had experienced more peritraumatic stress expressed all needs more strongly. In addition, the higher the age of the victims, the greater their need for known help routes, acknowledgment of the offense, being taken seriously as a victim, detection, arrest and prosecution of the offender, and prevention advice. Compared to men, women had a greater need for known support routes, acknowledgment of the offense, being taken seriously as a victim, practical help, someone to talk to, and prevention for others.

The more financial loss victims had experienced, the greater their need for known support, acknowledgment of the offense, being taken seriously as a victim, practical help, information about the offense, financial compensation, detection, arrest and prosecution of the offender, someone to talk to, and prevention advice.

Regarding the extent to which victims reported that they could have prevented the crime afterwards (avoidability), the interaction effect was significant, see Figure 6.1. For victims of traditional crime, the need for prevention for others increased with higher avoidability, whereas among cybercrime victims, no clear effect was observed.

Victims who indicated that they could resolve the offense and its consequences themselves (self-efficacy) reported less need for practical support, someone to talk to, and prevention advice.

The more victim blaming respondents had experienced from their social environment, the greater their reported need for prevention for others.

Table 6.2. Explanatory variables for victim needs in property crime (burglary and scam)

Independent variables (*N*)		Type (cyber) (579)	Peritraumatic stress (579)		Age (574)		Gender (female) (577)		Financial loss (566)		Avoidability (579)		Self-efficacy (579)		Victim blaming (579)		Total (560)
Dependent variables		Main effect	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	
Known support routes	*b*	.66**	.45**	-.15	.01*	.01	.37*	-.23	.11**	.15	.03	-.12	-.10	.10	.04	.07	
	Δ*F*	24.57	81.82	2.28	7.68	1.08	8.27	0.79	13.32	5.48	0.41	1.94	5.39	1.38	0.35	0.18	14.21**
	R^2 (adj)	.04	.16	.16	.05	.05	.05	.05	.06	.07	.04	.04	.05	.05	.04	.04	.16
Acknowledgement offense	*b*	.56**	.54**	-.09	.02**	.01	.45**	-.41	.13**	.06	.03	-.05	-.10	.04	.13	.10	
	Δ*F*	18.01	128.68	0.79	15.30	0.59	12.37	2.45	17.08	0.86	0.47	0.38	6.28	0.26	3.44	0.38	20.51**
	R^2 (adj)	.03	.20	.20	.05	.05	.05	.05	.06	.06	.03	.03	.04	.04	.03	.03	.22
Taken seriously as a victim	*b*	.43	.51**	-.07	.01*	-.01	.56**	-.17	.11**	.06	.02	-.04	-.07	.09	.11	.06	
	Δ*F*	10.39	104.30	0.49	9.61	0.48	18.90	0.40	11.17	0.38	0.31	0.25	2.62	1.11	2.40	0.11	15.87**
	R^2 (adj)	.02	.17	.17	.03	.03	.05	.05	.03	.03	.02	.01	.02	.02	.02	.02	.18
Praktical support	*b*	.48**	.42**	-.07	.01	.00	.40*	.11	.12**	-.01	-.01	.05	-.12*	.10	.12	.31	
	Δ*F*	11.99	64.21	0.45	3.90	0.23	8.96	0.16	13.55	0.03	0.03	0.30	7.32	1.13	2.50	3.30	10.43**
	R^2 (adj)	.02	.12	.12	.02	.02	.03	.03	.04	.04	.02	.02	.03	.03	.02	.03	0.12
Information about the crime	*b*	.75**	.42**	-.11	.01	.00	.18	-.17	.10*	-.07	.02	-.01	.00	.02	.14	.23	
	Δ*F*	34.38	74.49	1.21	4.19	0.15	2.06	0.45	10.42	1.35	0.24	0.02	0.00	0.03	3.88	2.05	15.22**
	R^2 (adj)	.06	.16	.16	.06	.06	.06	.06	.07	.07	.05	.05	.05	.05	.06	.06	0.17

Table 6.2. ***Continued***

Independent variables (*N*)		Type (cyber) (579)	Peritraumatic stress (579)		Age (574)		Gender (female) (577)		Financial loss (566)		Avoidability (579)		Self-efficacy (579)		Victim blaming (579)		Total (560)
Dependent variables		Main effect	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	
Financial compensation	*b*	.67**	.20**	.01	.00	.00	.06	.40	.20**	-.16	-.08	.02	-.03	.09	.12	.39	
	ΔF	22.05	12.98	0.00	0.88	0.07	0.17	1.96	37.60	5.91	2.65	0.06	0.44	0.88	2.32	4.69	9.12**
	R^2 (adj)	.04	.06	.05	.04	.03	.03	.04	.09	.10	.04	.04	.03	.03	.04	.04	.10
Detection, arrest, prosecution	*b*	.23	.21**	.07	.01*	.00	.28	.03	.14**	.05	.02	.00	-.07	-.02	.13	-.22	
	ΔF	3.02	15.55	0.49	6.84	0.17	4.69	0.02	21.38	0.71	0.24	0.00	3.25	0.04	3.40	1.79	5.60**
	R^2 (adj)	.00	.03	.03	.01	.01	.01	.01	.04	.04	.00	.00	.01	.01	.01	.01	.06
Someone to talk to	*b*	.24	.60**	-.02	.01	.00	.62**	-.19	.14**	.11	-.01	-.10	-.12*	.09	.12	.21	
	ΔF	3.22	156.80	0.03	3.61	0.00	22.83	0.51	20.59	2.82	0.04	1.18	7.47	1.14	2.78	1.58	20.70**
	R^2 (adj)	.00	.22	.21	.01	.01	.04	.04	.04	.04	.00	.00	.02	.02	.01	.01	.22
Prevention advice	*b*	.15**	.42**	-.04	.01**	.00	.22	-.03	.13**	.02	-.07	-.03	-.11*	.07	.07	.08	
	ΔF	16.42	77.16	0.16	11.77	0.24	3.13	0.02	19.45	0.16	2.71	0.17	7.57	0.66	0.91	0.24	13.69**
	R^2 (adj)	.03	.14	.14	.04	.04	.03	.03	.06	.06	.03	.03	.04	.04	.03	.03	.15
Prevention for others	*b*	.43**	.37**	-.06	.01	.00	.35*	-.21	.07	.13	.07	-.22*	-.05	.05	.21*	-.28	
	ΔF	11.48	58.24	0.30	3.54	0.06	8.05	0.70	5.64	4.14	2.80	7.13	1.62	0.32	8.70	3.03	10.27**
	R^2 (adj)	.02	.11	.11	.02	.02	.03	.03	.03	.03	.02	.03	.02	.02	.03	.03	.12

*$p < .01$; **$p < .001$ (two-sided).

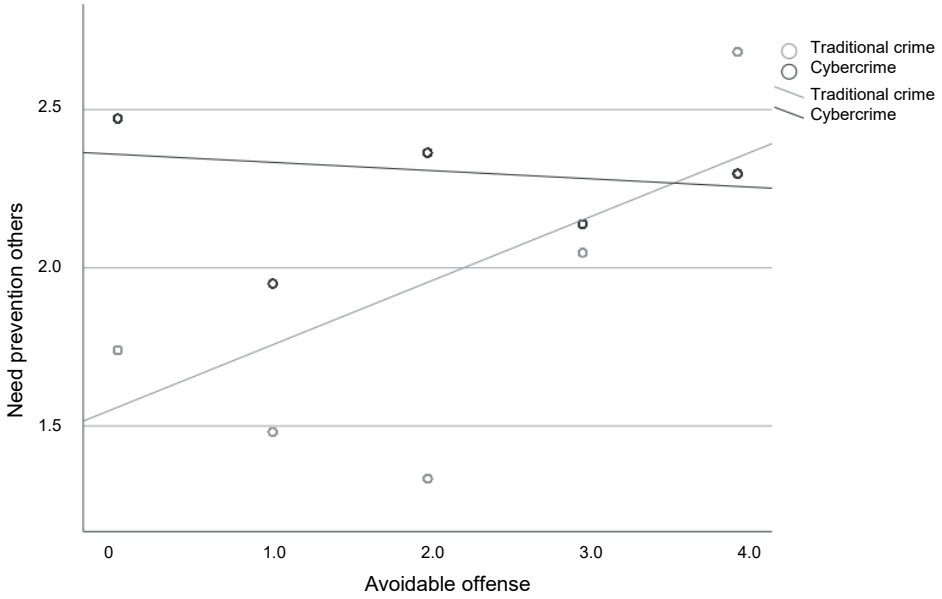


Figure 6.1. Avoidable offense and need for prevention for others (property crime).

To test the explanatory power of the independent variables for the needs variables, we added all the independent variables to the models simultaneously, excluding the interaction terms. The independent variables have an acceptable predictive value for needs, as this exceeds 10% (except for the need for detection, arrest and prosecution), and several significant predictors are present (Ozili, 2023).[14] From the foregoing, crime type, peritraumatic stress and financial loss emerged as relatively strong predictors for the needs of property crime victims.

6.5.3. Explanations for victim needs in person-centered crime (threat and violation of physical integrity)

Table 6.3 presents the explanatory variables for victim needs in person-centered crime. Compared to victims of person-centered traditional crime, victims of person-centered cybercrime needed less recognition of the crime, being taken seriously as a victim, detection, arrest and prosecution of the offender, someone to talk to, and prevention for others. Victims who had experienced more peritraumatic stress had

[14] Because 22% of the variance in acknowledgment of the offense was explained; 22% in someone to talk to; 18% in being taken seriously as a victim; 17% in information about the offense; 16% in known support routes; 15% in prevention advice; 12% in practical support; 12% in prevention for others; 10% in financial compensation; and 6% in detection, arrest, prosecution.

a greater need for known support routes, recognition of the offense, practical help, information about the crime, someone to talk to, prevention advice, and prevention for others. The higher the age of the victims of person-centered crime, the greater their need for detection, arrest and prosecution of the offender.

Female victims expressed a higher need of someone to talk to than male victims.

With increasing financial losses, victims were more in need of practical support, information about the offense, and financial compensation.

The more victims considered the crime avoidable in hindsight, the greater their need for information about the offense.

There was a significant interaction effect of crime type and avoidability: victims of traditional crime had a greater need of someone to talk to as the offense was perceived as more avoidable, whereas among cybercrime victims no clear effect was observed, see Figure 6.2.

The interaction effect between type of crime and avoidability was also significant, see Figure 6.3: victims of traditional crime had a greater need for prevention advice as perceived avoidability increased, whereas this effect was less pronounced for cybercrime victims.

There was also a significant interaction effect for self-efficacy and type of crime, see Figure 6.4: for traditional crime, the need for practical support decreases with increasing self-efficacy, whereas among cybercrime victims a slight increase in the need for practical support can be observed.

Finally, as victim blaming increased, victims had a greater need for information about the offense.

Again, we added all independent variables to the models simultaneously, excluding the interaction terms. The explanatory strength of the independent variables can only be considered acceptable for the need for practical support, information about the offense, financial compensation, someone to talk to and prevention advice (Ozili, 2023).[15] Furthermore, crime type, peritraumatic stress, and financial damage also appear to be the most important predictors of needs in person-centered crime.

[15] Because 16% of the variance in prevention advice was explained; 13% in information about the offense; 12% in practical support; 12% in someone to talk to; 9% in known support routes; 8% in acknowledgment of the offense; 8% in financial compensation; 7% in prevention for others; 6% in detection, arrest, prosecution; and 5% in being taken seriously as a victim.

Table 6.3. Explanatory variables for victim needs in person-centered crime (threat and violation physical integrity)

Independent variables (*N*)		Type (cyber) (331)	Peritraumatic stress (330)		Age (326)		Gender (female) (329)		Financial loss (305)		Avoidability (331)		Self-efficacy (331)		Victim blaming (331)		Total (299)
Dependent variables		Main effect	Main effect	Interac-tion	Main effect	Interac-tion	Main effect	Interac-tion	Main effect	Interac-tion	Main effect	Interac-tion	Main effect	Interac-tion	Main effect	Interac-tion	
Known support routes	*b*	-.36	.34**	-.20	.00	-.02	.41	-.37	.11	.06	.14	-.01	-.11	.17	.09	.17	
	ΔF	5.17	26.22	2.19	0.04	2.14	4.41	0.89	3.53	0.23	5.52	0.01	4.01	2.28	1.25	1.01	4.73**
	R^2 (adj)	.01	.09	.09	.01	.01	.02	.02	.02	.02	.03	.02	.02	.03	.01	.01	.09
Acknowledgement offense	*b*	-.44*	.25**	-.17	.01	.00	.32	-.12	.05	.00	.05	-.18	-.03	.17	.15	-.03	
	ΔF	8.15	14.62	1.66	6.43	0.03	2.90	0.09	0.82	0.00	0.74	2.20	0.38	2.72	3.69	0.03	4.32**
	R^2 (adj)	.02	.06	.06	.04	.03	.03	.02	.02	.02	.02	.02	.02	.02	.03	.03	.08
Taken seriously as a victim	*b*	-.43*	.15	-.20	.01	.01	.44	-.16	.01	.12	.04	-.21	.00	.10	-.03	.25	
	ΔF	8.43	5.32	2.34	1.65	1.44	6.00	0.20	0.03	1.16	0.54	3.19	0.00	1.02	0.12	5.53	2.87*
	R^2 (adj)	.02	.04	.04	.02	.03	.04	.03	.02	.02	.02	.03	.02	.02	.02	.02	.05
Practical support	*b*	-.32	.38**	-.09	.01	-.01	.05	-.72	.25**	-.19	.14	-.09	-.12	.36*	.06	.27	
	ΔF	3.61	28.71	0.43	0.93	0.51	0.05	2.92	18.84	2.37	5.45	0.41	4.68	9.62	0.51	2.25	6.05**
	R^2 (adj)	.01	.09	.08	.01	.01	.01	.01	.06	.07	.02	.02	.03	.05	.01	.01	.12
Information about the crime	*b*	-.36	.37**	-.16	.00	-.01	.22	-.78	.24**	-.13	.18*	-.05	-.05	.25	.24*	.07	
	ΔF	5.24	31.84	1.45	0.07	1.42	1.31	4.01	20.32	1.28	10.33	0.17	0.74	5.24	8.78	0.15	6.73**
	R^2 (adj)	.01	.10	.10	.01	.01	.01	.02	.07	.07	.04	.04	.01	.03	.04	.03	.13
Financial compensation	*b*	.01	.16	-.05	.01	-.02	-.20	-.28	.29**	-.18	-.03	-.05	-.07	.15	.06	.01	
	ΔF	0.01	5.63	0.15	1.82	4.28	1.16	0.57	31.89	2.93	0.22	0.14	1.89	2.12	0.53	0.00	4.41**
	R^2 (adj)	.00	.01	.01	.00	.01	.00	.00	.09	.10	-.01	-.01	.00	.00	.00	-.01	.08

Table 6.3. ***Continued***

Independent variables (*N*)		Type (cyber) (331)	Peritraumatic stress (330)		Age (326)		Gender (female) (329)		Financial loss (305)		Avoidability (331)		Self-efficacy (331)		Victim blaming (331)		Total (299)
Dependent variables		Main effect	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	Main effect	Interaction	
Detection, arrest, prosecution	*b*	-.50*	.08	-.13	.03**	.02	-.43	.24	.08	-.06	-.13	-.17	-.05	.04	-.10	-.06	
	ΔF	7.03	0.86	0.63	17.38	1.46	0.35	0.27	1.48	0.19	3.61	1.30	0.64	0.08	1.04	0.09	3.49**
	R^2 (adj)	.02	.02	.02	.07	.07	.02	.01	.02	.02	.03	.03	.02	.01	.02	.02	.06
Someone to talk to	*b*	-.51*	.38**	-.02	.00	.01	.56*	-.72	.07	-.03	.15	-.35*	-.09	.01	.11	.06	
	ΔF	9.68	31.07	0.02	0.15	0.86	8.04	3.27	1.37	0.07	6.68	7.76	2.80	0.01	1.67	0.11	6.18**
	R^2 (adj)	.03	.11	.11	.02	.02	.05	.05	.03	.02	.04	.06	.03	.03	.03	.03	.12
Prevention advice	*b*	.00	.48**	.00	.00	-.01	.05	-1.03	.15	.00	.27**	-.39*	-.11	.18	.18	.21	
	ΔF	0.00	50.36	0.00	0.20	0.65	0.07	6.34	6.69	0.00	20.52	9.55	3.58	3.17	4.52	1.48	8.00**
	R^2 (adj)	.00	.13	.13	-.01	-.01	-.01	.01	.02	.01	.05	.08	.01	.01	.01	.01	.16
Prevention for others	*b*	-.65**	.23*	.09	.01	.00	.56	-1.04	.03	-.02	.09	-.21	.00	-.06	.15	.17	
	ΔF	12.58	8.56	0.29	1.16	0.02	6.36	5.41	0.18	0.02	2.00	2.04	0.00	0.20	2.47	0.73	4.00**
	R^2 (adj)	.03	.06	.05	.03	.03	.05	.06	.03	.03	.04	.04	.03	.03	.04	.04	.07

*$p < .01$; **$p < .001$ (two-sided).

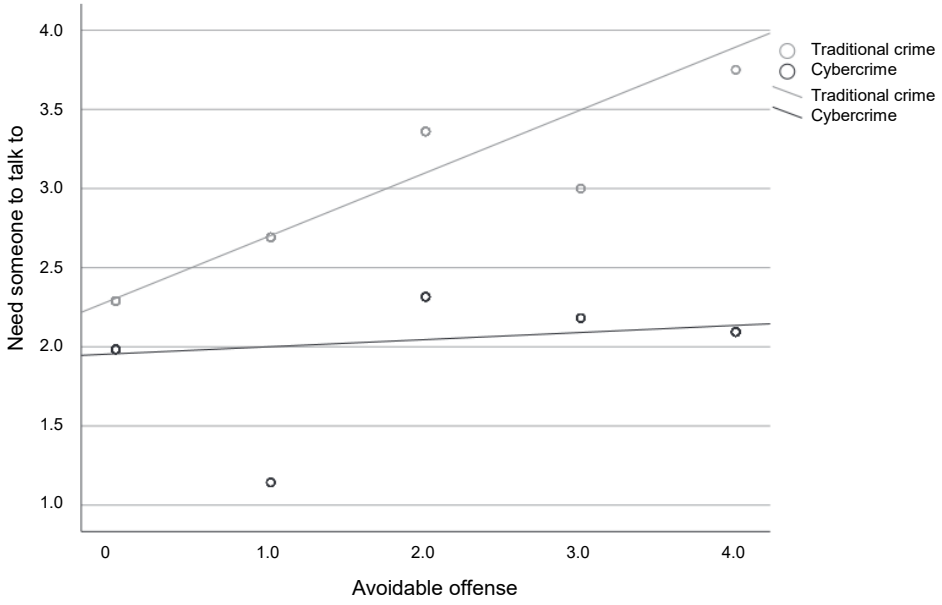


Figure 6.2. Avoidable offense and need of someone to talk to (person-centered crime).

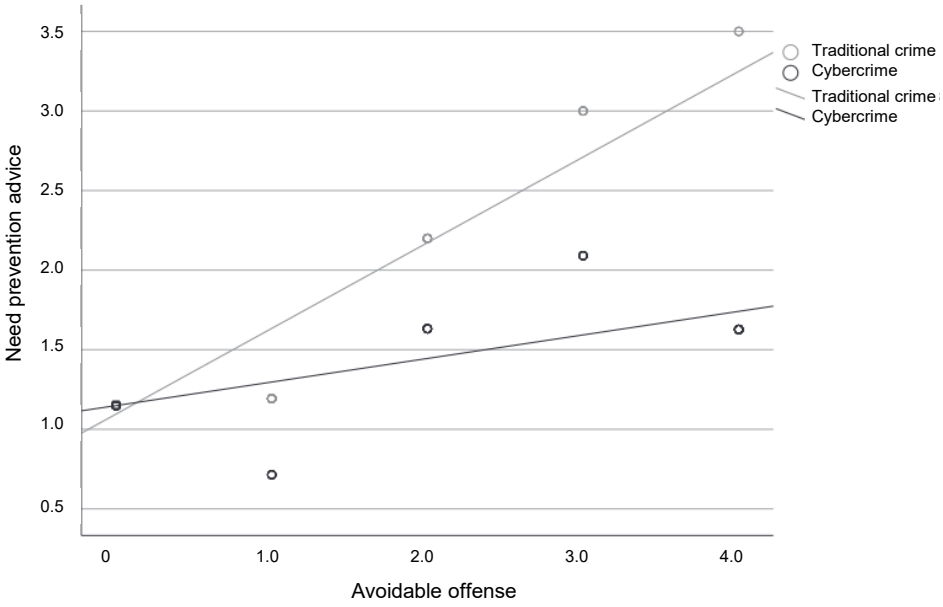


Figure 6.3. Avoidable offense and need of prevention advice (person-centered crime).

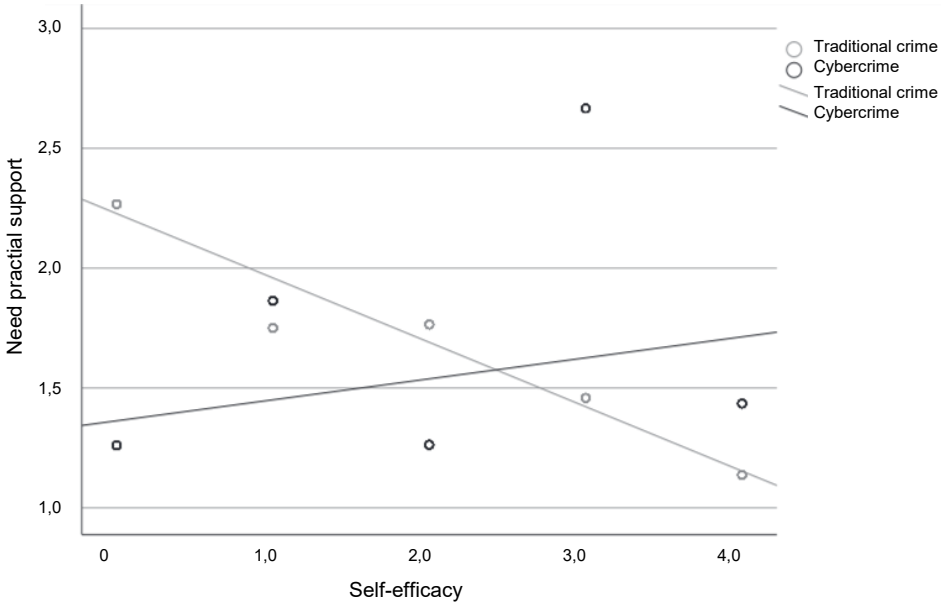


Figure 6.4. Self-efficacy and need for practical support (person-centered crime).

6.5.4. Victims' reporting experiences

Table 6.4 presents the *t* tests used to compare the reporting experiences among victims of the four crime pairs. Victims of image-based sexual abuse indicated to a greater extent that they had received sufficient information about the offense and prevention advice than victims of sexual assault. In addition, victims of image-based sexual abuse indicated to a lesser extent than victims of sexual assault that the impact increased as a result of police handling of the report. For the other crime pairs, we found no significant differences in reporting experience.

Table 6.4. T tests of differences in mean reporting experiences for four crime pairs

	Burglary		Scam		Threat		Violation physical integrity	
	Residential burglary (*N* = 130)	Online bank account hacking (*N* = 143)	Doorstep deception (*N* = 94)	Bank helpdesk fraud (*N* = 212)	Offline threat (*N* = 52)	Online threat (*N* = 56)	Sexual assault (*N* = 138)	Image-based sexual abuse (*N* = 85)
Reporting experience[a]	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)	*M* (*SD*)
Able to tell story	3.53 (0.87)	3.39 (1.11)	3.69 (0.82)	3.58 (0.94)	2.90 (1.40)	3.23 (1.22)	3.33 (1.09)	3.21 (1.09)
t	1.15[b]		1.03		-1.30		0.81	
p	.249		.303		.197		.420	
Information about offense	3.05 (1.24)	2.94 (1.34)	3.00 (1.32)	3.13 (1.25)	2.04 (1.57)	2.39 (1.47)	2.25 (1.34)	2.81 (1.25)
t	0.65		-0.84		-1.21		-3.10	
p	.514		.403		.229		.002*	
Prevention advice	2.83 (1.25)	2.64 (1.42)	2.69 (1.38)	2.90 (1.31)	1.25 (1.36)	1.93 (1.41)	1.44 (1.40)	2.67 (1.28)
t	1.20[b]		-1.24		-2.54		-6.57	
p	.230		.217		.012		<.001**	
Too little knowledge	0.80 (1.20)	0.90 (1.24)	0.72 (1.16)	0.67 (1.10)	1.48 (1.57)	1.25 (1.48)	0.91 (1.09)	1.07 (1.17)
t	-0.64		0.35		0.88		-1.02	
p	.521		.724		.433		.310	
Underestimating impact	0.60 (1.09)	0.57 (1.04)	0.59 (1.13)	0.55 (1.00)	1.75 (1.63)	1.30 (1.58)	1.07 (1.31)	1.14 (1.17)
t	0.21		0.29		1.44		-0.44	
p	.837		.770		.152		.662	
Victim blaming	0.15 (0.65)	0.27 (0.79)	0.24 (0.86)	0.24 (0.70)	0.63 (1.27)	0.25 (0.72)	0.42 (0.93)	0.48 (.089)
t	-1.45[b]		-0.12		1.92[b]		-0.49	
p	.147		.906		.059		.623	

Table 6.4. ***Continued***

	Burglary		Scam		Threat		Violation physical integrity	
	Residential burglary (*N* = 130)	Online bank account hacking (*N* = 143)	Doorstep deception (*N* = 94)	Bank helpdesk fraud (*N* = 212)	Residential burglary (*N* = 130)	Online bank account hacking (*N* = 143)	Doorstep deception (*N* = 94)	Bank helpdesk fraud (*N* = 212)
Report handled urgently	2.33 (1.31)	2.03 (1.47)	2.45 (1.43)	2.47 (1.36)	1.77 (1.66)	2.00 (1.57)	1.93 (1.36)	1.74 (1.36)
t	1.79		0.41		-0.74		1.04	
p	.075		.682		.460		.302	
Sufficient effort made	2.76 (1.30)	2.45 (1.38)	2.79 (1.29)	2.72 (1.29)	2.15 (1.65)	2.11 (1.42)	2.28 (1.36)	1.87 (1.26)
t	1.88		0.80		0.16[b]		2.30	
p	.061		.423		.876		.014	
Information on procedure	2.59 (1.47)	2.31 (1.50)	2.63 (1.37)	2.48 (1.52)	1.83 (1.67)	2.11 (1.56)	2.39 (1.38)	2.07 (1.38)
t	1.54		0.88		-0.90		1.69	
p	.124		.380		.368		.093	
Impact decreased by treatment	2.21 (1.32)	2.40 (1.30)	2.47 (1.38)	2.32 (1.40)	1.56 (1.41)	1.61 (1.51)	1.84 (1.36)	1.78 (1.34)
t	-1.20		-0.94		-0.18		0.34	
p	.229		.347		.861		.731	
Impact increased by treatment	0.86 (1.24)	0.65 (1.10)	0.40 (0.95)	0.51 (0.94)	1.31 (1.42)	1.27 (1.45)	1.22 (1.37)	0.73 (1.08)
t	1.48[b]		-0.94		0.14		2.99[b]	
p	.139		.347		.886		.003*	

*$p < .01$; **$p < .001$ (two-sided).
[a]Scale 0 to 4; [b]Equal variances not assumed.

6.6. Conclusion and discussion

6.6.1. Needs

Victims of property cybercrime (hacking of online bank account and bank helpdesk fraud) expressed stronger practical needs compared to victims of traditional property crime (residential burglary and doorstep deception), namely: known support routes, information about the crime, financial compensation, and prevention advice. In addition, they had stronger emotional/social needs: for acknowledgment of the crime and prevention for others. For person-centered offenses, victims of the traditional variants (offline threat and sexual assault) expressed stronger emotional/social needs: acknowledgment of the crime, being taken seriously as a victim, talking to someone and prevention for others than victims of the cybercrime variants (online threat and image-based sexual abuse). They also had a greater need for detection, arrest and prosecution of the offender. Stronger feelings of shame and self-blame in victims of image-based sexual abuse (Borwell et al., 2024) may have contributed to diminished emotional/social needs, as such feelings may inhibit victims from sharing their experiences.

Our study confirms that victims of cybercrime, just as victims of traditional crime, have needs across all categories (Leukfeldt et al., 2020). The comparisons we made allow us to add several nuances to this. Contrary to previous findings, our results do not indicate that cybercrime victims have fewer practical needs (Leukfeldt et al., 2018). The strong practical needs of cybercrime victims may be related to the technical complexity of the offenses and the lack of clear support routes (Borwell et al., 2021; Button et al., 2020). Furthermore, according to earlier qualitative research, victims of person-centered cybercrime such as cyberstalking and sexting would primarily want the perpetrator to be arrested (Leukfeldt et al., 2020), whereas we found that victims of person-centered crimes expressed the need to be taken seriously as a victim most strongly, as opposed to the need for investigation, arrest and prosecution of the perpetrator in the case of property crime. This divergent finding may be related to the probability that cyberstalking or sexting involves a known offender (Finkelhor et al., 2023), leading victims to focus more on the offender personally. A possible explanation for our findings is that the high emotional impact of person-centered crimes (Borwell et al., 2024) causes the need to be taken seriously as a victim to be regarded as more important than criminal prosecution.

In addition to comparisons between crime types, we sought to explain victim needs and examined whether these explanations differed for victims of cybercrime and traditional crime. For both property and person-centered crimes, peritraumatic stress

was relatively strongly related to needs of a practical and emotional/social nature. Also, for both crime types, the need for investigation and prosecution increased with age, which aligns with studies that found a relationship between age and punitive attitudes (Van Kesteren, 2009). For property crimes, some practical and emotional needs also increased with age. Among practical needs, this may be related to comprehending the offense, which can be particularly difficult for older individuals in the context of cybercrime (Cross, 2015). In terms of gender, both types of crimes showed that emotional needs were expressed more strongly by women, consistent with earlier research (Dinisman & Moroz, 2017; Ten Boom et al., 2008). In property crimes, financial loss created stronger needs in every area except prevention for others. In the person-centered offenses, it also created some stronger practical needs, consistent with previous research (Dinisman & Moroz, 2017).

Regarding the perceived avoidability of the offense, it was notable that for cybercrime there was less or no clear effect on certain needs, whereas in traditional crime it did lead to stronger needs. A possible explanation is self-blame among cybercrime victims, causing them—when the offense was preventable—to believe they should meet their own needs (Leukfeldt et al., 2018). In person-centered offenses, greater perceived avoidability also led to a greater need for information about the offense, possibly for tools to prevent recurrence. Higher self-efficacy in property crimes was associated with a lower need for practical help, someone to talk to and prevention advice. For person-centered crimes, the need for practical help also decreased with increasing self-efficacy for traditional victims, while it increased slightly for cybercrime victims. Possibly, cybercrime victims require external assistance to resolve problems caused by the offense, which may be related to the technical complexity of cybercrimes. More victim blaming from the social environment only led to a greater need for prevention for others in the case of property crimes (possibly to protect them from this or due to insight gained from their own experience) and a greater need for information about the crime in the case of personal offenses (possibly because such information was not provided by their environment). According to previous research, victim blaming is strongly associated with the need for recognition of the offense (Leukfeldt et al., 2018), which we did not observe.

The factors considered in this study explained victim needs to a limited extent, especially for person-centered offenses. This finding, along with the limited differences observed between cybercrime and traditional crime, confirms that most needs are widely shared across victim groups (Leukfeldt et al., 2018; Ten Boom et al., 2008). In addition to crime type, the strongest effects were found for peritraumatic stress, age, gender and financial loss. These are clear characteristics that the police can respond

to. For example, special attention can be given to those who have experienced more peritraumatic stress, are of higher age, are women (in the case of emotional needs) and have sustained more financial loss. A person-centered approach can be used to offer tailored support, so that those with greater needs actually receive appropriate help, in line with the consent paradigm. At the same time, the principle of equal justice must always be upheld, to ensure that justice is also done for those who, for instance, do not articulate strong needs or are unable to clearly express them (Dunn, 2007).

An adequate level of victim support and meeting emotional and practical needs is important for everyone who desires it, and it may be helpful to understand the factors that contribute to the emergence of greater needs. For example, the police can be more attentive to practical and emotional support for cybercrime victims. Practical support could include an information leaflet for victims, including names and contact details of organizations they can turn to with specific requests for help, information about cybercrime, and prevention advice. Regarding emotional support, an empathetic approach by a police officer is important, to which this study can contribute by raising awareness of victim needs. This can also be addressed in the context of online reporting, for instance by emphasizing that it is always possible to file a report in person at a police station. Although this study did not reveal indications of victim blaming by the police, other studies have shown that cybercrime victims are more often confronted with victim blaming from those around them and more often blame themselves for the offense (Borwell et al., 2024; Leukfeldt et al., 2018). It is therefore important that police officers avoid conscious and unconscious victim blaming—and thus secondary victimization—by being mindful of their choice of language and approaches that implicitly or explicitly place blame on the victim.

6.6.2. Reporting experiences

The experience of reporting is similar between cyber and traditional property and threat offenses. For violations of physical integrity, cybercrime victims rated certain aspects more positively, namely the information provided about the offense and advice on preventing recurrence. They also indicated to a lesser extent that the impact increased due to the way the police handled their report. The finding that cybercrime victims dit not report lower satisfaction with their reporting experience does not align with expectations from previous research (Leukfeldt et al., 2018). Previous studies suggested that especially emotional needs would be less well addressed and that there would a lack of knowledge would occur more often (Leukfeldt et al., 2018). It is possible that since these earlier studies, the police have learned lessons and have taken

steps to improve their support for cybercrime victims. Another explanation for the absence of (negative) differences is that we surveyed victims of relatively common and 'simple' forms of cybercrime. Victims of less common or more complex types of cybercrime may be less satisfied (Leukfeldt et al., 2020). In addition, reporters of cybercrime may have lower expectations of the police, resulting in less dissatisfaction (Graham et al., 2020). Victims of cybercrime may also be more likely to accept that certain needs remain unmet due to self-blame (Leukfeldt et al., 2018). Moreover, we only surveyed those who reported to the police, which excludes victims who did not want to or were unable to report the offense.

6.6.3. The role of the police

Cross and colleagues (2016) observed that fraud victims primarily filed reports because of their need for retribution. Our study also shows that among property crime victims, the need for detection, arrest and prosecution of the perpetrator is the strongest. Yet it is precisely this investigative process that often proves challenging in cybercrime cases. However, if the police set realistic expectations, act in a procedurally just manner, and address other victim needs, this is not necessarily problematic: when procedures and decisions are perceived as fair, the outcome often matters less (Graham et al., 2020; Ten Boom et al., 2008). According to previous research, victims of property crime primarily seek compensation and have little need for emotional support (Ten Boom et al., 2008). However, our study shows that victims of property crime do indeed have emotional needs. In the cybercrime variants, some of these were expressed more strongly than in the traditional variants, indicating an important consideration for the police.

According to Terpstra and colleagues (2019), the police have become more 'abstract' since the transition to the National Police in 2013: more distant, formalized, less personal and direct, and more decontextualized, with effectiveness and efficiency as justifications. With cybercrime, this tendency manifests in the promotion of online reporting—a development that, according to Terpstra and colleagues (2019), further distances citizens from the police. Among the victims of property cybercrime who completed our questionnaire, 20.5% had filed their report online. Compared to those who reported in person (e.g., at a police station or by phone), they were significantly less satisfied with being able to share their story, the information they received about the offense, the prevention advice, the urgency with which the case was handled, the efforts made, and the information provided about the procedures (for detailed analyses, see the Intermezzo).

Although the option of internet reporting is important for victims who prefer it or who would otherwise refrain from reporting due to shame, there is a risk that victims will be 'pushed' toward internet reporting due to capacity constraints. However, the original intent of the police's omni-channel strategy is that citizens' contact preferences should guide interactions with the police (Politie, 2019). The ambition in the Security Agenda is that "the entire intake and reporting process of the police for cybercrime and digitized crime will be fully digitized and optimized on schedule by the end of 2026" (Ministerie van Justitie en Veiligheid, 2022: 14-15), which does not seem to align with the needs of victims of property cybercrime. Although computer systems can play a role in victim contact, direct human interaction remains indispensable for fully understanding and addressing emotional needs in sensitive situations such as victimization (Landman, 2023; Terpstra et al., 2019).

Although cybercrime is not classified as one of the so-called "High-Impact Crimes" (HIC), such as residential burglary and street robbery (Van Dijk et al., 2021), its impact is no less severe (Borwell et al., 2024). Moreover, we observed that the needs of victims of property cybercrimes (such as hacking of online bank accounts) are greater than those of victims of traditional property crimes (such as residential burglary). In the case of HIC offenses, the police provide a personal follow-up within two weeks, offer the option to file the report at the victim's home, and maintain regular contact with victims (Biemolt et al., 2012). An investigative case file is also always created (Openbaar Ministerie & Politie, 2021). Based on our findings, the police could consider applying such protocols to cybercrime cases as well, or reclassifying cybercrime as HIC. In 2024, the East Netherlands police unit introduced the "Digitale Meldkamer" (literal translation: "Digital Incident Response Room"), and other units are adopting the approach. Here, police officers visit cybercrime victims in person, if the victims wish (Hoed & Leeneman, 2023). The aim is to treat cybercrime victims as HIC victims, with corresponding attention and support from the police, given the comparable or even greater impact of cybercrime (Borwell et al., 2024; Hoed & Leeneman, 2023). The approach is still being evaluated, but appears to align well with our findings.

Our findings show that adequate support and treatment by the police is also of great importance for cybercrime victims. However, the police appear to pay less attention to them (Bijleveld et al., 2021; Button et al., 2022; Leukfeldt et al., 2018; Nieuwenhuizen & Van Huijstee, 2022; Notté et al., 2021). The Digital Incident Response Room may signal a change in direction. Although support for victims does not have to be provided exclusively by the police, the police do play an important role, as they often function as the initial point of contact. Moreover, victims consider

the police to be the appropriate party for providing support (Leukfeldt et al., 2018). That support may also include referral to other organizations, such as Victim Support Netherlands (Slachtofferhulp Nederland) or to services that specialize in removing images from the internet and cleaning infected computers (Leukfeldt et al., 2018). Currently, many 'police tasks' are already carried out by other organizations, and this, together with digitization, may lead to a rethinking of the role of the police (Bijleveld et al., 2021; Stol et al., 2024). Society also does not necessarily expect the police to solve all problems, as long as they clearly stand on the side of the public (Van der Vijver, 1993). An approach that does justice to the needs of cybercrime victims—which are at least as high as for an offense such as residential burglary—can contribute to police legitimacy and victims' willingness to report (Schreurs, 2020).

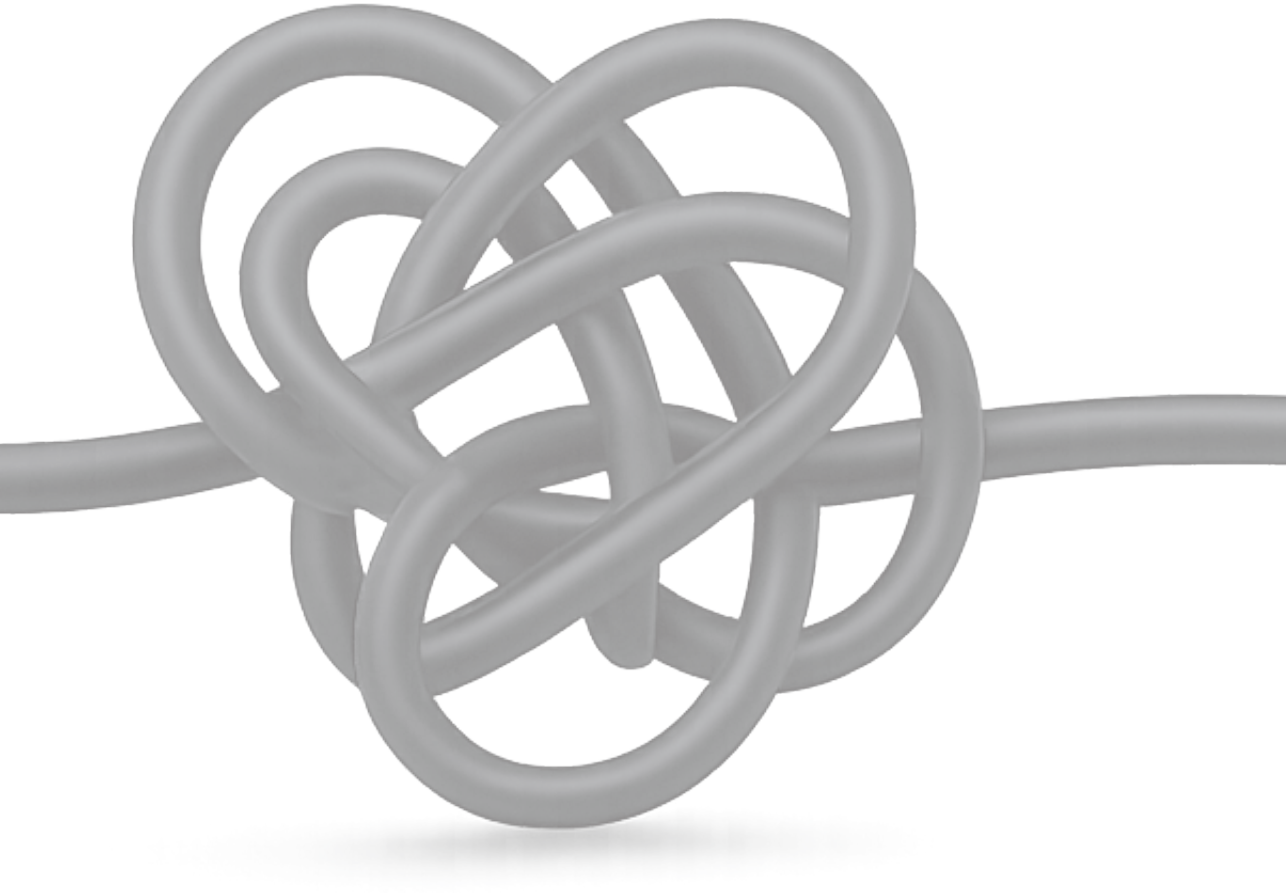
6.6.4. Limitations and future research

This study has several limitations that future research could address. As an initial step, it also provides a foundation for formulating hypotheses that can be tested in future studies to assess the robustness of the findings. Follow-up research may (also) focus on cybercrime victims who did not report the offense to the police, as previous studies suggest that their characteristics and experiences differ from those who do (De Kimpe et al., 2020; Van de Weijer et al., 2018). It is important to also map out the needs and experiences of this underrepresented group and examine how they can be supported in their recovery process, even when they are less likely to actively seek help from institutions such as the police—something we were not able to examine in this study, which focused on those who did report. In addition, future research could examine the influence of reporting experiences on victims' future willingness to report.

The absence of large effects of latent variables such as avoidability, self-efficacy and victim blaming may stem from limitations in how these constructs were measured. Follow-up studies could address this. In addition, victims of other types of offenses could be included, specifically more complex forms of cybercrime which the police may find more challenging to respond to. The reporting experiences and needs of these victims could be compared to those of victims of simpler cybercrime forms. Furthermore, additional predictors of needs should be examined, including more social factors—particularly in the case of person-centered offenses, where we found no strong associations. Future research could also explore the relationship between cybercrime victims' needs and the extent to which they are met in the reporting process. With the measurement method of the current study, it is possible that some needs are partly a result of the reporting experience itself, which can be better dis-

tinguished in this way. It is also important to pay attention to the specific needs of cybercrime victims, such as technical assistance (Button et al., 2020), or putting an end to the offense (Leukfeldt et al., 2020). Moreover, longitudinal follow-up research could provide insight into how victim needs develop over time (Dinisman & Moroz, 2017; Ten Boom et al., 2008).

Finally, interviews provide a richer picture of victims‘ needs and experiences (Leukfeldt et al., 2020). This is important, for example, for uncovering processes that may explain why victims of property cybercrime appear to have stronger needs than victims of traditional property crime. A qualitative follow-up study in which victims from the same population are interviewed would be of great added value in providing further interpretation of the differences in needs and reporting experiences between cybercrime and traditional crime victims.



Intermezzo

Reporting cybercrime online versus in-person: A comparison of victim experiences

I.1. Introduction

With the increasing trend toward digitalization in policing services, including greater reliance on online reporting systems, concerns have arisen about the reduction in personal interaction and emotional support for victims (Terpstra et al., 2019), especially in cases of cybercrime. The shift to digital reporting might diminish the perceived quality of victim support, as it reduces opportunities for empathetic, face-to-face interactions, which are often critical for victim recovery and satisfaction (Landman, 2023; Terpstra et al., 2019). As part of the broader focus on victims' experiences during the police reporting process (Chapter 6), this intermezzo examines how the method of reporting cybercrime—specifically, online versus in-person—shapes victims' evaluation of that process.

I.2. Methods

For this analysis, two types of financial cybercrime were selected—bank helpdesk fraud and hacking of online banking accounts—as online reporting is formally available for these offenses. In our financial cybercrime sample, 20.5% of the victims reported to the police online. Table I.1 presents an overview of the distribution of reporting methods.

Table I.1. Distribution of reporting channels among financial cybercrime victims

Method of reporting	*N*
At police station	176
At the crime scene	3
Via telephone	86
Via internet	71
Via 3D reporting desk	10
Other	9
Total	346

To assess differences in victim experiences, independent-samples *t* tests were performed, comparing those who reported online with those who reported in person, namely via telephone, 3D reporting desks, police stations, or at the 'crime scene'.

I.3. Results

The analysis, shown in Table I.2, reveals that victims who reported financial cybercrime online expressed lower satisfaction across several aspects of their reporting

Table I.2. T tests for mean differences in experience of internet vs. in-person reporting for financial cybercrime victims

Reporting experience[a]		Internet report (N = 71)		In-person report[b] (N = 275)
		M (*SD*)		*M* (*SD*)
Able to share story		3.89 (1.41)		4.64 (0.84)
	t		-4.33[c]	
	p		<.001**	
Information about the crime		3.15 (1.60)		4.26 (1.10)
	t		-5.49[c]	
	p		<.001**	
Prevention advice		2.96 (1.62)		3.97 (1.21)
	t		-4.95[c]	
	p		<.001**	
Police lacked knowledge		1.90 (1.61)		1.73 (1.53)
	t		1.11	
	p		.134	
Police underestimated impact		1.61 (1.02)		1.55 (1.03)
	t		0.39	
	p		.700	
Police blamed victim		1.34 (0.84)		1.22 (0.68)
	t		1.11[c]	
	p		.271	
Case treated as urgent matter		2.75 (1.42)		3.42 (1.39)
	t		-3.57	
	p		<.001**	
Police made sufficient effort		3.21 (1.45)		3.69 (1.29)
	t		-2.70	
	p		.007*	
Information about procedure		2.83 (1.67)		3.53 (1.44)
	t		-3.25[c]	
	p		.002*	
Impact decreased due to experience		2.99 (1.47)		3.42 (1.31)
	t		-2.44	
	p		.015	
Impact increased due to experience		1.69 (1.19)		1.55 (0.96)
	t		0.92[c]	
	p		.296	

* $p < .01$; ** $p < .001$ (two-sided).
[a]Scale 1 to 5; [b]Includes via telephone, at police station, at the crime scene, 3D reporting desk; [c]Equal variances not assumed.

experience compared to those who reported in person. Significant differences emerged in victims' perceptions of their ability to share their story, receiving information about the crime, receiving prevention advice, the urgency with which their case was treated, perceived effort by police, and information regarding procedural steps. There were no significant differences concerning perceptions of police knowledge, underestimation of impact, victim blaming, or whether the reporting experience led to a decrease or an increase in impact.

I.4. Conclusion

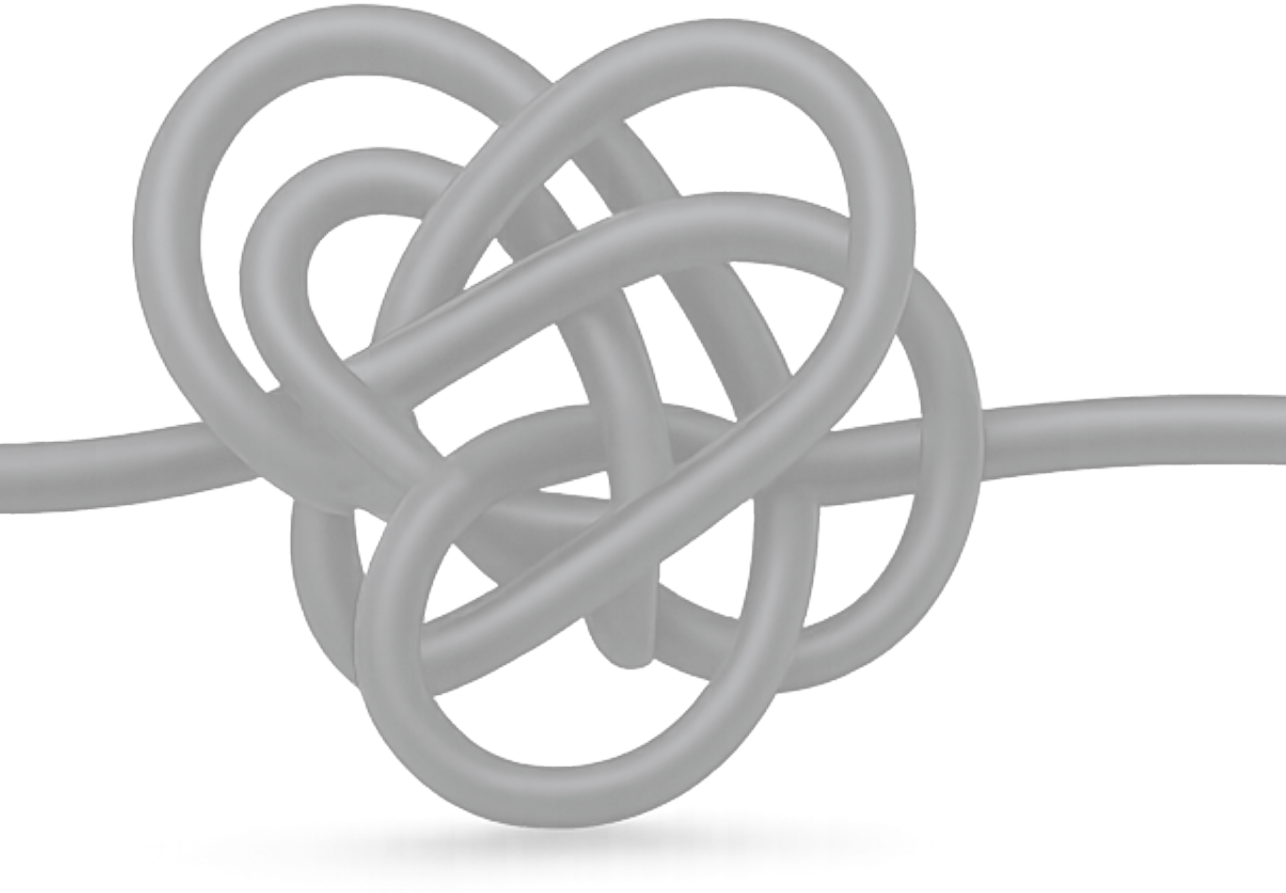
While online reporting can improve accessibility—particularly for victims hesitant to report crimes in person due to embarrassment, stigma, or logistical barriers—it currently results in less positive experiences. Victims may require personal interaction to feel adequately supported and heard during the reporting process. The results of the current analysis align with a study based on data from the Dutch Police Monitor (which includes items from the survey in Appendix 3 of this dissertation) that found lower satisfaction among crime victims who reported online (Jansen et al., 2024).

Dutch policy aims to fully digitize cybercrime reporting by 2026 (Ministerie van Justitie en Veiligheid, 2022). The findings raise concerns that, as online reporting increasingly replaces more personal forms of interaction—likely driven by growing pressure on police organizations to optimize resources—victims may not receive the support they need. Although the Dutch police's 'omni-channel strategy' formally seeks to prioritize citizens' preferred modes of contact (Politie, 2019), victims may, in practice, be steered toward online reporting. As illustrated by a survey respondent from the studies presented in Chapters 5 and 6—a victim of bank helpdesk fraud who lost between €10,000 and €50,000—this can come at the expense of feeling acknowledged and supported:

> "*I could not report it in person, it had to be online. […] I would have preferred reporting face-to-face, because I would have felt more heard.*"

In sum, the findings highlight the value of human interaction in cybercrime reporting. As digitization of police services continues, it is essential that victim-centered principles remain central. It may also be questioned whether it is appropriate to direct cybercrime victims back to the very environment in which the offense occurred (i.e., the internet), especially given their potentially damaged sense of online security (see Chapters 3 and 4). A more thoughtful approach to digital transformation is needed:

one that ensures efficiency gains do not come at the expense of emotional support, procedural clarity, or victims' sense of acknowledgment (Landman, 2023; Terpstra et al., 2019).



Chapter 7

General conclusion and discussion: The impact and needs of cybercrime victims and the implications for police practice

7.1. Introduction

Cybercrime is a high-impact crime that profoundly affects victims. This dissertation has shown that its emotional, psychological, and financial impact is mostly as severe as, or even exceeds that of traditional crimes such as residential burglary. While online offenses are frequently perceived as less serious by the police and the broader community, these findings challenge this assumption, emphasizing the need for improved victim support, awareness, and policy responses. To substantiate these conclusions, this chapter will reflect on the key findings of this dissertation and their implications. The central question of this dissertation is: "*What is the victim impact of cybercrime, and what does this mean for the role of the police?*"

Since the first sub-question of this dissertation concerns how to measure the victim impact of cybercrime and traditional crime—rather than the actual findings on that impact—this will only be briefly addressed here. Offenses were categorized into three main types: financial ('property') crime, person-centered crime, and violent/sexual crime, each encompassing various specific offenses. A victim-centered perspective guided the measurement of impact across psychological, financial, social, and physical dimensions. To assess victim impact, a comparative approach played a central role in this dissertation, pairing cybercrimes with traditional crimes that share similar characteristics, such as modus operandi and offender motivation. A further reflection on the methodologies is provided in Section 7.6, discussing limitations and future research directions.

Chapter 7 builds on the insights from the previous chapters to bring the main findings of this dissertation together. Chapter 1 provided an introduction to the study, outlining its scope and objectives. Chapter 2 outlined the strategies and frameworks used to assess impact, while Chapters 3 to 5 detailed the impact comparisons and key determinants, including crime-specific, personal and social factors. Chapter 6 compared the reporting experiences and needs of cybercrime and traditional crime victims, while also examining the factors that influence these needs. This final chapter synthesizes the dissertation's key findings by addressing its second and third sub-question in Section 7.2 and 7.3, offering insights and reflections. It then presents a theoretical reflection in Section 7.4, followed by practical recommendations for police and victim policies (7.5). The chapter concludes with a discussion of limitations and future research directions (7.6), and a forward-looking reflection on the evolving nature of cybercrime and its impact on victims (7.7).

7.2. Victim impact of cybercrime and comparison to traditional crime

Sub-question 2: What is the victim impact of cybercrime, and how does it compare to the victim impact of traditional crime?

7.2.1. Explaining the victim impact of cybercrime

This section starts with the victim impact of cybercrime and the factors that explain it before moving on to comparisons with traditional crime. To analyze cybercrime's victim impact, a dataset from Statistics Netherlands was used, including 2,415 cybercrime victims. The findings, detailed in Chapters 3 and 4, reveal that the psychological impact comprises two key components: *emotional well-being*, reflecting the direct impact on the emotional condition of the victim, and *cybercrime-related sense of security*, reflecting victims' sense of safety in the digital world. Several theoretical frameworks were applied to explain these impacts, including the shattered assumptions theory (SAT), the democratization of victimization, coping mechanisms, and cyborg theory. Although the theories will be discussed to some extent in this paragraph, a broader reflection on the theoretical frameworks is provided in Section 7.4.

The study described in Chapter 3 revealed that person-centered cybercrimes, such as stalking or threat, had a stronger impact on emotional well-being than financial cybercrime and hacking. In contrast, financial cybercrime and hacking had more impact on victims' sense of security, likely due to fear of repeat victimization and reduced trust in digital systems. Additionally, victims who knew the offender and those with lower socioeconomic status experienced more impact on emotional well-being. Financial compensation resulted in lower impact on emotional well-being. With this, the SAT demonstrated mixed results. While the SAT partially explained variations in emotional well-being, it did not explain variations in victims' sense of security. This suggests that emotional well-being reflects a more immediate and deeply personal impact fitting within the SAT's framework, whereas sense of security relates to cyber-specific concerns about digital safety and future risks, which the SAT is less equipped to predict.

Expanding on these findings, the study in Chapter 4 applied the cybercrime-specific frameworks of democratization of victimization and cyborg theory, and coping mechanisms to further examine the psychological impact of cybercrime. It explored both personal and circumstantial factors influencing emotional well-being and sense of security. Older individuals experienced a higher impact on their sense of security, likely due to lower digital literacy. Victims living alone and those with

lower socioeconomic status experienced a higher impact on their emotional well-being, underscoring the protective role of social support and resources, aligning with coping theory. Female victims reported a higher impact on their emotional well-being than men, although the impact on their sense of security was similar. Circumstantial factors also played a role. Device hacking—an invasive form of violation—resulted in higher psychological impact than account hacking, aligning with cyborg theory. Additionally, prolonged victimization intensified emotional distress, likely due to the continuous disruption of victims' lives and unresolved harm. No support was found for the democratization of victimization impact, as the impact varied across groups.

7.2.2. Comparing the impact of cybercrime and traditional crime

In Chapter 5, the victim impact of cybercrime was compared with that of traditional crime. Survey data was collected from 910 victims who reported one of eight crimes to the police: online and traditional forms of burglary (hacking of online bank account and residential burglary), scams (bank helpdesk fraud and doorstep deception), threat (online and offline threat), and violation of physical integrity (image-based sexual abuse and sexual assault). Victim impact was categorized into internalizing problems (e.g., anxiety, social withdrawal, and psychosomatic complaints), externalizing problems (e.g., anger, desire for retaliation, and fear of recurrence), damaged self-image (i.e., self-blame and shame), and financial impact (e.g., income loss and considerable damage). Additionally, peritraumatic stress, reflecting immediate reactions during or upon discovering the crime (e.g., shock, denial, and helplessness), was assessed. While internalizing and externalizing problems were similar across cybercrime and traditional crime categories, notable differences emerged for other impact types. Residential burglary led to more financial impact than online bank account hacking, yet cybercrime—except for threats, where no significant differences were observed—more severely affected victims' self-image. Furthermore, financial cybercrimes (hacking of online bank account and bank helpdesk fraud) resulted in higher levels of peritraumatic stress than their traditional counterparts. These findings challenge the assumption that crimes involving a physical component are inherently more serious (Palassis et al., 2021; Popham, 2021).

The study in Chapter 5 also examined the factors explaining victim impact across cybercrime and traditional crime, revealing many significant findings and a strong explanatory power. Notable differences between cybercrime and traditional crime emerged, for example regarding financial damage and damaged self-image. Greater direct financial loss was linked to increased self-image damage among cybercrime

victims—a pattern not observed for traditional crime victims. This suggests that financial victimization in the digital realm may carry a distinct psychological burden, possibly due to feelings of personal failure or embarrassment. Additionally, while financial compensation helped reduce internalizing problems and financial impact, it was less effective in alleviating damage to self-image for cybercrime victims. Damage to self-image, which was particularly pronounced among cybercrime victims, was most strongly associated with being misled by the offender, the possibility of avoidance of the crime in hindsight, neutralization/denial, and victim blaming. Furthermore, higher levels of victim blaming were linked to higher impact across all crime types, as were neutralization/denial, pre-existing psychological issues, lower education levels, lower self-efficacy, and recent victimization. The findings emphasize the interplay of crime-specific, personal and social factors that shape the impact of cybercrime, underlining the need for person-centered support strategies that extend beyond financial and practical aspects.

7.3. Implications for the role of the police

Sub-question 3: What implications does the victim impact of cybercrime have for the role of the police?

7.3.1. Needs and reporting experiences

Victim impact is closely linked to victims' needs: the higher the impact, the more support they require (Ten Boom et al., 2008). This section first examines the specific needs of cybercrime victims, followed by their experiences with reporting the crime. It then reflects on how the police's role can be adapted to more effectively address victim impact and support needs. More specific recommendations are provided in Section 7.5.

Chapter 6 shows that victim needs vary based on crime type, crime characteristics, impact, and personal and social factors. Victims of financial cybercrimes expressed stronger practical needs than their traditional counterparts, including the need for clear support routes, financial compensation, and prevention advice. This may be attributed to the technical complexity of the cybercrimes and the perceived lack of accessible resources (Button et al., 2020; Cross et al., 2016b; Stol, 2020). Additionally, emotional/social needs, namely the acknowledgment of the crime and concern for preventing victimization for others, were also more pronounced among victims of financial cybercrime compared to victims of financial traditional crime. In

contrast, victims of traditional person-centered crimes expressed stronger emotional needs, including being taken seriously as a victim and having someone to talk to. They also had a stronger need for the arrest and prosecution of the offender. The key determinants that were connected to victims' needs included the type of crime, as well as personal and circumstantial factors, namely age, gender, financial loss, and levels of peritraumatic stress. These findings suggest that victim support should be tailored based on crime-related, personal, and contextual factors, highlighting a potential role for the police in adapting their approach accordingly.

Cybercrime victims' experiences when reporting to the police were also assessed in Chapter 6, providing further direction on how the police role can be improved. Their experiences largely mirrored those of traditional crime victims, particularly in cases of financial crimes and threats. However, in offenses involving violations of physical integrity, cybercrime victims reported more positive experiences in specific areas, namely receiving information about the crime and advice on preventing recurrence. They also experienced less additional distress caused by police handling of their case. These findings contrast with prior studies (Leukfeldt et al., 2018; Notté et al., 2021), possibly indicating recent improvements in police responses to cybercrime, particularly for the common and relatively straightforward offenses included in this dissertation. Another possible explanation is that cybercrime victims approach the reporting process with lower expectations of police assistance, which could lead to less dissatisfaction. A previous study has shown that 67% of traditional theft victims expect the police to detect and arrest an offender, compared to 33% of cybercrime victims (Graham et al., 2020). Additionally, cybercrime victims' tendency toward self-blame may contribute to a greater acceptance of unmet needs (Leukfeldt et al., 2018). It is also important to note that this study did not include victims who were turned away when attempting to report cybercrime—an issue highlighted in previous research (Leukfeldt et al., 2020; Notté et al., 2021).

While these findings might seem to suggest some positive developments, they should not be interpreted as conclusive evidence that the police's role in cybercrime cases requires no improvement, given the other possible explanations. Furthermore, the satisfaction levels, measured on a scale of 0 to 4, predominantly fell between 2 and 3, thus clearly indicating room for improvement. Additionally, the differences in victim impact and needs identified in this dissertation emphasize the necessity of tailoring police responses to the challenges faced by cybercrime victims.

7.3.2. Implications for the role of the police

The findings underscore critical areas for improvement for the role of the police. Currently, cybercrime is not classified as a "High-Impact Crime" by the Dutch police (Van Dijk et al., 2021). The findings from Chapter 5 challenge this, revealing that the victim impact of cybercrime is mostly comparable to, or even surpasses, that of traditional crime. Particularly striking are the higher levels of peritraumatic stress experienced by financial cybercrime victims and the greater damage to self-image reported by victims of financial and sexual cybercrime compared to their traditional crime counterparts. While residential burglary leads to greater financial consequences than online bank account hacking, cybercrime victims report equal or higher levels of impact across all other dimensions.

These findings also challenge the perception that cybercrime primarily results in financial harm that can be remedied through compensation (Cross et al., 2016a; Jansen & Leukfeldt, 2018). To date, discussions around cybercrime have often focused on quantifiable metrics—such as the number of victims and financial losses—while overlooking its more intangible yet profound psychological consequences. A shift in perspective is needed, as recognizing these broader impacts could lead to different priorities in victim policies and legal frameworks. Increased awareness within the police and their partner organizations is important to ensure that victim support efforts align with the actual harm experienced. Furthermore, given the greater damage to self-image among cybercrime victims, police interactions should be particularly mindful of avoiding victim blaming in language or attitudes. Additionally, as demonstrated in Chapters 3 to 5, the impact varies depending on the nature of the crime, the victim, and the circumstances. This highlights the importance of providing personalized and thoughtful support to cybercrime victims to ensure effective assistance.

Regarding needs, Chapter 6 demonstrates that victims of financial cybercrime, on average, express higher practical and emotional needs than victims of traditional financial crime. While police efforts are primarily focused on investigation and prosecution—often with an increasing reliance on remote communication—victims report a strong need for emotional support, practical assistance, and guidance on preventing recurrence. Addressing these needs requires a shift in police strategies toward a more victim-centered approach, recognizing that the justice process is not solely about legal proceedings but also about recovery. Traditionally, criminal law has been structured around the perpetrator, with the legal system treating victims primarily as complainants who initiate proceedings (Van der Vijver, 1993). While victim support services have expanded, the overall framework remains offender-focused. For many victims, however, the justice process is an integral part of their recovery, and meaningful

support does not necessarily have to be legal in nature (Van der Vijver, 1993). This is particularly relevant for cybercrime victims, as the likelihood of offenders being identified and prosecuted is relatively low (Ruiter et al., 2023). As a result, victims often receive a standardized police notice that their case will not proceed, leaving them without support. To prevent this, police interactions should extend beyond the reporting process to address victims' specific needs. This can aid recovery, even when legal action is not an option.

Furthermore, as mentioned in Chapter 6, a notable finding is that victims who reported to the police online were less satisfied with the experience and procedure compared to those who reported in person (see Intermezzo). Given that the impact of cybercrime appears to be at least comparable to that of high-impact traditional crime, it should receive a similar level of urgency and attention. Initiatives such as the "Digitale Meldkamer" (literal translation: "Digital Incident Response Room"), which offers on-site support for cybercrime victims, demonstrate how police responses can be improved to better assist victims (Hoed & Leeneman, 2023). However, this does not mean that the police should handle all aspects of victim support. Referring victims to the appropriate resources or other organizations can often be the most effective approach. An integrated, multi-agency response, with external organizations collaborating with the police, is crucial for a more comprehensive support system. Ultimately, the police must offer empathetic yet realistic guidance—acknowledging the complexities of cybercrime investigations—while ensuring victims receive meaningful support beyond legal proceedings to address their diverse needs.

7.4. Theoretical considerations and contributions

This section reflects on the theoretical frameworks used to explore cybercrime victim impact, highlights their limitations, and suggests the need for new theoretical approaches. Two categories of theoretical models were used in this dissertation to gain insight into the impact on victims of cybercrime. These models provided a foundation for hypothesizing about impact and also guided the selection of explanatory variables. The first category included established theories of traditional crime, with particular focus on the shattered assumptions theory (SAT). This theory explains how victimization can disrupt core beliefs about control, predictability, and justice (Janoff-Bulman & Frieze, 1983; Vanderstraeten et al., 2012). In Chapter 3, the SAT demonstrated explanatory relevance for the more traditional impact domain of emotional well-being. Its applicability for explaining the cybercrime-specific impact on sense of security appeared limited. This discrepancy may reflect the necessity for

theoretical frameworks that incorporate digital-specific factors for cybercrime impact. Cybercrime's unique characteristics—such as its remoteness, anonymity, and digital complexity, as described in Chapter 2—may require theoretical models that account for these factors.

The second category encompasses theories specifically tailored to cybercrime victimization. Two frameworks emerged as particularly relevant: the cyborg theory and the democratization of victimization. The cyborg theory posits that the integration of digital devices in daily life creates an experiential fusion between humans and technology, leading individuals to perceive attacks on these devices as direct assaults on the self (Haraway, 1985; Longo, 2018; Van der Wagen & Pieters, 2018). In Chapter 3, this theory proved valuable in explaining psychological impact, particularly concerning the invasiveness of attacks and the duration of victimization. This underscores the importance of tailored frameworks to address the psychological consequences of cybercrime. However, further research is needed. For instance, future studies should determine whether victims with a stronger attachment to their devices experience higher impact. As society becomes increasingly intertwined with technology, this line of inquiry gains importance (Patgiri & Ahmed, 2016).

The concept of democratization of victimization, described in Chapter 4, posits an equal distribution of cybercrime victimization risks across groups (Jansen et al., 2013; Junger et al., 2017). While this does not necessarily imply that the impact of victimization is equally distributed, this dissertation expands on the democratization concept by analyzing whether cybercrime affects people equally. However, the findings did not support this. Instead, significant disparities were observed, with victim impact varying based on factors such as age, living situation, and socioeconomic status. These differences may stem from coping mechanisms, with more vulnerable individuals experiencing greater psychological impact. This dissertation's results suggest that while cybercrime victimization may affect a broad range of people, its consequences are unevenly distributed, depending on crime type, personal and circumstantial factors. This raises the question of whether democratization remains a meaningful concept in this context—if victims experience significantly different impacts, can we still regard this as true democratization of victimization?

Both the democratization of victimization theory and the cyborg theory align with aspects of the online disinhibition effect, particularly through the former's focus on status minimization and the latter's inclusion of dissociative imagination (Agustina, 2015; Suler, 2004). While the online disinhibition effect has primarily been studied in relation to offenders, its implications for victimization remain underexplored and require further research. For example, the asynchronicity of victim-perpetrator inter-

actions may intensify psychological impact by prolonging distress and uncertainty (Agustina, 2015). Apart from the further exploration of the online disinhibition effect, this dissertation highlights the value of further examining coping mechanisms and cyborg theory in understanding variations in victim impact. Specifically, the findings indicate that victims traditionally considered more vulnerable—such as those with lower social support, lower socioeconomic status, or older age—tend to experience higher psychological impact following cybercrime victimization. Coping theory can provide further understanding of how specific vulnerabilities influence cybercrime victim impact outcomes. Additionally, the degree of intrusiveness, such as whether the attack targeted a personal device or an online account and how long the victimization persisted, appears to influence impact, aligning with cyborg theory. Given these nuances, Chapter 5's comparison of cybercrime and traditional crime offers some further insights into how victim impact varies under different circumstances and crime types.

The findings from comparing the impact of cybercrime and traditional crime highlight the need for further theoretical and societal exploration of cybercrime victimization. The comparable impact of cybercrime when it comes to internalizing and externalizing problems, the greater damage to self-image, and the higher peritraumatic stress raise questions. For example, the specific characteristics of cybercrime, such as device-connectedness, the technical complexity of the crime, and the perceived distance between the offender and victim, warrant further investigation. It may be necessary to adapt existing theoretical frameworks to better capture the unique aspects of cybercrime victimization, particularly by exploring how cyber-specific factors mediate the relationship between victimization and its psychological impact. Moreover, the observation that the democratization of victimization does not extend to victim impact suggests the value of exploring resilience-based models, such as the stress and coping framework (Lazarus & Folkman, 1984), which has been minimally applied to cybercrime victimization (De Kimpe, 2020). Similarly, the coping mechanisms within the SAT could be explored further in relation to cybercrime, particularly the roles of government and other supportive agencies (Janoff-Bulman, 1985). The prominence of damaged self-image among cybercrime victims also points to the societal and relational influences on victim impact. Labelling theory could provide further insight into how societal perceptions and victim blaming may shape these experiences (Kenney, 2002).

A further theoretical contribution of this dissertation is the identification of 'new' victim impact categorizations, refining traditional classifications of psychological/emotional, physical, financial/material, and social/behavioral dimensions (Lamet &

Wittebrood, 2009; Mawby & Walklate, 1994; Shapland & Hall, 2007). The findings in Chapters 3 and 4 reveal two forms of psychological impact: emotional well-being and cybercrime-related sense of security, conceptually linked to crime-related *insecurity* (Berg & Johansson, 2016). This distinction highlights how cybercrime affects both immediate emotional states and perceptions of digital safety, a differentiation not commonly made in cybercrime impact studies.

Chapter 5 introduces internalizing problems, externalizing problems, financial impact, and damaged self-image as separate impact dimensions, allowing for a more nuanced categorization of victim experiences. Table 5.2 illustrates how these categories correspond to the initially anticipated dimensions of emotional/psychological, financial/material, physical, and social/behavioral impact. While internalizing and externalizing problems are well-established concepts in psychopathology (Achenbach et al., 2016), their application to cybercrime victimization remains underexplored. This distinction highlights that cybercrime-related psychological impact can manifest both inwardly (e.g., anxiety, depression, psychosomatic complaints) and outwardly (e.g., anger, fear of recurrence, revenge-seeking). Additionally, the identification of damaged self-image as an independent impact category highlights the role of self-blame and shame, which, although recognized in research on sexual and interpersonal violence, have received comparatively little attention in studies on cybercrime victimization. The new categorization provides a more nuanced framework for assessing victim experiences, moving beyond traditional models and emphasizing the need for targeted support strategies that address the diverse ways cybercrime victims experience harm. Further research is needed to explore the mechanisms underlying these impact dimensions, their interrelations, and how they develop over time.

Beyond theoretical considerations, the findings of this dissertation also raise important legal and policy questions about how cybercrime is classified and handled within the criminal justice system. A key issue is whether the tangible consequences of victimization (such as financial or physical damage) are sufficient to assess the severity of a crime, or if the focus should shift to the impact experienced by victims. Traditionally, criminal law centers on the perpetrator's actions, treating victims equally in principle (Dunn, 2007; Kunst, 2021). While legal systems do account for variations in tangible harm to some extent—for instance, more severe cases of assault may result in harsher penalties—the primary focus remains on the offense itself. If victim impact, rather than the mere fact of victimization, were to become a main criterion for determining crime severity, it could fundamentally alter policy and legal priorities. This taps into broader societal and political debates, including whether digitalization, with its often intangible effects, challenges how we categorize and prioritize

crimes. For instance, should the legal system place greater emphasis on the victim's psychological impact? And if so, how can this be integrated into the legal system while ensuring fairness and consistency in the treatment of cases? While answering these questions is beyond the scope of this dissertation, the following section offers some general recommendations for police and victim policies.

7.5. Recommendations for police and victim policies

This dissertation provides insights into how social and judicial responses to cybercrime victims can be improved, with a specific focus on the role of the police. For agencies to provide effective support, it is crucial to develop a thorough understanding of victims' experiences (Kunst et al., 2017). In addition to enhancing this knowledge by the research findings, the following sections present concrete recommendations to inform improvements in police practices and victim policies. This calls for coordination between the involved parties, with the police taking a leading or driving role.

Recommendation 1: Treat cybercrime victims as victims of "High-Impact Crime"

"High-Impact Crimes" (HICs) are typically defined by their severity and the significant impact they have on victims, leading to prioritization in police investigations and victim support services. In the Netherlands, traditional HICs include offenses such as residential burglary and street robbery, which are given special attention by law enforcement, such as ensuring personal follow-up within two weeks, offering reporting options at the victim's home, and the initiation of an investigation in every case (Openbaar Ministerie and Politie, 2021; Van Dijk et al., 2021). However, as far as can be determined from available policy documents, the classification of crimes as HIC or non-HIC is not informed by research regarding their actual impact on victims.

Based on the findings of this dissertation, it is worth reconsidering the exclusion of cybercrime from the HIC-classification. Victims of financial cybercrime, for example, experience peritraumatic stress levels that surpass those associated with traditional financial crimes, including those that are classified as HIC, namely residential burglary. Additionally, the damage to self-image is more profound for victims of financial cybercrime and image-based sexual abuse compared to the traditional counterparts. Practitioners and policymakers need to acknowledge the severity of cybercrime and allocate adequate resources to its investigation, prevention, and the provision of tailored victim support. This could include incorporating cybercrime victimization into existing frameworks for HICs, ensuring that victims receive appro-

priate moral and practical support. Such an approach would enhance the attention for cybercrime victims, improve reporting procedures, and facilitate better follow-ups. A victim-centered approach should be prioritized, with an emphasis on acknowledging the psychological harm caused by cybercrime and offering timely, tailored support.

Recommendation 2: Tailor cybercrime victim support to the type of cybercrime and its characteristics

This dissertation demonstrates that the impact of cybercrime affects both victims' emotional well-being and their sense of security in the digital environment, with the extent of the impact varying depending on the type of offense. As outlined in Chapter 3, person-centered cybercrimes (i.e., stalking, threats, and libel/slander) have a relatively high impact on emotional well-being, suggesting that emotional support is more important for victims of these crimes. In contrast, the impact of hacking and financial cybercrime (e.g., online banking fraud, identity fraud, and consumer fraud) on victims' sense of security within the digital environment is more substantial. For these offenses, interventions should prioritize restoring victims' perceptions of safety online and equipping them with strategies to prevent future victimization. The findings also indicate that the pervasive and intangible nature of these cybercrimes can increase feelings of vulnerability and fear of re-victimization. The police and other agencies involved with cybercrime victims, such as victim support services, specialized helplines and advisory organizations, banks and insurers, should provide tailored support that addresses the distinct emotional and digital-specific impact of each type of cybercrime.

The characteristics of a certain cybercrime can also significantly influence the experienced victim impact, and victim support can be important in addressing these effects. For example, Chapter 3 revealed higher psychological impact for victims whose devices were hacked compared to those with hacked accounts. This was also true for victims of cybercrimes with a longer duration (see Chapter 4). Addressing such invasive circumstances can serve as key areas for intervention. This could include quickly notifying individuals of account misuse or data breaches, a responsibility that could be shared between the police and other stakeholders, such as national cyber security authorities, cybersecurity companies and internet service providers (Jhaveri et al., 2017). Furthermore, preventing financial loss and offering loss compensation are important in mitigating both psychological and financial impact. As demonstrated in Chapters 3 and 5, financial compensation is linked to lower internalizing, externalizing and financial problems, and to lower impact on emotional well-being. On the other

hand, higher financial losses are linked to heightened financial impact, externalizing problems, and damaged self-image. Beyond minimizing the damage, the implementation of a specialized program for compensating cybercrime victims, analogous to existing schemes for victims of violent crimes (Kunst et al., 2017; Piquero, 2018), could help facilitate recovery and reduce the adverse consequences of victimization.

These suggestions are in line with recent strategic directions outlined by the Dutch police. The Strategic Agenda for 2025–2030 emphasizes the need for 'meaningful follow-up,' particularly in the context of scarce investigative resources. It calls for interventions that extend beyond prosecution, ensuring that victims have access to alternatives for formal reporting that match their needs (Politie, 2025, p. 27) The insights from this dissertation may support the development of such victim-centered alternatives.

Recommendation 3: Prioritize prevention and support for cybercrime victims most vulnerable to severe impact

Prevention and support measures should focus on (potential) cybercrime victims who are particularly vulnerable to experiencing severe impact. This dissertation identified several factors that contribute to heightened impact. As discussed in Chapter 3, victims with lower socioeconomic status experience greater impact on their emotional well-being. Chapter 4 further identifies people living alone, women, and religious individuals as particularly affected in terms of emotional well-being, while elderly victims report more impact on their cybercrime-related sense of security. Chapter 5 identifies additional factors associated with higher impact, including neutralization or denial by the victim, pre-existing psychological issues, repeat victimization, lower education levels, reduced self-efficacy, and being female. To address these findings, prevention and support strategies should adopt a more targeted approach. Prevention efforts should focus on reducing the likelihood of victimization for high-risk groups ('secondary prevention'), while people who have been victimized already should be supported in minimizing further harm and preventing repeat victimization ('tertiary prevention'). These efforts can include awareness campaigns, specialized support programs, improved victim notification processes, and increased collaboration with online platforms to implement preventative measures.

Recommendation 4: Address the practical and emotional needs of financial cybercrime victims

Chapter 6 reveals that victims of financial cybercrime report higher emotional, social, and practical needs compared to victims of traditional crimes, yet they often receive less support (Bijleveld et al., 2021; Button et al., 2022; Leukfeldt et al., 2018; Notté et al., 2021). To address this gap, law enforcement and partner organizations such as banks and support organizations must expand their focus beyond legal procedures and financial restitution, incorporating emotional and practical support into their response to ensure that victims are supported in their recovery. Victim policies should incorporate support frameworks that streamline referrals between organizations, provide practical resources, and focus on preventing repeat victimization. Given that cybercrime offenders frequently remain unidentified (Ruiter et al., 2023), support should extend beyond legal procedures, prioritizing victims' well-being over securing case outcomes (Graham et al., 2020; Ten Boom et al., 2008). It has been demonstrated that asking individuals about their expectations from the police during initial contact is an effective approach (Van Dijk & Hoogewoning, 2018). Additionally, Chapter 6 highlights that certain victim characteristics influence the level of support required: women report greater emotional needs, older individuals—especially in cases of financial cybercrime—require more practical assistance, and financial losses exacerbate nearly all identified needs. Furthermore, peritraumatic stress during the crime also plays a significant role in shaping victims' support needs. Therefore, police responses should provide personalized assistance, while upholding fair treatment for all victims.

Recommendation 5: Prioritize self-image restoration for cybercrime victims and prevent secondary victimization

The damage to self-image was found to be more pronounced among victims of financial cybercrime and image-based sexual abuse compared to victims of the traditional counterparts, as shown in Chapter 5. This supports previous research indicating that cybercrime victims often experience high levels of guilt and shame (Cross, 2015; Leukfeldt et al., 2018; Notté et al., 2021). Damaged self-image was most strongly associated with misleading actions by the offender, avoidance possibility, neutralization/denial and victim blaming, factors that appeared particularly pronounced among cybercrime victims. In response, police and other stakeholders should actively work to restore victims' self-image. A helpful approach may involve emphasizing that cybercrime affects many people, that victims are not at fault, and supporting them in regaining their sense of agency (Cross, 2015; Powell et al., 2019).

Public awareness campaigns can also be instrumental in validating victims' experiences, combating victim blaming, and reducing stigma. Fostering an environment where cybercrime victims are recognized and supported, both within their personal circles and by society at large, can act as a protective factor (Maercker & Horn, 2012). In addition to public campaigns, direct interactions with victims—whether by police officers, bank employees, victim support organizations, or other professionals—should prioritize empathy and avoid language that might unintentionally reinforce self-blame. Frontline staff should be trained to offer a supportive, non-judgmental response to prevent victim blaming and secondary victimization.

Recommendation 6: Evaluate and adapt reporting processes to meet cybercrime victims' impact and needs

The shift toward online reporting for cybercrime victims does not appear to meet their needs, as financial cybercrime victims report lower satisfaction with this experience compared to victims who reported in person (see Chapter 6 and Intermezzo). This aligns with previous research showing that victims who experience higher emotional impact prefer in-person reporting (Boekhoorn & Tolsma, 2016). Currently, crimes categorized as High-Impact Crime (HIC) by the Dutch police are not eligible for online reporting (Boekhoorn & Tolsma, 2016). However, this dissertation demonstrates that the psychological impact of cybercrime can exceed those of traditional HICs, specifically residential burglary. Consequently, the online reporting process for cybercrime victims requires re-evaluation. While maintaining an online reporting option remains important, integrating opportunities for direct contact with a police officer could enhance victims' experience—for example, by allowing victims to complete their report through alternative channels. Furthermore, a promising approach is the aforementioned project "Digital Incident Response Room", which treats cybercrime victims similarly to victims of traditional HICs, including on-site visits. This project is currently under evaluation, but appears to align with the impact and needs of cybercrime victims identified in this dissertation. Expanding pilot programs and exploring new strategies to support cybercrime victims and enhance their reporting experiences should be prioritized by the police.

7.6. Limitations and future research directions

While this dissertation provides valuable insights, several limitations should be acknowledged, which could be addressed in future research. Firstly, an important

limitation is the predominantly quantitative approach of this dissertation. Although this method has provided a strong foundation for understanding the impact, needs, and reporting experiences of cybercrime victims, qualitative research is needed to explore the underlying mechanisms and provide a deeper, more nuanced understanding of victims' experiences. Future qualitative studies could investigate why cybercrime victims experience higher damage to self-image or why financial cybercrime victims report higher peritraumatic stress than their traditional counterparts. Additionally, research could explore whether victim blaming extends beyond the victim's immediate environment and what factors drive the perception of being blamed. Another important avenue for exploration is understanding why factors such as financial loss and pre-existing psychological issues seem to significantly influence all aspects of victim impact. Furthermore, qualitative research could provide insights into why financial cybercrime victims report higher emotional, social, and practical needs. Finally, it would be valuable to assess whether cybercrime victims' seemingly comparable or even more positive reporting experiences genuinely reflect improvements in police responses or if they stem from factors such as lower expectations or feelings of self-blame.

Secondly, although Chapters 3 and 4 addressed cybercrime-related sense of security, this dissertation devoted relatively little attention to cybercrime-specific impacts and needs. This omission is particularly evident in Chapters 5 and 6, where the primary focus was on comparing cybercrime with traditional crime and examining 'general' impact types and needs that apply to both online and offline contexts. Cyber-specific factors, such as confidence in computer skills, which previous research suggests may play a key role in shaping the impact of cybercrime (Virtanen, 2017), received little attention. The same is true for cybercrime-specific needs, such as taking images offline or restoring computer systems (Leukfeldt et al., 2018). Similarly, impact types that are unique to the online environment, such as a diminished sense of online safety and restrictions on freedom of expression, were not extensively explored. Future studies should prioritize understanding and explaining these cybercrime-specific elements to gain insight into and better support victims of cybercrime.

Thirdly, this dissertation has some limitations regarding its scope. It primarily distinguishes between purely cyber and purely traditional crimes, yet many offenses blend online and offline elements (Notté et al., 2021; Weulen Kranenbarg & Van 't Hoff-de Goede, 2023). These hybrid crimes, especially person-centered offenses involving both digital and physical harassment, may intensify victim impact and should be explored in future research (Leukfeldt & Van 't Hoff-de Goede, 2023). Additionally, since this dissertation focuses on the Dutch context, its findings may not

fully apply to other countries. Police responses, prevalent cybercrimes, and financial compensation systems differ internationally, warranting broader, international research. Certain demographic groups were also not considered, as only victims aged 18 and above were included. The impact on victims' social circles was not examined, despite evidence that crime can create anxiety even among those indirectly exposed (Dinisman & Moroz, 2017; Mawby & Walklate, 1994). This also applies to individuals who have experienced attempted cybercrimes, as exposure to threats like phishing emails can cause impact even without direct victimization (Bluhm et al., 2022). Furthermore, the study covered a limited range of cyber-dependent crimes, leaving less understood offenses, such as malware and technical hacking, as areas for future research. Lastly, while several factors influencing victims' needs were explored, they did not strongly explain the variations observed. Future research should also further examine the links between victim impact, needs, and reporting experiences.

Fourthly, this dissertation relies on cross-sectional data, while longitudinal research is needed to understand how the impact and needs of cybercrime victims evolve over time and to better establish causal effects. It is acknowledged that victims undergo various stages of recovery following victimization, with some impacts, such as diminished trust in others, potentially persisting for years (Bonanno et al., 2011; Frieze et al., 1987; Jansen & Leukfeldt, 2018; Shapland & Hall, 2007). While this dissertation addressed temporal aspects by surveying victims up to 15 months post-incident, this approach does not fully capture the dynamic nature of recovery or delayed effects such as PTSD (Dunn, 2007; Kunst, 2010). Cybercrimes with ongoing consequences, such as the prolonged availability of personal details or images online, further underscore the necessity of tracking victims over extended periods using within-person data (Janssen et al., 2021). Building upon prior longitudinal studies (Sipma & Van Leijsen, 2019), future research could clarify both short- and long-term impacts, and establish causal links between explanatory factors, victim impact, needs, and reporting experiences.

Fifthly, this dissertation has limitations because of its reliance on existing data and the selection of victims from police records. The secondary data used in Chapters 3 and 4 were not specifically designed to explain victim impact, limiting their explanatory potential. Additionally, the victims surveyed in Chapters 5 and 6 were drawn from police data, which introduces selection effects. Not all victims are captured in these records, such as those who refrain from reporting due to self-blame or those discouraged to report by the police. Given the relatively low cybercrime reporting rates and the self-selection biases inherent in police reports (Agustina, 2015; Akkermans et al., 2024; Moitra, 2005; Van Wilsem et al., 2021; Wall, 2005), this sample does not represent the full spectrum of cybercrime victims. Prior studies

have indicated that non-reporting victims often possess different characteristics and experiences compared to those who report (De Kimpe et al., 2020; Van de Weijer et al., 2018). Future studies could address these issues by including non-reporting victims recruited through alternative methods. This approach would offer a more comprehensive understanding of the experiences and impact of non-reporting victims, as well as insights into how best to support them.

Sixthly, the findings of this dissertation are situated within a specific time frame, notably partly during the COVID-19 pandemic. The unique social and institutional circumstances introduced by the pandemic may have influenced both victim impact and responses by law enforcement. For instance, the transition to remote interactions resulted in an increased reliance on telephone reporting by the police, which might have affected victims' perceptions of reporting experiences. Furthermore, this period may have led to heightened emotional vulnerability and disrupted traditional support systems (Foster Campbell & Papacharissi, 2021).

Finally, it is important to note that cybercrime is an evolving phenomenon, driven by continual digital advancements (Hamby et al., 2018; Riek, 2017). This requires ongoing research into these developments, including the impact, needs and experiences of victims. Cybercriminals perpetually refine their methods, adapting to new technologies and exploiting emerging vulnerabilities. These advancements, in turn, influence victim experiences. For example, the increasing integration of AI and the proliferation of virtual worlds are reshaping how people engage with the online environment, potentially altering the nature and impact of cybercrime, but also the police response (Bellini, 2024; Landman, 2023). In anticipation of these developments, the next paragraph will explore future trends in cybercrime and victimization.

7.7. What lies ahead in cybercrime and its impact on victims

As this dissertation reaches publication, an increasing portion of human activity is shifting online, and reliance on technology is expected to grow even further. This trend is exemplified by the exponential growth in data volume, the launch of new websites, and the advancements in the Internet of Things, Artificial Intelligence (AI) and Cloud Computing (Landman, 2023; Patgiri & Ahmed, 2016). These advancements are opening new, and in some cases still unknown, opportunities for cybercriminals to exploit data and target victims. This is particularly true with emerging technologies, such as quantum computing.

The increasing sophistication of technology might result in an increase in the number of cybercrime victims, as cybercriminal tactics become more sophisticated

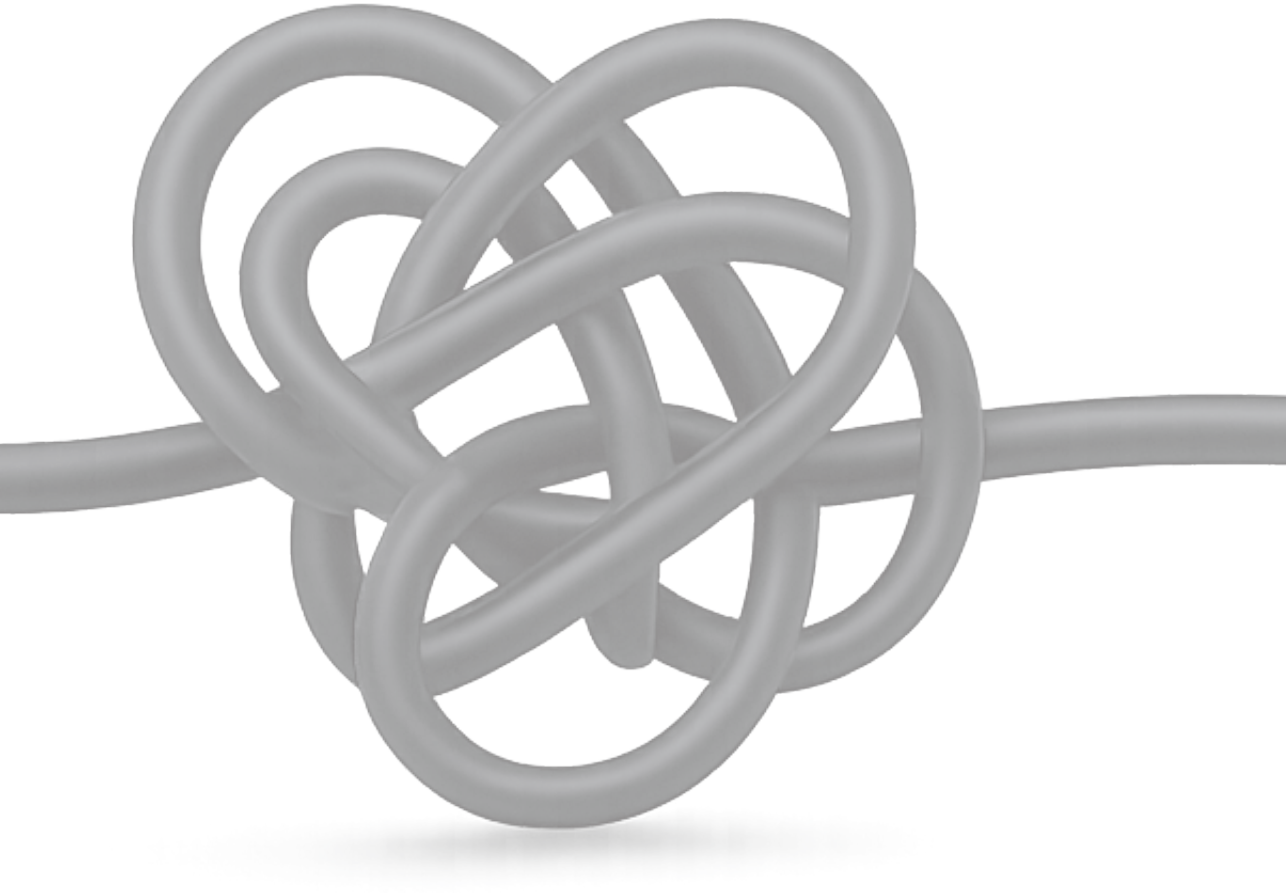
and deceptive (Palassis et al., 2021). The development of AI has the potential to significantly reshape the nature and scope of cybercrime, leading to the emergence of new crime types or the transformation of existing ones, and potentially resulting in changes to victim experiences (Landman, 2023). Some types of offenses discussed in this dissertation may be replaced or overshadowed by emerging offenses. Moreover, the role of technology in facilitating intimacy and social connections, particularly since the COVID-19 pandemic, has grown (Foster Campbell & Papacharissi, 2021). The increasing integration of technology into personal identity and interactions, facilitated by social media and similar platforms, might influence the experience of cybercrime for its victims, although this relationship remains to be fully explored.

At the same time, a countertrend is emerging, as seen in school smartphone bans driven by concerns over digitalization's effects (Böttger & Zierer, 2024). While technology remains deeply integrated, shifts in policy, regulation, or cultural attitudes could still influence its trajectory. This reflects a dynamic recognized already in 1934 by Mumford in Technics and Civilization, who emphasized that technological development is not linear but shaped by social, cultural, and moral forces that can redirect or constrain its course (Mumford, 2010).

The emergence of virtual worlds, often referred to as the 'metaverse,' may gain increasing importance in the future, heightening the need for understanding victim experiences within these environments. The metaverse is defined as "a massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence" (Ball, 2022, p. 29). It blurs the boundaries between digital and physical realities, aligning with the cyborg theory, which emphasizes the evolving relationship between humans and technology (Haraway, 1985). This evolution brings new challenges, including the emergence of harmful behaviors such as virtual sexual assault (Landman, 2023; Strikwerda, 2014). A notable case involved a female researcher who, while exploring "Horizon Worlds," was allegedly virtually assaulted within an hour of logging in, with others observing and passing a virtual bottle of vodka (Bellini, 2024). The use of hand controllers that vibrated upon contact intensified the assault experience, something that is also reported by users of 'haptic vests' that allow the wearer to feel physical sensations of what happens to the avatar (Bellini, 2024). This phenomenon, known as 'embodiment,' creates an illusion of ownership and agency over the virtual body. Current legislation has not yet adequately addressed these acts, as traditional sex crime laws do not apply to the metaverse, leaving victims without legal resources (Bellini, 2024). As technologies continue to evolve, it is important to further explore their implications for crime, victimhood, and justice.

The future of technology and its potential influence on cybercrime is constantly evolving, with emerging trends providing insight into what may lie ahead. One such trend is the increasing use of implantable medical devices, such as cardiac pacemakers and in vivo biosensors, which are connecting more individuals to technology and, in some cases, creating literal cyborgs—blends between humans and machines (Haddow, 2021). This transition not only redefines our relationship with technology but also brings new and complex risks, including cybersecurity threats. A notable illustration is the concern raised by former United States Vice President Dick Cheney, who, fearing hacking threats, requested the disabling of all wireless signals from his implanted defibrillator (Browning & Tuma, 2015). Furthermore, there has been an increase in individuals connecting technology to their bodies, as exemplified by the growing popularity of smartwatches (Sen et al., 2020) and non-medical implanted chips (Niininen et al., 2024). While these advancements offer convenience, they also introduce vulnerabilities, such as hacking and cloning.

This dissertation has demonstrated the profound impact of cybercrime, revealing how victims experience damage to their self-image, high peritraumatic stress, and significant emotional and practical needs. It has also identified key risk factors that exacerbate victim impact, such as lower socioeconomic status, age, repeat victimization, and psychological vulnerabilities. These findings demonstrate the necessity for law enforcement and policymakers to develop tailored, victim-centered responses that extend beyond legal procedures. As this dissertation underscores the urgency of addressing current cybercrime harms, it is equally important to recognize that emerging online threats will affect victims in yet unforeseen ways (Leukfeldt et al., 2020). As Max Weber noted in 1917, scientific progress is inherently transient—each discovery will be surpassed, although it serves as a stepping stone to new questions and further refinements (Weber, 2009). The rapidly evolving nature of cybercrime means that today's insights and solutions must be continuously reassessed and adapted. This dissertation contributes to that ongoing process by providing a deeper understanding of current cybercrime victim impact and laying the groundwork for more effective interventions. In doing so, it not only addresses present challenges but also informs future research and policy. This contributes to victim support systems that need to exhibit some of the same dynamics and flexibilities as the cybercrimes they aim to address.



References

Achenbach, T. M., Ivanova, M. Y., Rescorla, L. A., Turner, L. V., & Althoff, R. R. (2016). Internalizing/externalizing problems: Review and recommendations for clinical and research applications. *Journal of the American Academy of Child & Adolescent Psychiatry*, *55*(8), 647–656. https://doi.org/10.1016/j.jaac.2016.05.012

Agnew, R. S. (1985). Neutralizing the impact of crime. *Criminal Justice and Behavior*, *12*(2), 221–239. https://doi.org/10.1177/0093854885012002005

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

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. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., & Moons, E. (2024). *Veiligheidsmonitor 2023* [Safety monitor 2023]. Statistics Netherlands (CBS).

Akkermans, M., Kloosterman, R., Moons, E., Reep, C., & Tummers-Van der Aa, M. (2022). *Veiligheidsmonitor 2021* [Safety monitor 2021]. Statistics Netherlands (CBS).

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.

Arends, J., Derksen, E., & Morren, M. (2025). *Online criminaliteit en veiligheid 2024*. Statistics Netherlands (CBS).

Averdijk, M. D. E. (2010). *Individuals' victimization patterns over time* [Doctoral dissertation]. Vrije Universiteit Amsterdam.

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyber-attacks. In V. Benson & J. McAlaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Elsevier.

Ball, M. (2022). *The metaverse: And how it will revolutionize everything*. Liveright Publishing.

Barlow, J. P. (2019). A declaration of the independence of cyberspace. *Duke Law & Technology Review*, *18*(1), 5–7.

Bellini, O. (2024). Virtual justice: Criminalizing avatar sexual assault in Metaverse spaces. *Mitchell Hamline Law Review*, *50*(1), 3.

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

Berenblum, T., Weulen Kranenbarg, M., & Maimon, D. (2019). Out of control online? A combined examination of peer-offending and perceived formal and informal social control in relation to system-trespassing. *Journal of Crime and Justice*, *42*(5), 616–631. https://doi.org/10.1080/0735648X.2019.1692424

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. https://doi.org/10.1111/1467-9477.12069

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

Bijleveld, C., Salet, R., Damstra, A., & Stéfanovic, D. (2021). *Politiefunctie in een veranderende omgeving* [The police function in a changing environment]. Wetenschappelijke Raad voor het Regeringsbeleid.

Bluhm, K., Borwell, J., & Stol, W. (2022). De slachtofferimpact van cybercrime versus traditionele criminaliteit: Aanknopingspunten voor slachtofferzorg en preventieprioriteiten [The impact of cybercrime versus traditional crime on victims: Starting points for victim support and prevention priorities]. *Tijdschrift Voor Veiligheid*, *21*(3–4), 13–31. https://doi.org/10.5553/TvV/.000045

Blumer, H. (1954). What is wrong with social theory? *American Sociological Review*, *19*(1), 3–10.

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.

Boekhoorn, P., & Tolsma, J. (2016). *De aangifte van delicten bij de multichannelstrategie van de politie* [Crime reporting in the police's multichannel strategy]. Politie & Wetenschap; BBSO; Radboud Universiteit.

Bonanno, G. A., Westphal, M., & Mancini, A. D. (2011). Resilience to loss and potential trauma. *Annual Review of Clinical Psychology*, *7*(1), 511–535. https://doi.org/10.1146/annurev-clinpsy-032210-104526

Borwell, J., Jansen, J., & Stol, W. (2018). Human factors leading to online fraud victimisation: Literature review and exploring the role of personality traits. In J. McAlaney, L. Frumkin, & V. Benson (Eds.), *Psychological and behavioral examinations in cyber security* (pp. 26–45). IGI Global.

Borwell, J., Jansen, J., & Stol, W. (2021a). Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research*, *3*(3), 85–110.

Borwell, J., Jansen, J., & Stol, W. (2021b). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review*, *40*(4), 933–954. https://doi.org/10.1177/0894439320983828

Borwell, J., Jansen, J., & Stol, W. (2024). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology*, *31*(1), 156–181. https://doi.org/10.1177/02697580241282782

Borwell, J., Schuppers, K., Rooyakkers, J., & Harteveld, A. (2020). Het cybercrimebeeld van de Nederlandse politie: Van algemeen beeld naar verdiepende analyse en aanpak [The cybercrime picture of the Dutch police: From general overview to in-depth analysis and approach]. *Cahiers Politiestudies*, *3*(56), 39–62.

Böttger, T., & Zierer, K. (2024). To ban or not to ban? A rapid review on the impact of smartphone bans in schools on social well-being and academic performance. *Education Sciences*, *14*(8), 906. https://doi.org/10.3390/educsci14080906

Brands, J., & Van Wilsem, J. (2019). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*, *18*(2), 213–234. https://doi.org/10.1177/1477370819839619

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

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. https://doi.org/10.1111/j.1467-6494.1986.tb00391.x

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

Browning, J. G., & Tuma, S. (2015). If your heart skips a beat, it may have been hacked: Cybersecurity concerns with implanted medical devices. *South Carolina Law Review*, *67*, 637–677.

Budimir, S., Fontaine, J. R. J., Huijts, N. M. A., Haans, A., Loukas, G., & Roesch, E. B. (2021). Emotional reactions to cybersecurity breach situations: Scenario-based survey study. *Journal of Medical Internet Research*, *23*(5), e24879. https://doi.org/10.2196/24879

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., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021a). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 101675. https://doi.org/10.1016/j.tele.2021.101675

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021b). Victims of cybercrime: Understanding the impact through accounts. In M. W. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context: The Human Factor in Victimization, Offending, and Policing* (pp. 137–156). Springer.

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*, 36–54. https://doi.org/10.1057/sj.2012.11

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, *25*(2), 670–691. https://doi.org/10.1177/17488958221128128

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

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. https://doi.org/10.1111/rego.12125

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. https://doi.org/10.1186/s40163-019-0099-7

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

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. https://doi.org/10.1177/0269758015571471

Cross, C. (2018). (Mis)understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*, *13*(6), 757–776. https://doi.org/10.1080/15564886.2018.1474154

Cross, C., Richards, K., & Smith, R. (2016a). *Improving responses to online fraud victims: An examination of reporting and support*. Australian Institute of Criminology.

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

De Kimpe, L. (2020). *The human face of cybercrime: Identifying targets, victims, and their coping mechanisms* [Doctoral dissertation]. Universiteit Gent.

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 formal and informal support by victims of cybercrime]. *Cahiers Politiestudies*, *3*(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.

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., Toutenhoofd-Visser, M. H., & Stol, W. P. (2009). *Werkaanbod cybercrime bij de politie: Een verkennend onderzoek naar de omvang van het geregistreerde werkaanbod cybercrime* [Cybercrime workload at the police: An exploratory study into the volume of registered cybercrime workload]. Lectoraat Cybersafety, Noordelijke Hogeschool Leeuwarden.

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 types of crime]. 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.

Faubert, C., Décary-Hétu, D., Malm, A., Ratcliffe, J., & Dupont, B. (2021). Law enforcement and disruption of offline and online activities: A review of contemporary challenges. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context: Vol. I* (pp. 351–370). Springer International Publishing. https://doi.org/10.1007/978-3-030-60527-8_19

Finkelhor, D., Turner, H., & Colburn, D. (2023). Which dynamics make online child sexual abuse and cyberstalking more emotionally impactful: Perpetrator identity and images? *Child Abuse & Neglect*, *137*, 106020. https://doi.org/10.1016/j.chiabu.2023.106020

Foster Campbell, J., & Papacharissi, Z. (2021). Intimacy in the Time of COVID-19. *Journal of Digital Social Research*, *3*(2), 1–9. https://doi.org/10.33621/jdsr.v3i2.84

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

Gini, G., Card, N. A., & Pozzoli, T. (2018). A meta-analysis of the differential relations of traditional and cyber-victimization with internalizing problems. *Aggressive Behavior*, *44*(2), 185–198. https://doi.org/10.1002/ab.21742

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

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249.

Graham, A., Kulig, T. C., & Cullen, F. T. (2020). 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

Graves, J. T., Acquisti, A., & Anderson, R. (2019). Perception versus punishment in cybercrime. *The Journal of Criminal Law and Criminology (1973-)*, *109*(2), 313–364.

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.

Haddow, G. (2021). *Embodiment and everyday cyborgs: Technologies that alter subjectivity*. Manchester University press.

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). Palgrave Macmillan Cham.

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.

Hoed, S., & Leeneman, R. (2023). *Digitale meldkamer, afhandeling digitale criminaliteit* [Digital control room, handling of digital crime]. Politie Eenheid Oost-Nederland.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

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

Horsman, G. (2017). Can we continue to effectively police digital crime? *Science & Justice*, *57*(6), 448–454. https://doi.org/10.1016/j.scijus.2017.06.001

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* (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. https://doi.org/10.1111/j.1540-4560.1983.tb00138.x

Jansen, J., Leukfeldt, E. R., Kerstens, J., Veenstra, S., Van Wilsem, J., & Stol, W. (2013). Victimization in a digitized society and chances for prevention. In W. Stol & J. Jansen (Eds.), *Cybercrime and the Police* (pp. 29–43). Eleven International Publishing.

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. https://doi.org/10.21428/88de04a1.976bcaf6

Jansen, R. P., Ruiter, S., & Van Steden, R. (2024). Crime reporting and victim satisfaction with the police: A large-scale study among victims of crime in the Netherlands. *Crime Science*, *13*(]), 30. https://doi.org/10.1186/s40163-024-00231-9

Janssen, H. J., Oberwittler, D., & Koeber, G. (2021). Victimization and its consequences for well-being: A between- and within-person analysis. *Journal of Quantitative Criminology*, *37*, 101–140. https://doi.org/10.1007/s10940-019-09445-6

Jhaveri, M. H., Cetin, O., Gañán, C., Moore, T., & Eeten, M. V. (2017). Abuse reporting and the fight against cybercrime. *ACM Computing Surveys*, *49*(4), 68. https://doi.org/10.1145/3003147

Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in europe. *Proceedings of the International Conference On Cyber Situational Awareness, Data Analytics And Assessment*, 1–8. https://doi.org/10.1109/CyberSA.2017.8073391

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

Kenney, J. S. (2002). Victims of crime and labeling theory: A parallel process? *Deviant Behavior*, *23*(3), 235–265. https://doi.org/10.1080/016396202753561239

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

Koning, L., Junger, M., & Veldkamp, B. (2024). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International Review of Victimology*, *30*(3), 443–479. https://doi.org/10.1177/02697580231215839

Kunst, M. J. J. (2010). *The burden of interpersonal violence: Examining the psychological aftermath of victimisation* [Doctoral dissertation, Tilburg University]. Tilburg University Research Portal.

Kunst, M. J. J. (2021). Knowing from where to start: A plea for more and better systematic literature reviews about the effectiveness of legal rights for crime victims. *International Journal of Comparative and Applied Criminal Justice*, *45*(1), 115–125. https://doi.org/10.1080/01924036.2020.1719529

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

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. https://doi.org/10.1177/0886260515596535

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. https://doi.org/10.1002/jts.21774

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).

Landman, W. (2023). *Politiewerk aan de horizon: Technologie, criminaliteit en de toekomst van politiewerk* [Policing on the horizon: Technology, crime, and the future of police work]. Politie & Wetenschap.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer.

Leukfeldt, E. R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities* [Doctoral dissertation]. Open University.

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (Marijke). (2020). Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders*, *15*(1), 60–77. https://doi.org/10.1080/15564886.2019.1672229

Leukfeldt, E. R., Notté, R., & 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: A study on needs, consequences, and responsibilities following victimization of cybercrime and digitized crime]. WODC.

Leukfeldt, E. R., & Van 't Hoff-de Goede, S. (2023). Slachtofferschap van online criminaliteit [Victimization of online crime]. In J. Van Doorn, J. Brands, M. J. J. Kunst, E. R. Muller, & L. Van Reemst (Eds.), *Slachtoffers: Onderzoek, beleid en praktijk* [Victims: Research, policy and practice] (pp. 249–269). Wolters Kluwer.

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

Littleton, H. L. (2010). The impact of social support and negative disclosure reactions on sexual assault victims: A cross-sectional and longitudinal investigation. *Journal of Trauma & Dissociation*, *11*(2), 210–227. https://doi.org/10.1080/15299730903502946

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., & Horn, A. B. (2012). A socio-interpersonal perspective on PTSD: The case for environments and interpersonal processes: Socio-interpersonal perspective on PTSD. *Clinical Psychology & Psychotherapy*, *20*(6), 465–481. https://doi.org/10.1002/cpp.1805

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

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

Ministerie van Justitie en Veiligheid. (2022). *Veiligheidsagenda 2023-2026* [Safety agenda 2023–2026]. Ministerie van Justitie en Veiligheid.

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, ISSN*, *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. https://doi.org/10.1109/MSP.2015.107

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? *Proceedings of the 2013 European Intelligence and Security Informatics Conference*, 31–37. https://doi.org/10.1109/EISIC.2013.12

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

Mumford, L. (2010). *Technics and civilization*. University of Chicago Press.

Mumtaz, S. (2019). Future of victimized employees: A model based on long-run cascading effects of experienced victimization. *Deviant Behavior*, *40*(7), 835–850. https://doi.org/10.1080/01639625.2018.1442655

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.

Nieuwenhuizen, W., & Van Huijstee, M. (2022). Online ontspoord: Naar een beter begrip van schadelijk en immoreel gedrag online [Online off track: Toward a better understanding of harmful and immoral online behavior]. *Cahiers Politiestudies*, *1*(62), 141–162.

Niininen, O., Singaraju, S., & Arango, L. (2024). The Human RFID Implants Introduce a New Level of Human-Computer Interaction: Twitter Topic Detection Gauges Consumer Opinions. In V. Jeseo & J. Allen (Eds.), *Welcome to the new normal: Life after the chaos* (pp. 122–136). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-49039-2_12

Norris, F. H., & Kaniasty, K. (1991). The psychological experience of crime: A test of the mediating role of beliefs in explaining the distress of victims. *Journal of Social and Clinical Psychology*, *10*(3), 239–261. https://doi.org/10.1521/jscp.1991.10.3.239

Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, *27*(3), 272–294. https://doi.org/10.1177/02697580211010692

Office for National Statistics. (2021). *Crime in England and Wales: Year ending September 2020*. Office for National Statistics.

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies*, *8*(4), 298–309. https://doi.org/10.1080/17450128.2012.752119

Openbaar Ministerie & Politie. (2021). *Screenings- en selectiviteitskader misdrijven* [Screening and selectivity framework for criminal offenses]. Landelijk Platform VVC OM-Politie.

Ozili, P. K. (2023). The acceptable R-square in empirical modelling for social science research. In C. A. Saliya (Ed.), *Social research methodology and publishing results: A guide to non-native english speakers* (pp. 134–143). IGI Global.

Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological impact of hacking victimization. *SAGE Open*, *11*(4). https://doi.org/10.1177/21582440211061556

Patgiri, R., & Ahmed, A. (2016). Big Data: The V's of the Game Changer Paradigm. *Proceedings of the 18th International Conference on High Performance Computing and Communications*, 17–24. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0014

Pemberton, A. (2011). Just-world victimology: Revisiting Lerner in the study of victims of crime. In H. Morosawa, J. J. P. Dussich, & G. F. Kirchhoff (Eds.), *Victimology and human security: New horizons* (pp. 45–69). Wolf Legal Publishers.

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.

Piquero, N. L. (2018). White-collar crime is crime: Victims hurt just the same. *Criminology & Public Policy*, *17*(3), 595–600. https://doi.org/10.1111/1745-9133.12384

Politie. (2019). *Politie in verbinding: Werken aan nieuwe contacten tussen burgers en politie* [Police in connection: Working on new contacts between citizens and police]. Politie.

Politie. (2025). *Stevig staan in deze tijd: Strategische agenda politie 2025-2030* [Standing strong in the present day: Strategic agenda police 2025-2030]. Politie.

Popham, J. F. (2021). Assessing the detrimental impact of cyber-victimization on self-perceived community safety. In M. Weulen Kranenbarg & E. R. Leukfeldt (Eds.), *Cybercrime in Context: The human factor in victimization, offending, and policing* (pp. 103–122). Springer Nature.

Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Computers in Human Behavior*, *92*, 393–402. https://doi.org/10.1016/j.chb.2018.11.009

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*(10), 1290–1304. https://doi.org/10.1080/01639625.2019.1612980

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* [Doctoral dissertation]. Westfälische Wilhelms-Universität 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), tyy004. https://doi.org/10.1093/cybsec/tyy004

Rosoff, H., Cui, J., & John, R. (2014). Behavioral experiments exploring victims' response to cyber-based financial fraud and identity theft scenario simulations. *Proceedings of the 10th Symposium On Usable Privacy and Security*, 175–186.

Ruiter, S., Van Leuken, M., Van Ruitenburg, T., Schiks, J., & Leukfeldt, R. (2023). *In- en doorstroom van online criminaliteit in de strafrechtsketen* [Entry and progression of online crime cases in the criminal justice chain]. WODC.

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

Schreurs, W. (2020). Waarom melden burgers? Individuele, sociale en institutionele drijfveren voor meldgedrag in het verleden en toekomstige meldingsbereidheid [Why do citizens report? Individual, social, and institutional drivers of past reporting behavior and future reporting willingness]. *Tijdschrift Voor Veiligheid*, *19*(2–3), 8–28.

Sen, S., Maity, S., & Das, D. (2020). The body is the network: To safeguard sensitive data, turn flesh and tissue into a secure wireless channel. *IEEE Spectrum*, *57*(12), 44–49. https://doi.org/10.1109/MSPEC.2020.9271808

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/10.1177/026975800701400202

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* [Searching in the dark: An exploration of sources and methods to measure 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

Staats, W., Meerts, C., Kleemans, E. R., & Huisman, W. (2021). *Nieuwe manieren van samenwerken. Een systematische literatuurreview naar de (effectiviteit van) publiek-private samenwerking op het gebied van financieel-economische criminaliteit en cybercrime* [New ways of cooperation: A systematic literature review on (the effectiveness of) pubic-private partnerships in the field of financial and economic crime and cybercrime]. Vrije Universiteit.

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

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

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 (CBS).

Statistics Netherlands (CBS). (2019). *Digitale veiligheid & criminaliteit 2018* [Digital safety & crime 2018]. Statistics Netherlands (CBS).

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

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

Stol, W. (2022). Digitalisering en maatschappelijke veiligheid. In R. Spithoven, M. Vanderland, L. Klijer-Kool, F. Vorenkamp, E. De Pauw, J. Wildenburg, & B. Nissen (Eds.), *Basisboek integrale veiligheid* (pp. 105–126). Boom Criminologie.

Stol, W., Jansen, J., & Landman, W. (2024). Digitalisering en de politiefunctie: Hoe het speelveld verandert en wat dat van de politie vraagt [Digitization and the police function: How the playing field is changing and what it demands of the police]. *Tijdschrift Voor Veiligheid*, *23*(1–2), 53–70.

Stol, W. P., van Treeck, R., & van der Ven, A. (1999). *Criminaliteit in cyberspace* [Crime 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* [Doctoral dissertation]. University of Twente.

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

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.

Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2013). *Using multivariate statistics*. Pearson.

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

Terpstra, J., Fyfe, N. R., & Salet, R. (2019). The Abstract Police: A conceptual exploration of unintended changes of police organisations. *The Police Journal: Theory, Practice and Principles*, *92*(4), 339–359. https://doi.org/10.1177/0032258X18817999

Toutenhoofd-Visser, M., Veenstra, S., Domenie, M., Leukfeldt, E., & Stol, W. (2009). *Politie en cybercrime—Intake en eerste opvolging: Een onderzoek naar de intake van het werkaanbod cybercrime door de politie* [Police and cybercrime—Intake and initial follow-up: A study on how the police handle incoming cybercrime workload]. NHL Hogeschool.

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(4), 710–729. 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 Andel, W., & Joosten, M. (2017). *Inwoners van Nederland naar leeftijd, geslacht, etniciteit en stedelijkheid, 2016* [Residents of the Netherlands by age, gender, ethnicity, and degree of urbanization]. Statistics Netherlands (CBS).

Van Bourgondien, C. M. J. (2017). *Jaarverslag 2017 Programma Dienstverlening* [2017 annual report Service Program]. 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?]. *Cahiers Politiestudies*, *1*(46), 33–48.

Van de Ven, P. (2022). *The role of social support in the aftermath of victimization: Interpersonal aspects of coming to terms with a victimization experience* [PhD Thesis]. Tilburg University.

Van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, 486–508. https://doi.org/10.1177/1477370818773610

Van der Plas, T., Kuilaars, G., & Geveke, H. (2022). Nederlandse politie en ketenpartners onderzoeken noodzakelijke ontwikkelsprongen voor versnelling in digitale transformatie [The Dutch police and criminal justice system partners explore necessary development leaps to accelerate digital transformation]. *Cahiers Politiestudies*, *1*(62), 63–82.

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 provision in the context of the police]. *Cahiers Politiestudies*, *1*(46), 19–32.

Van Dijk, B., Van Soomeren, P., Jongejan, A., & Krom, M. (2021). *Basisboek ProHIC: Probleemgericht werken aan High Impact Crime* [ProHIC basic handbook: Problem-oriented work on High Impact Crime]. Boom Criminologie.

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

Van Kesteren, J. (2009). Public attitudes and sentencing policies across the world. *European Journal on Criminal Policy and Research*, *15*(1–2), 25–46. https://doi.org/10.1007/s10610-009-9098-7

Van Wilsem, J., Sipma, T., & Meijer-van Leijsen, E. (2021). Show me the money! Identity fraud losses, capacity to act, and victims' efforts for reimbursement. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in context: The human factor in victimization, offending, and policing* (pp. 123–136). Springer.

Vanderstraeten, B., Mestdagh, K., Vanfraechem, I., & Aertsen, I. (2012). Slachtofferschap bij diefstal in woningen [Victimization in residential burglary]. *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 *Cybercrime en de politie* [Cybercrime and the police] (pp. 77–90). Boom Lemma uitgevers.

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law*, *24*(3), 323–338. https://doi.org/10.1080/13218719.2017.1315785

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.

Walrave, M., & Van de Heyning, C. (2022). De beelden waren de druppel: Waarom beelden van seksuele misdrijven online gedeeld worden vanuit sociaalwetenschappelijk en juridisch perspectief [The images were the last straw: Why images of sexual crimes are shared online from a socio-scientific and legal perspective]. *Cahiers Politiestudies*, *1*(62), 163–189.

Weber, M. (2009). *From Max Weber: Essays in sociology* (H. H. Gerth & C. W. Wright Mills, Eds.). Routledge.

Weulen Kranenbarg, M., & Van 't Hoff-de Goede, S. (2023). Online criminaliteit in criminologisch perspectief: Recente ontwikkelingen in het onderzoek naar daders en slachtoffers van online criminaliteit. *Tijdschrift Voor Criminologie*, *65*(4), 400–419. https://doi.org/10.5553/TvC/0165182X2023065004002

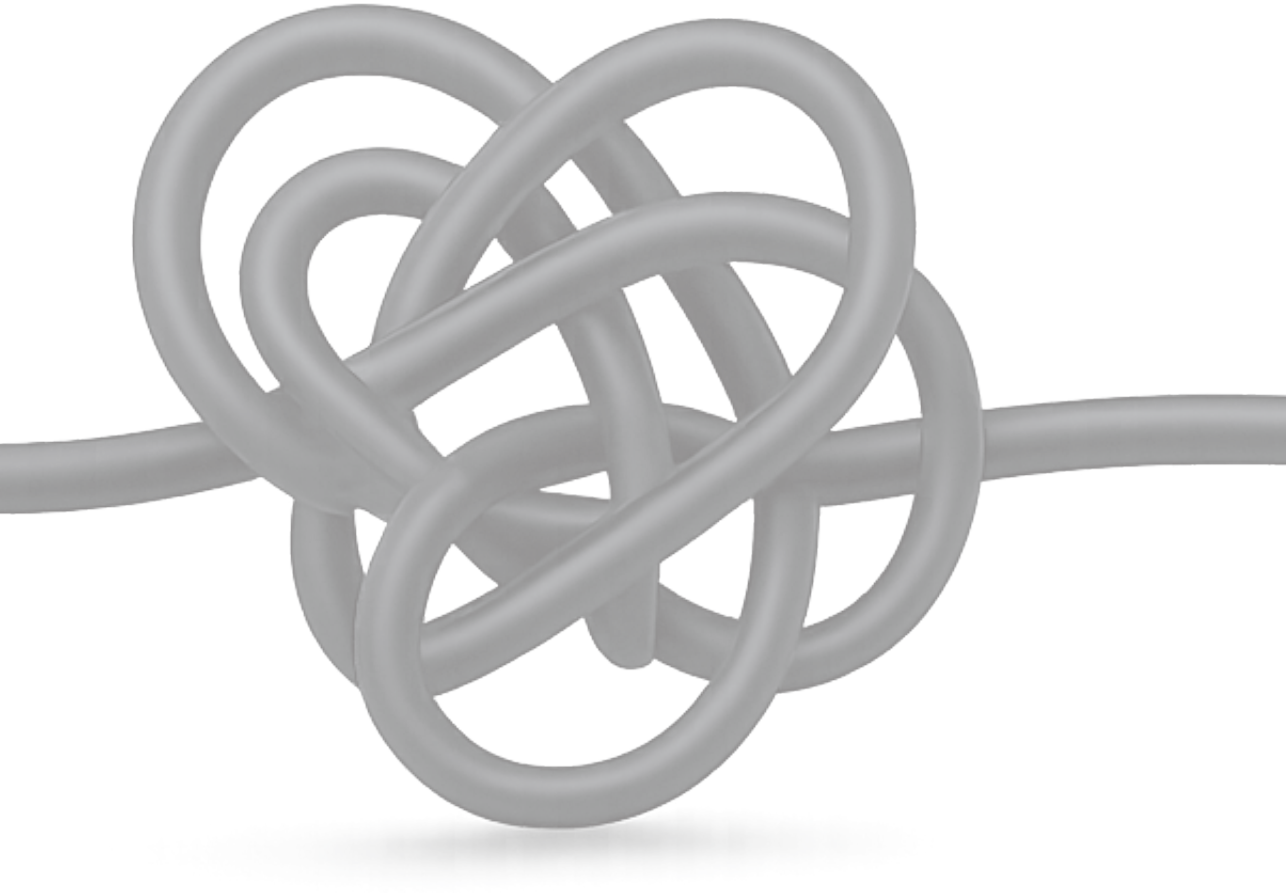
Whitty, M. T. (2015). Mass-marketing fraud: A growing concern. *IEEE Security & Privacy*, *13*(4), 84–87. https://doi.org/10.1109/MSP.2015.85

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. https://doi.org/10.1177/1748895815603773

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. https://doi.org/10.1093/oxfordjournals.bjc.a014258

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

References



Appendices

Appendix 1. Variations in impact by cybercrime type – Chapter 4

A.1.1. Impact by age and crime category

We performed two additional one-way between-groups ANCOVA tests, to discover whether the results differed by cybercrime type (hacking, person-centered and financial cybercrime). For emotional well-being, there were significant differences between the age groups. The impact of hacking increases with age, while the impact of person-centered cybercrime was highest for people aged 36 to 50 and decreases afterwards, see Figure A.1.1. Financial cybercrime has the most impact for the group aged 66 and over and is relatively stable in the other groups. The one-way between-groups ANCOVA test showed no significant results for sense of security. The differences by crime type may explain the non-significant effect for the age groups in total.

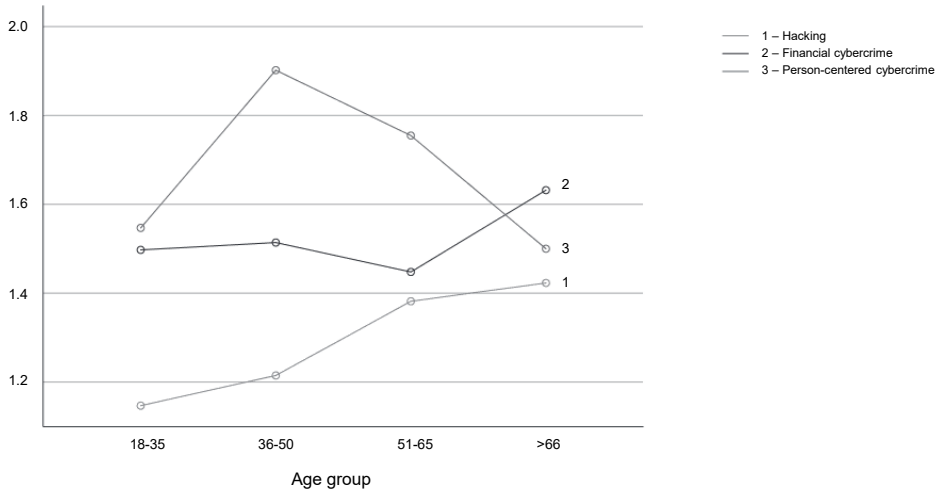


Figure A.1.1. Mean emotional well-being per age group and crime category.

A.1.2. Impact by household situation and crime category

Additional one-way between-groups ANCOVA tests which included household situation and crime type did not result in any additional statistically significant differences.

A.1.3. Impact by gender and crime category

We conducted additional one-way between-groups ANCOVA tests with gender and crime category. The results showed that person-centered cybercrime had a higher

impact on the emotional well-being of women than of men, see Figure A.1.2. There were no significant results for sense of security.

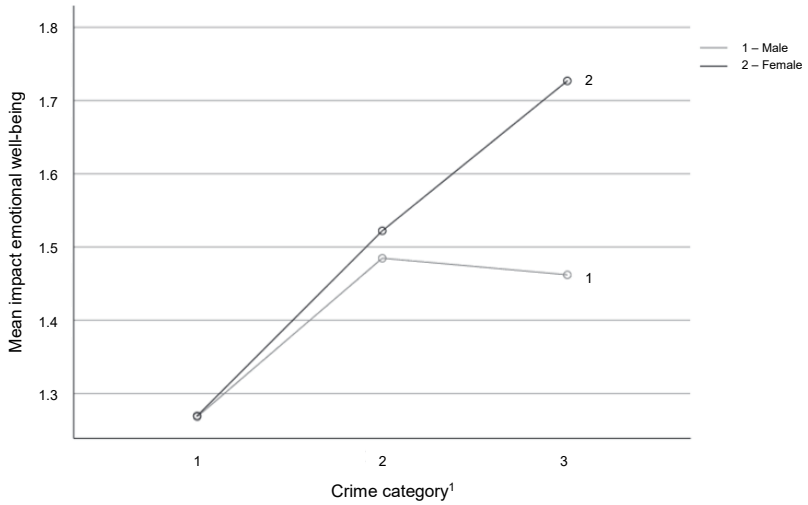


Figure A.1.2. Mean emotional well-being for women and men per crime category.
[1] 1: hacking; 2: financial cybercrime; and 3: person-centered cybercrime.

A.1.4. Impact by origin and crime category

Additional one-way between-groups ANCOVA tests with origin showed no significant differences for the identified cybercrime types either.

A.1.5. Impact by religion and crime category

When we conducted additional one-way between-groups ANCOVA tests with religion, no differences were found for the three cybercrime types.

Appendix 2. Survey design and data collection – Chapters 5 and 6

A.2.1. Victim selection criteria and procedure per crime type

In order to identify victims relevant for this study, we extracted samples from the Dutch police records repository known as the "Basisvoorziening Informatie" (BVI). Our sampling strategy encompassed both official police reports ("aangiftes") and general incident reports ("meldingen")[16]. Official reports initiate formal criminal prosecution, whereas general reports notify the police of an incident. This dual approach was adopted to mitigate potential selection bias as victimization can be reported in either way. The extraction process involved employing the Cognos and BlueIntel software platforms. Cognos enables searches within the BVI police records, allowing us to filter based on dates, police categories, and specific queries (Borwell et al., 2018). BlueIntel functions as an online crime categorization system, utilizing the "National Cybercrime Query" to identify online crime cases within the BVI. The resulting reports are subsequently classified by the Dutch National Police Intelligence Service. We utilized some of these classifications for the current study. Prior to the actual victim selection, we tested the sampling of police registrations and the selection of relevant victims per crime type. Based on this, minor procedural adjustments were implemented.

For cybercrime offenses, an assessment was conducted to ensure they aligned with the definition of cybercrime, following the approach suggested by Montoya and colleagues (2013). 'Hybrid' crime forms were excluded from our analysis, such as bank helpdesk fraud involving physical presence at a victims' home. For traditional offenses, we additionally examined whether they fell outside the definition of cybercrime. In some instances, cases involving simultaneous commission of another offense were included, but only when the intended offense was one of the primary offenses or the primary offense reported. Offenses related to the other discerned crimes were generally not included, except in cases where hacking of an online bank account preceded bank helpdesk fraud, with bank helpdesk fraud clearly identified as the main offense. In cases where ambiguity could arise about the selection, decisions were recorded to ensure consistency in subsequent cases. The precise definitions and selection methods for the specific offense types are presented below.

[16] We have employed Dutch terminology to align with the Dutch police systems and to present our exact queries. We translated directly into English where this was evident and fitting to enhance comprehensibility and readability.

A.2.1.1. Burglary

Within the burglary category, we encompassed victims of residential burglary and hacking into an online bank account. In both crime types, something is broken into—either a physical residence or a digital account. The primary motivation behind these cases is typically financial gain. Victims and researchers sometimes draw parallels between cybercrime and residential burglary (Button et al., 2021, 2022; Jansen and Leukfeldt, 2018; Palassis et al., 2021), heightening the interest in comparing the actual impact experienced by victims. The victims in the police reports are included when a physical home or digital bank account has been illicitly accessed or compromised, leading to the theft of possessions or unauthorized money transfers, even if the subsequent damage was compensated or the bank intervened to block a payment.

Residential burglary. Our definition of residential burglary partly aligns with article (art.) 311 of the Dutch Penal Code (Sr) (aggravated theft). It pertains to theft within a dwelling by an unauthorized individual, without the knowledge or permission of the rightful owner. This definition excludes theft from an enclosed yard surrounding a home, unless specific circumstances like an indoor garage are present. Selection was conducted through Cognos, targeting police records categorized under "theft in/out of home (qualified)" and assessing their compatibility with the definition.

Hacking of online bank account. The hacking of an online bank account refers to the illicit intrusion into a victim's digital banking environment. Typically, this begins with phishing, a technique involving false identities and persuasion tactics—social engineering—to obtain the victim's login credentials (Rooyakkers and Weulen Kranenbarg, 2020). The two primary variations of this offense are as follows: 1) payment request fraud, wherein the perpetrator poses as a buyer on an online market place and persuades a seller (the victim) to make a small money transfer or undergo identity verification. Subsequently, the victim is directed to a phishing website to capture their details for unauthorized account access; and 2) phishing through email or SMS impersonating trusted entities like banks or reputable organizations. Again, the victim is led to a phishing site to input their information. We selected online crime reports categorized as "fraud with bank data/internet banking" in BlueIntel, excluding reports with the labels "bank helpdesk fraud", "government helpdesk fraud", "safeguard" and "safe", as these refer to bank helpdesk fraud.

A.2.1.2. Scam

In the scam category, we chose doorstep deception and bank helpdesk fraud. These two offenses share a common thread of employing social engineering, manipulat-

ing victims through misrepresentation (Cross, 2015). Doorstep deception occurs in face-to-face interactions, while bank helpdesk fraud employs ICT (telephone and internet). In both instances, the motive behind the offense is financial gain. Our selection criteria encompass cases where money was actually defrauded or property was stolen, even if eventual compensation was provided. Additionally, victims for whom bank payments were blocked were included; the key criterion was the transfer of money from the victim's account.

Doorstep deception. Doorstep deception is a method commonly used to commit theft from a home or from a person. As defined by the Dutch Center for Crime Prevention and Safety (CCV), doorstep deception involves an offender using an excuse or falsehood to gain entry to a victim's home, with the intent of committing theft (Centrum voor Criminaliteitspreventie en Veiligheid (CCV), n.d.). Notably, our selection criteria also encompass instances of 'doorstep' deception occurring in public areas with the aim of theft. This includes cases where distractions are employed to facilitate pickpocketing (e.g., dropping an item and excusing themselves; asking for a cigarette). To identify relevant cases, we employed the query babbeltru* OR "babbel tru*" OR "babeltru*" OR "babel tru*" with Cognos to search the police database ("babbeltruc" is the Dutch term for doorstep deception). When this approach did not yield sufficient cases, we expanded our selection including the specified crime categories "theft with violence" and "theft without violence", with modes operandi labelled "distracting/luring attention"; "false name/qualification"; "calling/speaking/touching"; "gift/promises"; "switcheroo/handiness".

Bank helpdesk fraud. Bank helpdesk fraud involves scammers impersonating Dutch banks or government entities such as the Ministry of Justice and Security or the Supreme Court. These offenders engage victims over the phone, fabricating issues with their bank accounts (Politie, n.d.). They might claim to have detected suspicious transactions or that the victim is a target of identity fraud. Victims are then coerced into transferring their funds to purportedly secure accounts, safe deposit accounts, or taking action to prevent further harm, often under the guise of blocking payments or identifying the culprits. However, the funds are redirected to accounts controlled by criminals. Often, a remote access tool is employed to infiltrate victims' computers. To identify bank helpdesk fraud cases, we selected cybercrime reports categorized in BlueIntel as "fraud with bank data/internet banking", "helpdesk fraud" and "telecom fraud", with the labels "bank helpdesk fraud", "government helpdesk fraud", "safeguard" and "safe". Registrations categorized as "collect" or "courier" were omitted due to the physical elements associated with these cases.

A.2.1.3. Threat

The inclusion of the threat category in our study enables a comparative analysis between cyber and traditional person-centered offenses. Threat occurs widely across both separate contexts, presenting an opportunity for differentiation that might be less straightforward with other person-centered offenses such as stalking or defamation/libel. Furthermore, the motivation and modus operandi between the online and offline variants often exhibit minimal differences, making it suitable for a meaningful comparison. Additionally, the same legal article applies to both scenarios. In our study, the term "threat" pertains to offenses falling within the penal definition, encompassing threats of murder, rape, openly committing violence against individuals or property, aggravated assault, hostage-taking, or arson (art. 285 Sr). Satisfying this criterion involves the threatened individual experiencing a reasonable fear of the threat's realization, that the perpetrator's intention was to cause that fear, and the victim being aware of the threat (Hoge Raad der Nederlanden, 1984). While certain cases may not have provided explicit clarity on the presence of the required fear, we regarded the act of filing a report as evidence of its existence. Exclusively telephone-based threats were excluded since, although they technically fall within the cybercrime (ICT) definition, they are not commonly regarded as such.

Offline threat. We utilized Cognos to select police registrations categorized under the category of "threat" in the BVI for offline threat instances. In cases where online threat registrations were identified, they were reclassified into that category.

Online threat. To identify online threat cases, we selected online crime registrations in BlueIntel classified as "threat" were selected. Furthermore, we used a query through Cognos within the threat category of the BVI, using the following query: "facebook" OR "instagram" OR "twitter" OR "snapchat" OR "linkedin" OR "whatsapp" OR "tiktok" OR "mail" OR "e-mail" OR "reddit" OR "social media" OR "sociale media" OR "chat" OR "discord" OR "4chan" OR "facetime" OR "telegram".

A.2.1.4. Violation of physical integrity

For the main category "violation of physical integrity", we chose a comparison between sexual assault and image-based sexual abuse. Image-based sexual abuse includes a physical dimension that is scarce within the realm of cybercrime. Furthermore, the similarity between sexual assault and cyber offenses has been noted by cybercrime victims (Button et al., 2020), rendering a direct comparison particularly insightful. This parallel extends to cases of rape as well. However, the appropriateness of comparing with sexual assault stems from the fact that image-related sexual abuse

also does not necessitate bodily penetration. Image-based sexual abuse was chosen as an overarching category due to the intricate nature of its sub-variants, which often leads to confusion and misclassification (McGlynn et al., 2017).

Sexual assault. Our definition of sexual assault is based on art. 246 Sr. This entails forcing an individual to engage in or endure sexual or sexually oriented acts. It excludes acts involving bodily penetration, which are classified as rape. Our data extraction method involved utilizing Cognos to target registrations under the main category of "sexual assault". Instances were omitted where the nature of the act's sexual orientation was unclear, such as cases involving brief, potentially accidental touches, or actions with the intent to physically harm. Additionally, the component of force was deemed inherent when the victim was unable to repel the assault.

Image-based sexual abuse. This category pertains to the unwanted online sharing and/or creation of sexual imagery. Three commonly distinguished forms are: 1) sextortion (the extortion of money or additional explicit images to prevent the further distribution of images); 2) escalated/unwanted sexting (voluntarily shared images are subsequently disseminated without consent); and 3) revenge porn (the non-consensual dissemination of existing images with motives such as revenge, defamation, or libel) (Lomba et al., 2021; McGlynn and Rackley, 2017; Notté et al., 2021; Walrave and van de Heyning, 2022). If an individual voluntarily creates and transmits sexual imagery and threats of dissemination arise but are not enacted, it does not meet the criteria for image-based sexual abuse—unless payment is made to prevent distribution. Furthermore, instances without voluntary creation may involve scenarios where victims were deceived or when imagery was captured through hacking. We extracted crime reports falling under the categories "sexting" (Cognos and BlueIntel) or "sextortion" (BlueIntel). Also, the query "wraakporno" OR "wraak porno" OR "revengeporn" OR "revenge porn" OR sexting OR sextortion OR sextorsion was utilized to search the police offense database using Cognos.

A.2.2. Survey and invitation letters

Our survey broadly consisted of questions about: 1) experienced impact; 2) impact determinants (crime characteristics, explanatory theories, personal and social factors). The invitation letters and emails provided an overview of the research project, accompanied by instructions for accessing the online survey through weblinks that corresponded to the specific offense and victimization period. Emphasis was placed on ensuring anonymity throughout the survey process. Additionally, the invitations included a link to a dedicated website hosted by the Dutch Police Academy, which

offered further information about the research project. Contact details of the research team and resources provided by the Dutch organization for victim support were also provided. Prior to proceeding with the questionnaire, respondents were required to provide their consent by approving an informed consent form.

The invitation letter and survey underwent a pre-testing process involving eleven academic and professional peers. Additionally, the language and Dutch proficiency level (B1) of the invitation letter and questionnaire were reviewed by two copywriters from the communication department of the Dutch police. Furthermore, cognitive interviews were conducted with two elderly (65+) and one younger (40-) lay persons. The feedback of academic and professional peers was sought on various aspects of the invitation letter and survey, including the clarity of the invitation letter, the survey's completion time, and its overall user-friendliness. The cognitive interviews employed "thinking aloud" and "verbal probing" techniques (Priede and Farrall, 2010; Willis, 1999). This allowed the authors to understand their interpretation of the questions, the process of retrieving information from their memory, the decision-making process, and the alignment of their answers with the provided categories (Willis, 1999). The objective was to identify any areas of ambiguity or difficulty experienced by the participants. Changes of the questionnaire that followed were focused on clarifying terms, improving logical structure, and streamlining the overall design. Based on the testing and feedback, non-substantive changes were made to the questionnaire.

A.2.3. Data collection

The end date of the offense was used as one of the selection criteria for relevant cases. We also took offenses into account where the onset was earlier, or which were discovered during the intended period. When there was an insufficient number of victims within the intended time interval (for instance, six to nine months ago), we waited until there were enough victims in the intended interval and opened a new survey to ensure that only victims belonging to that interval participated. Current addresses of selected victims were obtained through the Municipal Personal Records Database ("Basisregistratie Personen", BRP) using the Citizen Service Number ("burgerservicenummer", BSN).

Inviting respondents of the violation of physical integrity category was done by phone to address the sensitivity of these offenses and the potential for someone in the household, unaware of the police report, to notice a letter from the police. The latter decision was informed by advice from Dutch police professionals specializing in sexual crimes and approved by the ethical authorities. To ensure respondents filled

in the survey during the intended time period, we selected a more recent portion of the group and closed the surveys when victims would no longer fit within that group. Participants who received letters were given a minimum of three weeks to complete the survey (1.5 weeks plus 1.5 weeks after the reminder), while the victims reached by telephone and email were given a minimum of two weeks. Out of the 3,006 invitation letters, 12 initial letters and 20 reminders were returned, primarily due to victims who had relocated or did not have a suitable mailbox. Among these, 8 victims had both the initial letter and the reminder returned.

The phone calls were conducted by a team of five police employees, including the first author; also approved by the Netherlands Public Prosecution Service. The authors prepared a call script and developed a brief training program, which included evaluation moments for the other callers. Each victim was contacted a maximum of four times, with two calls made from an anonymous phone number and two from a recognizable mobile phone number. Failure to reach victims was primarily due to their non-response after four attempts, as well as instances of non-existent phone numbers. For the victims who were reached but who declined to receive the invitation email, their reasons included lack of interest, psychological incapacity, language barrier (not speaking Dutch), time constraints, unwillingness to confront the incident again, or previous negative experiences with the police.

The response rate for doorstep deception, threat, and image-based sexual abuse, as shown in Table A.2.1, is relatively low, measuring below 25%. Through telephone conversations with the victims, previous research and analysis of police reports, we have identified potential factors that may have contributed to the lower response rate. Notably, a significant number of doorstep deception victims consisted of elderly individuals without internet access, posing challenges to participate in the online survey. Regarding threat victims, during the selection process, we observed that relatively many of them had a history of frequent offending. This could impact their perception of the police and potentially reduce their willingness to respond. Additionally, victims of image-based sexual abuse often experience feelings of embarrassment and reluctance to discuss the issue, as is clear from previous studies (Lomba et al., 2021; Walrave and van de Heyning, 2022), and became apparent during the invitation process.

Table A.2.1. Reached victims and survey response

	Traditional crime				Cybercrime				
	N reached *N* response			*N* total reached *N* response (%)	*N* reached *N* response			*N* total reached *N* response (%)	*N* total reached *N* response (%)
Victimization period	1	2	3		1	2	3		
Scam	Doorstep deception				Bank helpdesk fraud				
Reached[a]	165	166	166	497	167	167	167	501	
Response	33	24	39	96 (19.3%)	66	71	77	214 (42.7%)	
Burglary	Residential burglary				Hacking of online bank account				
Reached[a]	166	167	164	497	167	166	165	498	
Response	41	44	45	130 (26.2%)	45	57	41	143 (28.7%)	
Threat	Offline threat				Online threat				
Reached[a]	166	165	164	495	166	165	163	494	
Response	20	16	22	58 (11.7%)	24	19	22	65 (13.2%)	
Violation of physical integrity	Sexual assault				Image-based sexual abuse				
Reached[b]	138	129	125	392	132	131	136	399	
Invitation sent[c]	116	109	107	332	99	100	117	316	
Response	54	36	49	139 (35.5%)	28	21	39	88 (22.1%)	
				1.881				1.892	3.773
				423 (22.5%)				510 (27.0%)	933 (24.7%)

[a]Estimated from returned letters; [b]Successful phone calls to victims; [c]Victims who agreed to receive the survey invitation email.

A.2.4. Comparing respondents' characteristics with victim sample

To examine possible selective non-response, we compared our participants' characteristics with those of the entire group of 4,008 selected victims. We used chi-square goodness of fit tests (for gender) and one-sample *t* tests (for age) to assess representativeness, two-sided and with a significance level of $p < .05$. One selected victim in the hacking of online bank account category had the label "unknown" for gender and was therefore excluded from analysis. Our chi-square test revealed no significant difference between the proportion of men in our respondent group (45.8%) and among selected victims (48.6%), χ^2 (1, N = 906) = 2.82, p = .09. For age, we calculated approximate mean age by subtracting birth year from selection year for all victims. The *t* tests demonstrated that the overall selected victims' mean age (M = 47.9, SD = 21,71) was significantly lower than respondents' mean age (M = 55.9, SD = 21.08), t(899) = 11.48, $p < .001$. We applied the same tests to all discerned crime types:

Residential burglary. the male proportion in the current sample (54.3%) did not differ significantly from the proportion among selected victims (59.9%), χ^2 (1, N = 129) =1.71, p = .19. Respondents had a significantly higher approximate mean age (M = 62.28, SD = 15.36) compared to the approximate mean age of selected victims (M = 54.48, SD = 18.23), t(126) = 5.73, $p < .001$.

Hacking of online bank account. the male proportion in the current sample (58.0%) did not differ significantly from the proportion among selected victims (51.2%), χ^2 (1, N = 143) = 2.68, p = .10. Respondents had a significantly higher approximate mean age (M = 60.02, SD = 14.43) compared to the approximate mean age of selected victims (M = 49.86, SD = 16,67), t(142) = 8.42, $p < .001$.

Doorstep deception: the male proportion in the current sample (37.2%) did not differ significantly from the proportion among selected victims (36.3%), χ^2 (1, N = 94) = .04, p = .85. Respondents had a significantly higher approximate mean age (M = 75.65, SD = 16.53) compared to the approximate mean age of selected victims (M = 71.58, SD = 22.23), t(93) = 2.39, p = .02.

Bank helpdesk fraud. the male proportion in the current sample (48.3%) did not differ significantly from the proportion among selected victims (48.1%), χ^2 (1, N = 211) = .01, p = .94. Respondents had a significantly higher approximate mean age (M = 71.04, SD = 9.26) compared to the approximate mean age of selected victims (M = 68.38, SD = 13.12), t(209) = 4.17, $p < .001$.

Offline threat: the male proportion in the current sample (48.1%) was significantly lower than the proportion among selected victims (64.1%), χ^2 (1, N = 52) = 5.80, p = .02. Respondents had a significantly higher approximate mean age (M =

46.35, *SD* = 14.31) compared to the approximate mean age of selected victims (*M* = 40.12, *SD* = 13.85), $t(50) = 3.11$, $p = <.01$.

Online threat. the male proportion in the current sample (51.8%) did not differ significantly from the proportion among selected victims (43.9%), χ^2 (1, *N* = 56) = 1.41, $p = .23$. Respondents had a significantly higher approximate mean age (*M* = 44.96, *SD* = 14.47) compared to the approximate mean age of selected victims (*M* = 38.25, *SD* = 13.50), $t(55) = 3.47$, $p < .01$.

Sexual assault. the male proportion in the current sample (2.2%) did not differ significantly from the proportion among selected victims (5.0%), χ^2 (1, *N* = 136) = 2.24, $p = .14$. Respondents' approximate mean age (*M* = 30.80, *SD* = 13.90) did not significantly differ from the approximate mean age of selected victims (*M* = 29.83, *SD* = 12.66), $t(136) = .81$, $p = .42$.

Image-based sexual abuse. the male proportion in the current sample (80.0%) did not differ significantly from the proportion among selected victims (80.0%), χ^2 (1, *N* = 85) = .00, p =1.00 Respondents' approximate mean age (*M* = 33.13, *SD* = 14.06) did not significantly differ from the approximate mean age of selected victims (*M* = 30.42, *SD* = 12.22), $t(81) = 1.75$, $p = .08$.

A.2.5. Factor analysis

Prior to conducting the PCA, we assessed the suitability of the data for factor analysis. The correlation coefficients indicated many values of .3 and above, and the Kaiser-Meyer-Olkin measure was .95, surpassing the recommended threshold of .6 (Shrestha, 2021). The Bartlett's Test of Sphericity yielded a statistically significant result ($p <$ .001), supporting the appropriateness of the factor analysis. The screeplot from the PCA exhibited breaks after the second and fourth component. Also considering the expected differences in impact factors, we retained the four factors for further examination. The communality values for the four-factor solution were all above .3, with the lowest value being .35. Therefore, all items were retained for further analysis. Given the relatively high component correlation (.45 being the highest), an Oblimin rotation solution was employed, as it permits correlated factors (Tabachnick et al., 2013). The rotated solution exhibited a clear structure with strong loadings on the four components. The first four factor solution is shown in Table A.2.2.

Table A.2.2. PCA pattern coefficients impact items with Oblimin rotation

Item	Pattern coefficients				Communalities
	Factor 1	Factor 2	Factor 3	Factor 4	
Concentration difficulties	**.87**				.77
Nausea	**.81**				.60
Impaired work/study functioning	**.77**				.71
Weight change	**.76**				.56
Headache	**.76**				.70
Suicidal ideation	**.76**				.50
Reduced social interaction	**.71**				.56
Relationship issues	**.70**				.52
Fear/panic	**.68**	.32			.72
Sleep disturbances	**.68**				.71
Depression/sadness	**.67**				.76
Decreased self-worth	.57			.39	.67
Decreased self-esteem	.53			.39	.69
Reliving the offense	.53	.41			.69
Anger		**.79**			.62
Frustration/irritation		**.76**			.66
Sense of privacy violation		**.71**			.53
Persistent thoughts of the crime		**.65**			.67
Applying protective measures		**.60**			.35
Desire for retaliation		**.56**			.44
Fear of recurrence	.34	**.55**			.54
Stress/tension	.47	.53			.71
Diminished trust in others	.34	.47			.54
Financial hardships			**.87**		.75
Substantial loss			**.83**		.74
Decreased income			**.83**		.77
Self-blame				**.92**	.79
Feelings of shame				**.85**	.78
Heightened caution		.36		.47	.44

Note. Items selected per factor are bolded; items shown in grey were excluded from further analysis.

A.2.6. Impact comparisons: moment of victimization and crime type

We examined the influence of moment of victimization and crime type (cybercrime or traditional crime) on the four discerned types of current impact. For this purpose, a two-way between-groups analysis of variance was employed, with a significance level of $p < .05$ (two-sided). The outcomes were as follows:

Internalizing problems. Regarding internalizing problems, the interaction effect between the moment of victimization and crime type did not reach statistical signifi-

cance, F (2, 904) = 1.02, p = .36. The main effect for moment of victimization was statistically significant, F (2, 904) = 8.82, p < .001. Further post-hoc comparisons using the Tukey HSD test revealed that the mean score for internalizing problems among the most recent group, victimized 0-3 months ago (M = .69, SD = .91), was higher than among those victimized 6-9 (M = .39, SD = .81) or 12-15 (M = .50, SD = .80) months ago. However, no significant difference emerged between the victimization groups of 6-9 months ago and 12-15 months ago.

Externalizing problems. The interaction effect between the moment of victimization and crime type concerning externalizing problems also did not reach statistical significance, F (2, 904) = .58, p = .56. The main effect for the moment of victimization was statistically significant, F (2, 904) = 12.77, p < .001. Subsequent post-hoc comparisons using the Tukey HSD test demonstrated that the mean score for externalizing problems among the most recent group, victimized 0-3 months ago (M = 2.28, SD = 1.05), was higher compared to the groups victimized 6-9 (M = 1.87, SD = 1.09) or 12-15 (M = 1.92, SD = 1.12) months ago. Again, there was no significant difference between the 6-9 months ago group and the 12-15 months ago group.

Financial impact. For financial impact, the interaction effect between the moment of victimization and crime type also did not reach statistical significance, F (2, 904) = 3.24, p = .04—we adopted a significance level of p < .01 due to the statistically significant result of Levene's test of equality of error variances. The main effect for the moment of victimization was statistically significant, F (2, 904) = 11.14, p < .001. Follow-up post-hoc comparisons using the Tukey HSD test indicated that the mean score for financial impact among the most recent group victimized up to 3 months ago (M = .46, SD = .89) was higher compared to the groups victimized 6-9 (M = .22, SD = .67) or 12-15 (M = .20, SD = .54) months ago. Once again, the 6-9 and 12-15 months ago groups did not exhibit significant differences between each other.

Damaged self-image. In terms of damaged self-image, the interaction effect between the moment of victimization and crime type was also not statistically significant, F (2, 904) = .81, p = .45. The main effect for the moment of victimization did not yield statistical significance, F (2, 904) = 3.46, p = .03—we adopted a significance level of p < 0.01 due to the statistically significant outcome of Levene's test of equality of error variances.

A.2.7. Impact comparisons: education level and crime type

We examined the influence of education level (low, medium and high) and crime type (cybercrime or traditional crime) on the four discerned types of current impact.

To this end, we used a two-way between-groups analysis of variance for two-sided tests with a significance level of $p < .05$. The results for the different impact types were as follows:

Internalizing problems. Regarding internalizing problems, the interaction effect between education level and crime type was not statistically significant, F (2, 882) = 2.41, p = .09. The main effect for education level was statistically significant, F (2, 882) = 24.75, p <. 001. Subsequent post-hoc comparisons employing the Tukey HSD test revealed that the mean internalizing problems score for the higher educated group (M = .31, SD = .63) was lower than for the lower (M = .62, SD = .91) and medium (M = .71, SD = .95) educated groups. There was no statistically significant difference between the lower and medium educated groups.

Externalizing problems. In terms of externalizing problems, the interaction effect between education level and crime type did not reach statistical significance, F (2, 882) = .35, p = .71. The main effect for education level was statistically significant, F (2, 882) = 27.25, p < .001. Post-hoc comparisons conducted through the Tukey HSD test revealed that the mean externalizing problems score for the higher educated group (M = 1.70, SD = 1.03) was lower than for the lower (M = 2.24, SD = 1.03) and medium (M = 2.22, SD = 1.16) educated groups. Again, there was no statistically significant difference between the lower and medium educated groups.

Financial impact. For financial impact, the interaction effect between education level and crime type was also not statistically significant, F (2, 882) = .25, p = .78. Furthermore, there was no significant main effect for education level, F (2, 882) = 4.35, p = .01—we employed a significance level of $p < .01$ due to the statistical significance observed in Levene's test of equality of error variances.

Damaged self-image. Regarding damaged self-image, the interaction effect between education level and crime type was also not statistically significant, F (2, 882) = 1.43, p = .24. The main effect for education level was statistically significant, F (2, 882) = 16.95, p < .001. Further examination through post-hoc comparisons, utilizing the Tukey HSD test, revealed that the mean score for damaged self-image among the higher educated group (M = 1.16, SD = 1.31) was lower than for the lower (M = 1.88, SD = 1.52) and medium (M = 1.86, SD = 1.50) educated groups. The lower and medium educated groups again did not differ significantly from each other.

A.2.8. References Appendix 2

Borwell, J., Jansen, J., & Stol, W. (2018). Human factors leading to online fraud victimisation: Literature review and exploring the role of personality traits. In J. McAlaney, L. Frumkin, & V. Benson (Eds.), *Psychological and behavioral examinations in cyber security* (pp. 26–45). IGI Global.

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). Victims of cybercrime: Understanding the impact through accounts. In M. W. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context: The Human Factor in Victimization, Offending, and Policing* (pp. 137–156). Springer.

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, *25*(2), 670–691. https://doi.org/10.1177/17488958221128128

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

Centrum voor Criminaliteitspreventie en Veiligheid (CCV). (n.d.). *Babbeltruc* [Doorstep deception]. Retrieved March 4, 2021, from https://hetccv.nl/onderwerpen/senioren-en-veiligheid/specifieke-themas/babbeltruc/

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187–204. https://doi.org/10.1177/0269758015571471

Hoge Raad der Nederlanden. (1984, January 17). *ECLI:NL:HR:1984:AC8252 [Supreme Court Decision]*. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:1984:AC8252

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. https://doi.org/10.21428/88de04a1.976bcaf6

Lomba, N., Navarra, C., & Fernandes, M. (2021). *Combating gender-based violence: Cyber violence*. European Parliamentary Research Service.

McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies*, *37*(3), 534–561. https://doi.org/10.1093/ojls/gqw033

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies*, *25*, 25–46. https://doi.org/10.1007/s10691-017-9343-2

Montoya, L., Junger, M., & Hartel, P. (2013). How "digital" is traditional crime? *Proceedings of the 2013 European Intelligence and Security Informatics Conference*, 31–37. https://doi.org/10.1109/EISIC.2013.12

Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, *27*(3), 272–294. https://doi.org/10.1177/02697580211010692

Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological impact of hacking victimization. *SAGE Open*, *11*(4). https://doi.org/10.1177/21582440211061556

Politie. (n.d.). *Pas op voor telefonische oplichting! Laat u niet onder druk zetten [Beware of telephone fraud! Don't let yourself be pressured]*. Retrieved February 20, 2023, from https://www.politie.nl/binaries/content/assets/politie/onderwerpen/bankhelpdeskfraude-spoofing/folder-bankhelpdeskfraude-inclusief-anydesk.pdf

Priede, C., & Farrall, S. (2010). Comparing results from different styles of cognitive interviewing: 'Verbal probing' vs. 'thinking aloud.' *International Journal of Social Research Methodology*, *14*(4), 271–287. https://doi.org/10.1080/13645579.2010.523187

Rooyakkers, J., & Weulen Kranenbarg, M. (2020). Vissen met een nieuwe hengel: Een onderzoek naar betaalverzoekfraude [Fishing with a new rod: A study on payment request fraud]. *Justitiële Verkenningen*, *46*(2), 19–43. https://doi.org/10.5553/JV/016758502020046002003

Shrestha, N. (2021). Factor analysis as a tool for survey analysis. *American Journal of Applied Mathematics and Statistics*, *9*(1), 4–11. https://doi.org/10.12691/ajams-9-1-2

Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2013). *Using multivariate statistics*. Pearson.

Walrave, M., & van de Heyning, C. (2022). De beelden waren de druppel: Waarom beelden van seksuele misdrijven online gedeeld worden vanuit sociaalwetenschappelijk en juridisch perspectief [The images were the last straw: Why images of sexual crimes are shared online from a socio-scientific and legal perspective]. *Cahiers Politiestudies*, *62*(1), 163–189.

Willis, G. B. (1999). *Cognitive interviewing: A "how to" guide*. Research Triangle Institute.

Appendix 3. Victim survey – Chapters 5 and 6

Questionnaire for crime impact research[17]

Consent Statement

By signing this statement, you are indicating that the points below apply to you. This consent statement is required to participate in this study.

- I read the information in the invitation letter.
- I understand how to ask questions about the study.
- I was able to reflect on my participation in the study.
- I understand that I can drop out of the study at any time without having to provide a reason.
- I understand that all data I share in this study is collected anonymously and therefore cannot be traced back to me.
- I understand that I will be asked for personal information (age, gender, education, employment and living situation, nationality, income, and religion), and I can choose not to answer these questions.
- I consent to the use of the anonymous data that I share solely for this study and will be used exclusively by the researchers.
- I understand that the data collected will be kept for a maximum of ten years, anonymously and securely. (This will allow the quality of this research to be checked at a later date).

Do these points apply to you and would you like to participate in the study? Then click below to sign this consent form.

☐ The above points apply to me and I want to participate in the study.

[17] The original questionnaire (in Dutch), as administered to respondents, follows after the English translation.

Questionnaire

What is an offense?
An "offense" is another word for a criminal offense. An example of a criminal offense is bicycle theft. The perpetrator can be prosecuted and punished for this. This means that the perpetrator can receive a punishment from a judge for the bicycle theft. In this case, we call the bicycle theft the offense.

According to our records, in the period between ... and …, you have reported to the police[18]

<'Face to face' scam (such as on the street or at the door)>
<Bank helpdesk fraud (telephone and/or online scams)>
<Residential burglary>
<Misuse of Internet banking account (transferring money or withdrawing money without your permission)>
<Sexual assault / sexual violence>
<Sexting, sextortion or revenge porn>
<Threat>
<Online threat>

	yes	no
Is it true that you reported this offense?	☐	☐
No → go to landing page 1		
Did you report this offense on your own behalf?	☐	☐
No → go to landing page 1		

Landing page 1
You are not part of the target audience for this questionnaire. Thank you for your effort to participate in this study.

This questionnaire is about the offense you reported: [...].[19]

If between ... and ... you experienced this offense multiple times and reported it multiple times, please base your responses on the most recent incident.

[18] The time frame and offense varied between respondents.
[19] Refers to one of eight specific offenses on the basis of which the respondent was selected.

The questions are about:

- The impact of the offense on you;
- the needs you had following the offense;
- your personal circumstances;
- your interaction with the police.

How did you report to the police?
☐ At the police station (in person)
☐ At the scene of the offense
☐ By phone
☐ Via the Internet
☐ Through a 3D reporting kiosk (TV screen at police station)
☐ At the police station (in person)

Do you remember whether it was an official report or a notification?
☐ Notification
☐ Official report
☐ I don't know

The following questions are about the offense.[20]

'Face to face' scam (such as on the street or at the door)			
	yes	no	I don't know
Did the scam take place in or near your home (e.g., at the door)?	☐	☐	☐

[20] Initial questions varied by offense type.

Bank helpdesk fraud (telephone and/or online scams)			
Please check which situation applies most to you: ☐ The perpetrator posed as a bank employee. ☐ The perpetrator posed as a government employee (for example, from the police, a ministry, or a court). ☐ The perpetrator claimed to work for another organization, namely: [open text field]			
	yes	no	I don't know
Was your computer remotely accessed so that the perpetrator could control it?	☐	☐	☐

Residential burglary			
	yes	no	I don't know
Were items stolen from you that had emotional value to you?	☐	☐	☐

Misuse of Internet banking account (transferring or withdrawing money without your permission)
Please check which situation applies most to you: ☐ I was in contact about a purchase or sale (for example, through Marktplaats or Facebook Marketplace). In doing so, the perpetrator asked to enter my bank details or pay a small amount, such as for a payment service, verification, identity verification, insurance or shipping costs. I then entered my details. ☐ I entered my details after clicking on a link in a message (e.g., email or text) that appeared to come from a trusted entity. ☐ I don't know how the perpetrators could have misused my online banking account. ☐ The perpetrators got the details of my online bank account by another means, namely: [open text field]

Sexual assault / Sexual violence			
	yes	no	I do not know
Did the sexual assault involve violence or threats of violence by the perpetrator(s)?	☐	☐	☐

Sexting, sextortion or revenge porn

a. Please check which situation applies most to you:

☐ Someone possessed sexually explicit material of me (for example, nude photos or videos) against my will and distributed it.

☐ Someone possessed sexually explicit material of me (for example, nude photos or videos) against my will and threatened to distribute it.

☐ I sent sexually graphic explicit material of myself (for example, nude photos or videos) to someone. Then this material was distributed against my will.

☐ I sent sexually explicit material of myself (for example, nude photos or videos) to someone. I was then threatened that it would be distributed.

☐ Other, namely: [open text field]

	yes	no	I do not know
b. Did the perpetrator ask you for money to prevent dissemination of the material?	☐	☐	☐
Yes→ Did you then pay to prevent dissemination of the material?	☐	☐	☐
c. Did the perpetrator ask you for more sexually explicit images of you to prevent the dissemination of the material?	☐	☐	☐
Yes→ Did you then send more sexually explicit images of you to prevent dissemination of the material?	☐	☐	☐

Threat

Please check which situation applies most to you:

☐ I have been threatened with death in a public place (for example, on the street or in a government building).

☐ I have been threatened in a public place (for example, on the street or in a government building) with something else (for example, aggravated assault).

☐ I received death threats at home.

☐ I have been threatened at home with something else (e.g. aggravated assault).

☐ I received death threats elsewhere.

☐ I have been threatened with something else elsewhere (e.g. aggravated assault).

☐ I was threatened in another way, namely: [open text field]

Online threat
a. Please check which situation applies most to you:
☐ I received death threats online.
☐ I was threatened online with something else (e.g. aggravated assault).
b. Please check which situation applies most to you (multiple answers possible):
☐ I was threatened via email.
☐ I was threatened via a messaging service (e.g., WhatsApp or Signal) or via text message.
☐ I was threatened via social media (e.g., Instagram, Twitter or Facebook) via private message (DM).
☐ I was threatened via social media (e.g., Instagram, Twitter or Facebook) through a message that others could also see.
☐ I was threatened in another way, namely: [open text field]

The following questions are about the characteristics of the offense you reported.

1.			
a.	Please check which situation applies most to you:		
	☐ I did not know the perpetrator(s).		
	☐ I somewhat knew the perpetrator(s).		
	☐ I knew the perpetrator(s) well.		
	☐ I don't know if I knew the perpetrator(s).		
b.	Do the following statements apply to the offense?	yes	no
	The perpetrator persuaded or deceived me into doing or allowing something.	☐	☐
	I had direct contact with the offender during the offense (for example, by phone, through a messaging service such as WhatsApp or in person).	☐	☐
	I was at home when the offense occurred or when I discovered that the offense had occurred.	☐	☐
c.	Do the following statements apply (scale from 1: definitely not, to 5: definitely yes)?	definitely not	definitely yes
	I believe the offense was specifically targeted at me	1☐ 2☐ 3☐ 4☐ 5☐	
	Because of my own reaction during the offense, I managed to prevent worse.	1☐ 2☐ 3☐ 4☐ 5☐	
	The offense was unexpected to me.	1☐ 2☐ 3☐ 4☐ 5☐	
	Looking back on the experience, I could have prevented the offense from happening at the time.	1☐ 2☐ 3☐ 4☐ 5☐	

2. How long did the offense you reported last?
☐ One-time occurrence
☐ Less than 1 week
☐ More than 1 week but less than 1 month
☐ Longer than 1 month but less than 3 months
☐ 3 months to 6 months
☐ Half a year to a year
☐ Longer than 1 year
☐ I don't know

We now ask you first about the consequences of the offense **when it occurred or when you discovered it had occurred**.

First, we ask you about the consequences of the offense when you discovered the offense was occurring or had occurred.

3. Did the offense when it occurred or when you discovered it had occurred have the following consequences for you (scale from 1: not experienced, to 5: very strongly experienced)?		
	then not experienced	then experienced very strongly
I experienced psychological shock (acute, severe stress).	1☐ 2☐ 3☐ 4☐ 5☐	
I denied what had happened or found it hard to believe.	1☐ 2☐ 3☐ 4☐ 5☐	
It made me feel desperate.	1☐ 2☐ 3☐ 4☐ 5☐	
It made me feel helpless.	1☐ 2☐ 3☐ 4☐ 5☐	
I had physical symptoms such as palpitations, dizziness, trembling or abdominal pain because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
Other consequences, namely: [open text field]		

4. Have you sought professional help as a result of the offense (for example, Victim Support Netherlands or psychological support)?
☐ Yes
☐ No
☐ I don't know
☐ Prefer not to say

5. After the offense, how much time did it take you to take the initial measures (e.g., repair work, seek for help, go to the police)?
☐ Less than 1 hour
☐ Between 1 and 5 hours
☐ Between 5 and 10 hours
☐ Between 10 and 20 hours
☐ More than 20 hours
☐ I don't know

Hereunder we mean the **direct financial loss** before you possibly received compensation. **Do not** count any damages from the recovery or handling of the offense.

6. What was the direct financial loss from the offense (such as money taken from you)?
☐ The offense did not result in any direct loss to me.→ *go to question 8*
☐ Less than €100
☐ Between €100 and €500
☐ Between €501 and €1,000
☐ Between €1,001 and €2,000
☐ Between €2,001 and €5,000
☐ Between €5,001 and €10,000
☐ Between €10,001 and €50,000
☐ More than €50,000
☐ I don't know
☐ Prefer not to say

7. Did you get any of this back or are you going to get it back (for example, through the bank, insurance or other agency)?
☐ Yes, the entire loss amount
☐ Yes, most of the loss amount
☐ Yes, part of the loss amount but not most of it
☐ No, did not try
☐ No, tried but did not receive
☐ I don't know (yet)
☐ Prefer not to say

Hereunder we mean the **indirect financial loss** before you possibly received compensation.

8. What was the indirect financial loss caused by the offense for recovery or its handling (such as replacement of belongings or assistance with processing)?

- ☐ The offense did not result in indirect loss to me → *go to question 10*
- ☐ Less than €100
- ☐ Between €100 and €500
- ☐ Between €501 and €1,000
- ☐ Between €1,001 and €2,000
- ☐ Between €2,001 and €5,000
- ☐ Between €5,001 and €10,000
- ☐ Between €10,001 and €50,000
- ☐ More than €50,000
- ☐ I don't know
- ☐ Prefer not to say

9. Did you get any of this back or are you going to get it back (for example, through the bank, insurance or other agency)?

- ☐ Yes, the entire damage amount
- ☐ Yes, most of the damage amount
- ☐ Yes, part of the damage amount, but not most of it
- ☐ No, not tried
- ☐ No, tried but did not receive
- ☐ I don't know (yet)
- ☐ Prefer not to say

The following questions are about how the offense is currently affecting you.

10.			
a.	*Does the offense currently have the following emotional effects on you (scale from 1: not at all, to 5: very strongly)?*		
		I am not experiencing this at all	I am experiencing this very strongly
	I experience stress or tension because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
	I have anxiety or panic symptoms because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
	This makes me angry.	1☐ 2☐ 3☐ 4☐ 5☐	
	I am frustrated or irritated about this.	1☐ 2☐ 3☐ 4☐ 5☐	
	I blame myself for what happened.	1☐ 2☐ 3☐ 4☐ 5☐	
	I am ashamed of what happened.	1☐ 2☐ 3☐ 4☐ 5☐	
	I have less self-confidence because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
	My self-esteem is lower because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
	I have become more cautious because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
	I often think about what happened.	1☐ 2☐ 3☐ 4☐ 5☐	
	I relive the event over and over again.	1☐ 2☐ 3☐ 4☐ 5☐	
	This makes me feel depressed, sad or dejected.	1☐ 2☐ 3☐ 4☐ 5☐	
	This makes me afraid of going through something like this again.	1☐ 2☐ 3☐ 4☐ 5☐	
	I experience an invasion of my privacy because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
	This makes me feel less safe on the Internet (including online apps and social media/WhatsApp).	1☐ 2☐ 3☐ 4☐ 5☐	
	This makes me feel less safe in physical spaces (such as at home, on the street or in other places inside or outside).	1☐ 2☐ 3☐ 4☐ 5☐	
	Other emotional effects, namely: [open text field]		
b.	*Does the offense currently have the following social or behavioral effects on you (scale from 1: not at all, to 5: very strongly)?*		
	I have less contact with other people because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
	I am reluctant to express myself freely on the Internet (including online apps and social media/WhatsApp) because of this.	1☐ 2☐ 3☐ 4☐ 5☐	
	I am reluctant to express myself freely in physical space (such as at home, on the street or in other places inside or outside) because of this.	1☐ 2☐ 3☐ 4☐ 5☐	

	This causes me to avoid certain places or situations on the Internet (including online apps and social media/ WhatsApp).	1☐ 2☐ 3☐ 4☐ 5☐
	This causes me to avoid certain places or situations in the physical space (such as at home, on the street or in other places inside or outside).	1☐ 2☐ 3☐ 4☐ 5☐
	I have less confidence in other people because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	I have feelings of revenge towards the perpetrator(s) because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	I function less well in my work/study because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	As a result of this, I am taking measures to avoid experiencing a similar offense again.	1☐ 2☐ 3☐ 4☐ 5☐
	I have problems in my relationships (for example with partner, friends or family) because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	Other social or behavioral effects, namely: [open text field]	
c.	*Does the offense currently have the following physical effects on you (scale from 1: not, to 5: very much)?*	
	I sleep worse because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	I suffer from headaches because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	I suffer from nausea because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	I no longer want to live because of this or have thoughts about this.	1☐ 2☐ 3☐ 4☐ 5☐
	My weight has changed because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	I have concentration difficulties because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	Other physical effects, namely: [open text field]	
d.	*Does the offense currently have the following financial effects on you (scale from 1: not at all, to 5: very much)?*	
	I have less income because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	The financial loss I suffer as a result is significant for me.	1☐ 2☐ 3☐ 4☐ 5☐
	I have financial problems because of this.	1☐ 2☐ 3☐ 4☐ 5☐
	Other financial effects, namely: [open text field]	

The following questions are about needs you had due to the offense in the period immediately following the offense.

11.	In the period shortly after the offense, did you have the following needs (scale from 1: I did not have this need, to 5: I had this need very strongly)?		
		I did not have this need	I had this need very strongly
	Knowing where I could turn for help and support during or after the offense.	1☐ 2☐ 3☐ 4☐ 5☐	
	Acknowledgment of the offense that happened to me.	1☐ 2☐ 3☐ 4☐ 5☐	
	Being taken seriously as a victim.	1☐ 2☐ 3☐ 4☐ 5☐	
	Practical help with problems created by the offense, such as recovery or arranging matters.	1☐ 2☐ 3☐ 4☐ 5☐	
	Information about the offense and how it could have happened.	1☐ 2☐ 3☐ 4☐ 5☐	
	Financial compensation for the damage I suffered.	1☐ 2☐ 3☐ 4☐ 5☐	
	Detection, arrest, and prosecution of the perpetrator.	1☐ 2☐ 3☐ 4☐ 5☐	
	Someone to talk to with whom I could share my feelings.	1☐ 2☐ 3☐ 4☐ 5☐	
	Advice to avoid experiencing such an offense again.	1☐ 2☐ 3☐ 4☐ 5☐	
	Professional therapy or guidance to deal with the consequences of the offense.	1☐ 2☐ 3☐ 4☐ 5☐	
	Preventing other people from experiencing the same offense.	1☐ 2☐ 3☐ 4☐ 5☐	
	Other needs, namely: [open text field]		

The following questions are about some personal circumstances related to the offense you experienced.

12.	Do the following statements apply to you (scale from 1: definitely not, to 5: definitely yes)?		
		definitely not	definitely yes
	Sometimes it feels as if the offense didn't really happen to me.	1☐ 2☐ 3☐ 4☐ 5☐	
	I have learned from the offense.	1☐ 2☐ 3☐ 4☐ 5☐	
	I see myself as a victim of the offense that happened to me.	1☐ 2☐ 3☐ 4☐ 5☐	
	I can solve the offense and its consequences myself.	1☐ 2☐ 3☐ 4☐ 5☐	
	I received adequate support from those around me (e.g. partner, friends or family) after the offense.	1☐ 2☐ 3☐ 4☐ 5☐	
	Those around me (e.g. partner, friends or family) blame me for the offense.	1☐ 2☐ 3☐ 4☐ 5☐	
	Those around me (e.g. partner, friends or family) understand what I went through.	1☐ 2☐ 3☐ 4☐ 5☐	
	I find it difficult to tell people about the offense I experienced.	1☐ 2☐ 3☐ 4☐ 5☐	
	Society takes the offense that I experienced seriously.	1☐ 2☐ 3☐ 4☐ 5☐	

The following questions concern personal circumstances.

13.	Do the following statements apply to you (scale from 1: definitely not, to 5: definitely yes)?		
		definitely not	definitely yes
	Before the offense took place, I had psychological problems.	1☐ 2☐ 3☐ 4☐ 5☐	
	I have experienced major setbacks in my life, such as a traumatic experience or serious illness / death of a partner or close family member.	1☐ 2☐ 3☐ 4☐ 5☐	
	Before the offense took place, I had a positive view of the world.	1☐ 2☐ 3☐ 4☐ 5☐	
	I often do things on a whim, without giving it much thought.	1☐ 2☐ 3☐ 4☐ 5☐	
	I would feel restless if I did not have access to the Internet (including online apps and social media/WhatsApp) for 24 hours.	1☐ 2☐ 3☐ 4☐ 5☐	
	My digital identity (for example, on social media) is an inseparable part of my overall identity.	1☐ 2☐ 3☐ 4☐ 5☐	

14. How much time do you spend per day on the Internet (including online apps and social media/ WhatsApp), including for work or study?

- ☐ Less than 1 hour
- ☐ Between 1 and 2 hours
- ☐ Between 2 and 5 hours
- ☐ Between 5 and 10 hours
- ☐ Between 10 and 15 hours
- ☐ More than 15 hours
- ☐ I don't know

15. In the past 2 years, have you personally experienced the same offense more often?

- ☐ Yes
- ☐ No
- ☐ I don't know
- ☐ Prefer not to say

16. Have you personally experienced any other offense in the past 2 years?

- ☐ Yes
- ☐ No
- ☐ I don't know
- ☐ Prefer not to say

The following questions are about your experience with the police regarding the offense you reported.

17.	Do the following statements apply to you (scale from 1: definitely not, to 5: definitely yes)?		
		definitely not	definitely yes
	I was able to share my story with the police.	1☐ 2☐ 3☐ 4☐ 5☐	
	I received sufficient information from the police about the offense and how it could have happened.	1☐ 2☐ 3☐ 4☐ 5☐	
	I received sufficient advice from the police on how I can prevent experiencing such an offense again.	1☐ 2☐ 3☐ 4☐ 5☐	
	The police had too little knowledge to be able to help me properly.	1☐ 2☐ 3☐ 4☐ 5☐	
	The police underestimated the consequences the offense had for me.	1☐ 2☐ 3☐ 4☐ 5☐	
	I had the feeling that the police blamed me for the offense.	1☐ 2☐ 3☐ 4☐ 5☐	
	The police treated my report as an urgent matter.	1☐ 2☐ 3☐ 4☐ 5☐	
	The police put in enough effort after my report.	1☐ 2☐ 3☐ 4☐ 5☐	
	I received sufficient information from the police about what they did or will do with my report.	1☐ 2☐ 3☐ 4☐ 5☐	
	The negative consequences of the offense decreased because of how the police handled my report.	1☐ 2☐ 3☐ 4☐ 5☐	
	The negative consequences of the offense increased because of how the police handled my report.	1☐ 2☐ 3☐ 4☐ 5☐	
	Would you like to share anything further about your experience with the police, for example in relation to the needs you had? [open text field]		

We would like to close with questions about personality characteristics.

18.	What is your gender?
☐	Man
☐	Woman
☐	Non-binary
☐	Prefer not to say

19.	What is your year of birth (yyyy)?
....[21]	
☐	Prefer not to say

20.	What is the highest education you have completed with a diploma, certificate or degree?
☐	No education
☐	Primary school (including special education, e.g., lom, blo, etc.)
☐	Lower vocational education (lbo, lts), vmbo basic vocational or framework vocational track
☐	Mavo, vmbo theoretical or mixed curriculum, ulo, mulo
☐	Havo, vwo, gymnasium, hbs, mms
☐	Intermediate vocational education (mbo, bol, bbl)
☐	Propedeuse, candidate, bachelor's degree, higher professional education (hbo)
☐	PhD, master's degree, scientific education (wo)
☐	Doctorate, PhD
☐	I don't know

21.	Which description fits you best?
☐	Paid employment / self-employed → *go to question 22*
☐	Unemployed / between jobs
☐	Volunteer
☐	Incapacitated
☐	Pupil or student
☐	Househusband / housewife
☐	Retired or on early retirement
☐	None of these
☐	I don't know
☐	Prefer not to say

22.	Do you work at least 12 hours per week on average?
☐	Yes
☐	No
☐	I don't know
☐	Prefer not to say

[21] This item was presented as a multiple-choice question in the original questionnaire.

23. How many people are in your household, including yourself?

1 → go to question 25

- ☐ Prefer not to say
- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ 6
- ☐ 7
- ☐ 8
- ☐ 9
- ☐ 10
- ☐ 11
- ☐ 12
- ☐ 13
- ☐ 14
- ☐ 15
- ☐ More than 15

24. How many of those people are younger than 15 years old?

- ☐ Prefer not to say
- ☐ 0 (none)
- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ 6
- ☐ 7
- ☐ 8
- ☐ 9
- ☐ 10
- ☐ 11
- ☐ 12
- ☐ 13
- ☐ 14
- ☐ Over 14

This question is about your **gross annual income**, not the income of any other members of your household.

25.	What was your gross annual income in 2021?
☐	€10,000 or less
☐	€10,001 - €20,000
☐	€20,001 - €30,000
☐	€30,001 - €40,000
☐	€40,001 - €50,000
☐	€50,001 - €60,000
☐	€60,001 - €70,000
☐	€70,001 - €80,000
☐	€80,001 - €90,000
☐	€90,001 - €100,000
☐	More than €100,000
☐	I don't know
☐	Prefer not to say

26.	What was the total combined gross annual income of all members of your household in 2021?
☐	€10,000 or less
☐	€10,001 - €20,000
☐	€20,001 - €30,000
☐	€30,001 - €40,000
☐	€40,001 - €50,000
☐	€50,001 - €60,000
☐	€60,001 - €80,000
☐	€80,001 - €100,000
☐	€100,001 - €150,000
☐	€150,001 - €200,000
☐	More than €200,000
☐	I don't know
☐	Prefer not to say

27.	Which situation best applies to you?
☐	Married or in a registered partnership
☐	Living together (cohabiting)
☐	Unmarried / single
☐	Divorced
☐	Widowed
☐	Prefer not to say

28.	Do you consider yourself part of a religious or spiritual group?
☐	Yes
☐	No
☐	I don't know
☐	Prefer not to say

29.	What is your nationality (multiple answers possible)?
☐	Dutch nationality
☐	Other nationality
☐	Both (Dutch and other nationality)
☐	Prefer not to say

Thank you very much for your participation in this study. Your participation will allow us to explore the impact of crime on victims. This will give us insight into how we can improve our work in victim care and crime control.

May we possibly invite you for a personal conversation later? In this conversation, we can ask more questions about the impact of the offense. If we may invite you for this, please send an email to [email address omitted].

This research is about the consequences of crime, which can be profound. For emotional support, help in the criminal process or assistance in getting compensation for your losses, go to www.slachtofferhulp.nl, or call 0900 - 01 01.

Vragenlijst voor onderzoek naar de impact van criminaliteit[22]

Toestemmingsverklaring
Door deze toestemmingsverklaring te ondertekenen, geeft u aan dat onderstaande punten voor u gelden. Deze verklaring is nodig om deel te nemen aan dit onderzoek.

- Ik heb de informatie in de uitnodigingsbrief gelezen.
- Ik begrijp hoe ik vragen over het onderzoek kan stellen.
- Ik heb over mijn deelname aan het onderzoek kunnen nadenken.
- Ik begrijp dat ik op elk moment met het onderzoek kan stoppen en daar geen reden voor hoef op te geven.
- Ik begrijp dat alle gegevens die ik in dit onderzoek deel, anoniem worden verzameld en dus niet naar mij terug te leiden zijn.
- Ik begrijp dat er wordt gevraagd naar persoonskenmerken (leeftijd, geslacht, opleidingsniveau, werk- en woonsituatie, nationaliteit, inkomen en religiositeit), en ik ervoor kan kiezen om deze vragen niet te beantwoorden.
- Ik geef toestemming voor het gebruik van de anonieme gegevens die ik uitsluitend voor dit onderzoek deel en die uitsluitend door de onderzoekers worden gebruikt.
- Ik begrijp dat de verzamelde gegevens maximaal tien jaar, anoniem en op een veilige manier worden bewaard. (Zo kan op een later moment de kwaliteit van dit onderzoek worden gecontroleerd.)

Gelden deze punten voor u en wilt u meedoen aan het onderzoek? Klik dan hieronder om dit toestemmingsformulier te tekenen.

☐ Bovenstaande punten gelden voor mij en ik wil deelnemen aan het onderzoek.

[22] Original questionnaire (in Dutch) as administered to respondents.

Vragenlijst

Wat is een delict?
Een 'delict' is een ander woord voor een strafbaar feit. Een voorbeeld van een strafbaar feit is een fietsdiefstal. De dader is hiervoor strafbaar. Dat betekent dat de dader van een rechter een straf kan krijgen voor de fietsdiefstal. De fietsdiefstal noemen we in dit geval het delict.

Volgens onze gegevens heeft u in de periode tussen … en … melding of aangifte gedaan bij de politie van[23]

<Oplichting in persoon (zoals op straat of aan de deur)>
<Bankhelpdeskfraude (telefonische en/of online oplichting)>
<Woninginbraak>
<Misbruik van internetbankieren-account (geld overschrijven of pinnen zonder toestemming)>
<Aanranding / seksueel geweld>
<Sexting, sextortion of wraakporno>
<Bedreiging>
<Online bedreiging>

	ja	nee
Klopt het dat u melding of aangifte heeft gedaan van dit delict?	☐	☐
Nee → ga naar landingspagina 1		
Heeft u deze melding of aangifte gedaan voor uzelf?	☐	☐
Nee → ga naar landingspagina 1		

Landingspagina 1
U behoort niet tot de doelgroep van deze vragenlijst. Bedankt voor uw moeite om deel te nemen aan dit onderzoek.

Deze vragenlijst gaat over het delict waarvan u aangifte of melding deed: [...].[24]

Heeft u tussen … en …meerdere keren dit delict meegemaakt en daarvan meerdere keren aangifte of melding gedaan, neem dan de laatste keer als uitgangspunt voor deze vragenlijst.

[23] The time frame and offense varied between respondents.
[24] Refers to one of eight specific offenses on the basis of which the respondent was selected.

De vragen gaan over:

- de gevolgen van het delict voor u;
- de behoeftes die u had na het delict;
- uw persoonlijke situatie;
- het contact met de politie.

Hoe heeft u aangifte of melding bij de politie gedaan?
☐ Op het politiebureau (persoonlijk)
☐ Op de plaats van het delict
☐ Telefonisch
☐ Via internet
☐ Via een 3D-aangifteloket (tv-scherm op politiebureau)
☐ Op het politiebureau (persoonlijk)

Weet u nog of het ging om een aangifte of een melding?
☐ Melding
☐ Aangifte
☐ Weet ik niet

De volgende vragen gaan over het delict.[25]

Oplichting in persoon (zoals op straat of aan de deur)			
	ja	nee	weet ik niet
Vond de oplichting plaats in of bij uw woning (bijvoorbeeld aan de deur)?	☐	☐	☐

[25] Initial questions varied by offense type.

Bankhelpdeskfraude (telefonische en/of online oplichting)			
Kruis aan welke situatie op u het meest van toepassing is: ☐ De dader deed zich voor als bankmedewerker. ☐ De dader deed zich voor als overheidsmedewerker (bijvoorbeeld van de politie, een ministerie of rechtbank). ☐ De dader zei te werken bij een andere instantie, namelijk: [open text field]			
	ja	nee	weet ik niet
Is de besturing over uw computer overgenomen, zodat de dader deze kon bedienen?	☐	☐	☐

Woninginbraak			
	ja	nee	weet ik niet
Zijn er spullen van u gestolen die voor u emotionele waarde hadden?	☐	☐	☐

Misbruik van internetbankieren-account (geld overschrijven of pinnen zonder uw toestemming)
Kruis aan welke situatie op u het meest van toepassing is: ☐ Ik had contact over een koop of verkoop (bijvoorbeeld via Marktplaats of Facebook Marketplace). Hierbij vroeg de dader om mijn bankgegevens in te voeren of een klein bedrag te betalen, bijvoorbeeld voor een betaalservice, verificatie, identiteitscontrole, verzekering of verzendkosten. Ik heb toen mijn gegevens ingevoerd. ☐ Ik heb mijn gegevens ingevoerd na het klikken op een link in een bericht (bijvoorbeeld e-mail of sms) die van een betrouwbare instantie leek te komen. ☐ Ik weet niet hoe de daders misbruik hebben kunnen maken van mijn online bankaccount. ☐ De daders zijn op een andere manier aan de gegevens van mijn online bankaccount gekomen, namelijk: [open text field]

Aanranding			
	ja	nee	weet ik niet
Was er bij de aanranding sprake van geweld of bedreiging met geweld door de dader(s)?	☐	☐	☐

Sexting, sextortion of wraakporno
a. Kruis aan welke situatie op u het meest van toepassing is:
☐ Iemand beschikte tegen mijn wil over seksueel getint beeldmateriaal van mij (bijvoorbeeld naaktfoto's of filmpjes) en heeft dit verspreid.
☐ Iemand beschikte tegen mijn wil over seksueel getint beeldmateriaal van mij (bijvoorbeeld naaktfoto's of filmpjes) en dreigde met verspreiding hiervan.
☐ Ik heb seksueel getint beeldmateriaal van mij (bijvoorbeeld naaktfoto's of filmpjes) naar iemand opgestuurd. Daarna is dit materiaal tegen mijn wil verspreid.
☐ Ik heb seksueel getint beeldmateriaal van mij (bijvoorbeeld naaktfoto's of filmpjes) naar iemand opgestuurd. Daarna werd er gedreigd met verspreiding van dit materiaal.
☐ Anders, namelijk: [open text field]

	ja	nee	weet ik niet
b. Vroeg de dader u om geld om verspreiding van het beeldmateriaal te voorkomen?	☐	☐	☐
Ja → Heeft u toen betaald om verspreiding van het beeldmateriaal te voorkomen?	☐	☐	☐
c. Vroeg de dader u om meer seksueel getint beeldmateriaal van u om verspreiding van het beeldmateriaal te voorkomen?	☐	☐	☐
Ja → Heeft u toen meer seksueel getint beeldmateriaal van u verstuurd om verspreiding van het beeldmateriaal te voorkomen?	☐	☐	☐

Bedreiging
Kruis aan welke situatie op u het meest van toepassing is:
☐ Ik ben in de openbare ruimte (bijvoorbeeld op straat of in een overheidsgebouw) bedreigd met de dood.
☐ Ik ben in de openbare ruimte (bijvoorbeeld op straat of in een overheidsgebouw) bedreigd met iets anders (bijvoorbeeld zware mishandeling).
☐ Ik ben thuis bedreigd met de dood.
☐ Ik ben thuis bedreigd met iets anders (bijvoorbeeld zware mishandeling).
☐ Ik ben ergens anders bedreigd met de dood.
☐ Ik ben ergens anders bedreigd met iets anders (bijvoorbeeld zware mishandeling).
☐ Ik ben op een andere manier bedreigd, namelijk: [open text field]

Online bedreiging
a. Kruis aan welke situatie op u het meest van toepassing is:
☐ Ik ben online bedreigd met de dood.
☐ Ik ben online bedreigd met iets anders (bijvoorbeeld zware mishandeling).
b. Kruis aan welke situatie op u het meest van toepassing is (meerdere antwoorden mogelijk):
☐ Ik ben via e-mail bedreigd.
☐ Ik ben via een berichtenservice (bijvoorbeeld WhatsApp of Signal) of via sms bedreigd.
☐ Ik ben via sociale media (bijvoorbeeld Instagram, Twitter of Facebook) bedreigd via een privébericht (DM).
☐ Ik ben via sociale media (bijvoorbeeld Instagram, Twitter of Facebook) bedreigd via een bericht dat anderen ook konden zien.
☐ Ik ben op een andere manier bedreigd, namelijk: [open text field]

De volgende vragen gaan over de kenmerken van het delict waarvan u aangifte of melding deed.

1.			
a.	Kruis aan welke situatie op u het meest van toepassing is:		
	☐ Ik kende de dader(s) niet.		
	☐ Ik kende de dader(s) een beetje.		
	☐ Ik kende de dader(s) goed.		
	☐ Ik weet niet of ik de dader(s) kende.		
b.	Do the following statements apply to the offense?	ja	nee
	De dader heeft me overtuigd of misleid om me iets te laten doen of toe te laten.	☐	☐
	Ik heb tijdens het delict direct contact gehad met de dader (bijvoorbeeld telefonisch, via een berichtenservice zoals WhatsApp of persoonlijk).	☐	☐
	Ik was thuis toen het delict plaatsvond of toen ik ontdekte dat het delict had plaatsgevonden.	☐	☐
c.	Zijn de volgende stellingen van toepassing (schaal van 1: zeker niet, tot 5: zeker wel)?	zeker niet	zeker wel
	Naar mijn idee was het delict specifiek op mij gericht.	1☐ 2☐ 3☐ 4☐ 5☐	
	Door mijn eigen reactie tijdens het delict heb ik erger weten te voorkomen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Het delict kwam voor mij onverwachts.	1☐ 2☐ 3☐ 4☐ 5☐	
	Terugkijkend op de ervaring, had ik destijds kunnen voorkomen dat het delict plaatsvond.	1☐ 2☐ 3☐ 4☐ 5☐	

2. Hoe lang duurde het delict waarvan u aangifte of melding deed?
☐ Eenmalig
☐ Minder dan 1 week
☐ Meer dan 1 week maar minder dan 1 maand
☐ Langer dan 1 maand maar minder dan 3 maanden
☐ 3 maanden tot een half jaar
☐ Half jaar tot een jaar
☐ Langer dan 1 jaar
☐ Weet ik niet

We vragen u nu eerst naar de gevolgen van het delict **toen het plaatsvond of toen u ontdekte dat het had plaatsgevonden**.

Eerst vragen we u naar de gevolgen van het delict toen u ontdekte dat het delict plaatsvond of had plaatsgevonden.

3. Had het delict toen het plaatsvond of toen u ontdekte dat het had plaatsgevonden voor u de volgende gevolgen (schaal van 1: niet ervaren, tot 5: zeer sterk ervaren)?		
	toen niet ervaren	toen sterk ervaren
Ik was hierdoor in psychische shock (acute, ernstige stress).	1☐ 2☐ 3☐ 4☐ 5☐	
Ik ontkende wat er gebeurd was of kon het moeilijk geloven.	1☐ 2☐ 3☐ 4☐ 5☐	
Ik voelde me hierdoor wanhopig.	1☐ 2☐ 3☐ 4☐ 5☐	
Ik voelde me hierdoor hulpeloos.	1☐ 2☐ 3☐ 4☐ 5☐	
Ik had hierdoor lichamelijke klachten zoals hartkloppingen, duizeligheid, trillen of buikpijn.	1☐ 2☐ 3☐ 4☐ 5☐	
Andere gevolgen, namelijk: [open text field]		

4. Heeft u professionele hulp ingeschakeld als gevolg van het delict (bijvoorbeeld Slachtofferhulp Nederland of psychologische begeleiding)?
☐ Ja
☐ Nee
☐ Weet ik niet
☐ Zeg ik liever niet

5. Hoeveel tijd kostte het u om na het delict de eerste maatregelen te nemen (bijvoorbeeld aan herstelwerk, inschakelen van hulp, naar de politie gaan)?

☐ Minder dan 1 uur
☐ Tussen 1 en 5 uur
☐ Tussen 5 en 10 uur
☐ Tussen 10 en 20 uur
☐ Meer dan 20 uur
☐ Weet ik niet

We bedoelen hieronder de **directe financiële schade** voordat u eventueel schadevergoeding kreeg. Tel daarbij **niet** de eventuele schade door het herstel of de afhandeling van het delict.

6. Wat was de directe financiële schade door het delict (zoals geld dat van u is weggenomen)?

☐ Het delict leverde voor mij geen directe schade op → *ga naar vraag 8*
☐ Minder dan €100
☐ Tussen €100 en €500
☐ Tussen €501 en €1.000
☐ Tussen €1.001 en €2.000
☐ Tussen €2.001 en €5.000
☐ Tussen €5.001 en €10.000
☐ Tussen €10.001 en €50.000
☐ Meer dan €50.000
☐ Weet ik niet
☐ Zeg ik liever niet

7. Heeft u daar iets van teruggekregen of gaat u dit nog terugkrijgen (bijvoorbeeld via de bank, een verzekering of andere instantie)?

☐ Ja, het hele schadebedrag
☐ Ja, het grootste deel van het schadebedrag
☐ Ja, een deel van het schadebedrag maar niet het grootste deel
☐ Nee, niet geprobeerd
☐ Nee, wel geprobeerd maar niet ontvangen
☐ Weet ik (nog) niet
☐ Zeg ik liever niet

We bedoelen hieronder de **indirecte financiële schade** voordat u eventueel schadevergoeding kreeg.

8. Wat was de indirecte financiële schade door het delict voor het herstel of de afhandeling ervan (zoals vervanging van spullen of hulp bij de verwerking)?

☐ Het delict leverde voor mij geen indirecte schade op → *ga naar vraag 10*

☐ Minder dan €100

☐ Tussen €100 en €500

☐ Tussen €501 en €1.000

☐ Tussen €1.001 en €2.000

☐ Tussen €2.001 en €5.000

☐ Tussen €5.001 en €10.000

☐ Tussen €10.001 en €50.000

☐ Meer dan €50.000

☐ Weet ik niet

☐ Zeg ik liever niet

9. Heeft u daar iets van teruggekregen of gaat u dit nog terugkrijgen (bijvoorbeeld via de bank, een verzekering of andere instantie)?

☐ Ja, het hele schadebedrag

☐ Ja, het grootste deel van het schadebedrag

☐ Ja, een deel van het schadebedrag, maar niet het grootste deel

☐ Nee, niet geprobeerd

☐ Nee, wel geprobeerd maar niet ontvangen

☐ Weet ik (nog) niet

☐ Zeg ik liever niet

De volgende vragen gaan over de gevolgen die het delict op dit moment voor u heeft.

10.			
a.	*Heeft het delict op dit moment de volgende emotionele gevolgen voor u (schaal van 1: niet, tot 5: zeer sterk)?*		
		ervaar ik nu niet	ervaar ik nu zeer sterk
	Ik ervaar hierdoor stress of spanning.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik heb hierdoor angst- of paniekklachten.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik maak me hier boos over.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik ben hier gefrustreerd of geïrriteerd over.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik geef mezelf de schuld van wat er gebeurd is.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik schaam me voor wat er gebeurd is.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik heb hierdoor minder zelfvertrouwen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Mijn gevoel van eigenwaarde is hierdoor lager.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik ben hierdoor voorzichtiger geworden.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik denk vaak aan wat er gebeurd is.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik beleef de gebeurtenis steeds opnieuw.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik voel me hierdoor depressief, verdrietig of neerslachtig.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik ben hierdoor bang om nog een keer zoiets mee te maken.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik ervaar hierdoor een inbreuk op mijn privacy.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik voel me hierdoor op het internet (waaronder online apps en sociale media/WhatsApp) minder veilig.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik voel me hierdoor in de fysieke ruimte (zoals thuis, op straat of op andere plaatsen binnen of buiten) minder veilig.	1☐ 2☐ 3☐ 4☐ 5☐	
	Andere emotionele gevolgen, namelijk: [open text field]		
b.	*Heeft het delict op dit moment de volgende sociale of gedragsmatige gevolgen voor u (schaal van 1: niet, tot 5: zeer sterk)?*		
	Ik heb hierdoor minder contact met andere mensen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik durf me hierdoor op het internet (waaronder online apps en sociale media/WhatsApp) minder vrij te uiten.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik durf me hierdoor in de fysieke ruimte (zoals thuis, op straat of op andere plaatsen binnen of buiten) minder vrij te uiten.	1☐ 2☐ 3☐ 4☐ 5☐	

	Ik vermijd hierdoor bepaalde plaatsen of situaties op het internet (waaronder online apps en sociale media/ WhatsApp).	1☐ 2☐ 3☐ 4☐ 5☐
	Ik vermijd hierdoor bepaalde plaatsen of situaties in de fysieke ruimte (zoals thuis, op straat of op andere plaatsen binnen of buiten).	1☐ 2☐ 3☐ 4☐ 5☐
	Ik heb hierdoor minder vertrouwen in andere mensen.	1☐ 2☐ 3☐ 4☐ 5☐
	Ik heb hierdoor wraakgevoelens tegenover de dader(s).	1☐ 2☐ 3☐ 4☐ 5☐
	Ik functioneer hierdoor minder goed in mijn werk / studie.	1☐ 2☐ 3☐ 4☐ 5☐
	Ik neem hierdoor maatregelen om niet nogmaals een soortgelijk delict mee te maken.	1☐ 2☐ 3☐ 4☐ 5☐
	Ik heb hierdoor problemen in mijn relaties (met bijvoorbeeld partner, vrienden of familie).	1☐ 2☐ 3☐ 4☐ 5☐
	Andere sociale of gedragsmatige gevolgen, namelijk: [open text field]	
c.	*Heeft het delict op dit moment de volgende lichamelijke gevolgen voor u (schaal van 1: niet, tot 5: zeer sterk)?*	
	Ik slaap hierdoor slechter.	1☐ 2☐ 3☐ 4☐ 5☐
	Ik heb hierdoor last van hoofdpijn.	1☐ 2☐ 3☐ 4☐ 5☐
	Ik heb hierdoor last van misselijkheid.	1☐ 2☐ 3☐ 4☐ 5☐
	Ik wil hierdoor niet meer leven of heb hier gedachten over.	1☐ 2☐ 3☐ 4☐ 5☐
	Mijn gewicht is hierdoor veranderd.	1☐ 2☐ 3☐ 4☐ 5☐
	Ik heb hierdoor concentratieproblemen.	1☐ 2☐ 3☐ 4☐ 5☐
	Andere lichamelijke gevolgen, namelijk: [open text field]	
d.	*Heeft het delict op dit moment de volgende financiële gevolgen voor u (schaal van 1: niet, tot 5: zeer sterk)?*	
	Ik heb hierdoor minder inkomen.	1☐ 2☐ 3☐ 4☐ 5☐
	De financiële schade die ik hierdoor lijd is voor mij aanzienlijk.	1☐ 2☐ 3☐ 4☐ 5☐
	Ik heb hierdoor financiële problemen.	1☐ 2☐ 3☐ 4☐ 5☐
	Andere financiële gevolgen, namelijk: [open text field]	

De volgende vragen gaan over behoeftes die u had door het delict in de periode vlak na het delict.

11.	Had u in de periode vlak na het delict de volgende behoeftes (schaal van 1: deze behoefte had ik niet, tot 5: deze behoefte had ik zeer sterk)?		
		had ik niet	had ik zeer sterk
	Weten waar ik terecht kon voor hulp en ondersteuning tijdens of na het delict.	1☐ 2☐ 3☐ 4☐ 5☐	
	Erkenning van het delict dat me is overkomen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Serieus genomen worden als slachtoffer.	1☐ 2☐ 3☐ 4☐ 5☐	
	Praktische hulp bij door het delict ontstane problemen, bijvoorbeeld bij herstel of het regelen van zaken.	1☐ 2☐ 3☐ 4☐ 5☐	
	Informatie over het delict en hoe het heeft kunnen plaatsvinden.	1☐ 2☐ 3☐ 4☐ 5☐	
	Financiële compensatie voor de schade die ik heb geleden.	1☐ 2☐ 3☐ 4☐ 5☐	
	Opsporing, aanhouding en vervolging van de dader.	1☐ 2☐ 3☐ 4☐ 5☐	
	Iemand om mee te praten met wie ik mijn gevoelens kon delen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Advies om te voorkomen dat ik nog eens zo'n delict meemaak.	1☐ 2☐ 3☐ 4☐ 5☐	
	Professionele therapie of begeleiding om de gevolgen van het delict te verwerken.	1☐ 2☐ 3☐ 4☐ 5☐	
	Voorkomen dat andere mensen hetzelfde delict meemaken.	1☐ 2☐ 3☐ 4☐ 5☐	
	Andere behoeftes, namelijk: [open text field]		

De volgende vragen gaan over enkele persoonlijke omstandigheden in relatie tot het delict dat u heeft meegemaakt.

12.	Zijn de volgende stellingen op u van toepassing (schaal van 1: zeker niet, tot 5: zeker wel)?		
		zeker niet	zeker wel
	Het voelt soms alsof het delict mij niet echt is overkomen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik heb geleerd van het delict.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik zie mezelf als slachtoffer van het delict dat me is overkomen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik kan het delict en de gevolgen ervan zelf oplossen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik heb na het delict voldoende ondersteuning gekregen van mijn omgeving (bijvoorbeeld partner, vrienden of familie).	1☐ 2☐ 3☐ 4☐ 5☐	
	Mijn omgeving (bijvoorbeeld partner, vrienden of familie) geeft mij de schuld van het delict.	1☐ 2☐ 3☐ 4☐ 5☐	
	Mijn omgeving (bijvoorbeeld partner, vrienden of familie) begrijpt wat ik heb doorgemaakt.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik vind het moeilijk om mensen te vertellen over het delict dat ik heb meegemaakt.	1☐ 2☐ 3☐ 4☐ 5☐	
	De maatschappij neemt het delict dat ik heb meegemaakt serieus.	1☐ 2☐ 3☐ 4☐ 5☐	

De volgende vragen gaan over persoonlijke omstandigheden.

13.	Zijn de volgende stellingen op u van toepassing (schaal van 1: zeker niet, tot 5: zeker wel)?		
		zeker niet	zeker wel
	Voordat het delict plaatsvond, had ik psychologische problemen.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik heb in mijn leven zware tegenslagen meegemaakt, zoals een traumatische ervaring of ernstige ziekte / dood van een partner of nabije familie.	1☐ 2☐ 3☐ 4☐ 5☐	
	Voordat het delict plaatsvond, had ik een positief beeld over de wereld.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik doe dingen vaak in een opwelling, zonder er lang over na te denken.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik zou me onrustig voelen als ik 24 uur geen toegang zou hebben tot het internet (waaronder online apps en sociale media/WhatsApp).	1☐ 2☐ 3☐ 4☐ 5☐	
	Mijn digitale identiteit (bijvoorbeeld op sociale media) is een onlosmakelijk onderdeel van mijn algehele identiteit.	1☐ 2☐ 3☐ 4☐ 5☐	

14. Hoeveel tijd brengt u per dag op het internet door (waaronder online apps en sociale media/ WhatsApp), inclusief voor werk of studie?

☐ Minder dan 1 uur

☐ Tussen 1 en 2 uur

☐ Tussen 2 en 5 uur

☐ Tussen 5 en 10 uur

☐ Tussen 10 en 15 uur

☐ Meer dan 15 uur

☐ Weet ik niet

15. Heeft u in de afgelopen 2 jaar vaker hetzelfde delict persoonlijk meegemaakt?

☐ Ja

☐ Nee

☐ Weet ik niet

☐ Zeg ik liever niet

16. Heeft u in de afgelopen 2 jaar een ander delict persoonlijk meegemaakt?

☐ Ja

☐ Nee

☐ Weet ik niet

☐ Zeg ik liever niet

De volgende vragen gaan over uw ervaring met de politie vanwege het delict waarvan u aangifte of melding deed.

17.	Zijn de volgende stellingen op u van toepassing (schaal van 1: zeker niet, tot 5: zeker wel)?		
		zeker niet	zeker wel
	Ik kon mijn verhaal kwijt bij de politie.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik kreeg voldoende informatie van de politie over het delict en hoe dit kon gebeuren.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik kreeg voldoende advies van de politie over hoe ik kan voorkomen om nog eens zo'n delict mee te maken.	1☐ 2☐ 3☐ 4☐ 5☐	
	De politie had te weinig kennis om mij goed te kunnen helpen.	1☐ 2☐ 3☐ 4☐ 5☐	
	De politie onderschatte de gevolgen die het delict voor mij had.	1☐ 2☐ 3☐ 4☐ 5☐	
	Voor mijn gevoel gaf de politie mij de schuld van het delict.	1☐ 2☐ 3☐ 4☐ 5☐	
	De politie heeft mijn aangifte of melding behandeld als een dringende zaak.	1☐ 2☐ 3☐ 4☐ 5☐	
	De politie heeft genoeg inspanning verricht na mijn aangifte of melding.	1☐ 2☐ 3☐ 4☐ 5☐	
	Ik kreeg voldoende informatie van de politie over wat ze gedaan hebben of nog gaan doen met mijn aangifte of melding.	1☐ 2☐ 3☐ 4☐ 5☐	
	De negatieve gevolgen van het delict namen af door hoe de politie mijn aangifte of melding heeft behandeld.	1☐ 2☐ 3☐ 4☐ 5☐	
	De negatieve gevolgen van het delict namen toe door hoe de politie mijn aangifte of melding heeft behandeld.	1☐ 2☐ 3☐ 4☐ 5☐	
	Wilt u verder nog iets kwijt over uw ervaring bij de politie, bijvoorbeeld in relatie tot de behoeftes die u had? …		

Graag sluiten we af met vragen over persoonskenmerken.

18.	Wat is uw geslacht?
☐	Man
☐	Vrouw
☐	Non-binair
☐	Zeg ik liever niet

19.	Wat is uw geboortejaar (jjjj)?
....[26]	
☐	Zeg ik liever niet

20.	Wat is de hoogste opleiding die u heeft afgerond met een diploma, akte of getuigschrift?
☐	Geen opleiding
☐	Lagere school (inclusief speciaal onderwijs, bijvoorbeeld lom, blo, enzovoort)
☐	Lager beroepsonderwijs (lbo, lts), vmbo basisberoepsgerichte of kaderberoepsgerichte leerweg
☐	Mavo, vmbo theoretische of gemengde leerweg, ulo, mulo
☐	Havo, vwo, gymnasium, hbs, mms
☐	Middelbaar beroepsonderwijs (mbo, bol, bbl)
☐	Propedeuse, kandidaats, bachelor, hoger beroepsonderwijs (hbo)
☐	Doctoraal, master, wetenschappelijk onderwijs (wo)
☐	Doctoraat, PhD
☐	Weet ik niet

21.	Welke omschrijving past het beste bij u?
☐	Werkende met betaald werk / zelfstandige → *ga naar vraag 22*
☐	Werkloos / tussen twee banen in
☐	Vrijwilliger
☐	Arbeidsongeschikt
☐	Scholier of studerende
☐	Huisman / huisvrouw
☐	Gepensioneerd of met de VUT
☐	Geen van deze
☐	Weet ik niet
☐	Zeg ik liever niet

22.	Werkt u gemiddeld 12 uur per week of meer?
☐	Ja
☐	Nee
☐	Weet ik niet
☐	Zeg ik liever niet

[26] This item was presented as a multiple-choice question in the original questionnaire.

23.	Uit hoeveel personen bestaat uw huishouden, uzelf meegerekend? (voer een getal in)
1 → ga naar vraag 25	
☐	Zeg ik liever niet
☐	1
☐	2
☐	3
☐	4
☐	5
☐	6
☐	7
☐	8
☐	9
☐	10
☐	11
☐	12
☐	13
☐	14
☐	15
☐	Meer dan 15

24.	Hoeveel personen daarvan zijn jonger dan 15 jaar?
☐	Zeg ik liever niet
☐	0 (geen)
☐	1
☐	2
☐	3
☐	4
☐	5
☐	6
☐	7
☐	8
☐	9
☐	10
☐	11
☐	12
☐	13
☐	14
☐	Meer dan 14

Deze vraag gaat over uw **bruto jaarinkomen**, niet om het inkomen van eventuele andere leden van uw huishouden.

25.	Wat was uw bruto jaarinkomen in 2021?
☐	€10.000 of minder
☐	€10.001 - €20.000
☐	€20.001 - €30.000
☐	€30.001 - €40.000
☐	€40.001 - €50.000
☐	€50.001 - €60.000
☐	€60.001 - €70.000
☐	€70.001 - €80.000
☐	€80.001 - €90.000
☐	€90.001 - €100.000
☐	Meer dan €100.000
☐	Weet ik niet
☐	Zeg ik liever niet

26.	Wat was het totale gezamenlijke bruto jaarinkomen van alle leden van uw huishouden in 2021?
☐	€10.000 of minder
☐	€10.001 - €20.000
☐	€20.001 - €30.000
☐	€30.001 - €40.000
☐	€40.001 - €50.000
☐	€50.001 - €60.000
☐	€60.001 - €80.000
☐	€80.001 - €100.000
☐	€100.001 - €150.000
☐	€150.001 - €200.000
☐	Meer dan €200.000
☐	Weet ik niet
☐	Zeg ik liever niet

27.	Welke situatie past het beste bij u?
☐	Gehuwd of geregistreerd partnerschap
☐	Samenwonend
☐	Ongehuwd / alleenstaand
☐	Gescheiden
☐	Verweduwd
☐	Zeg ik liever niet

28.	Rekent u zichzelf tot een religieuze of levensbeschouwelijke groep
☐	Ja
☐	Nee
☐	Weet ik niet
☐	Zeg ik liever niet

29.	Wat is uw nationaliteit? (meerdere antwoorden mogelijk)
☐	Nederlandse nationaliteit
☐	Andere nationaliteit
☐	Beide (Nederlandse en andere nationaliteit)
☐	Zeg ik liever niet

Hartelijk dank voor uw deelname aan dit onderzoek. Dankzij uw deelname kunnen we onderzoeken wat de gevolgen van delicten voor slachtoffers zijn. Hiermee krijgen we inzicht in hoe we ons werk op het gebied van slachtofferzorg en criminaliteitsbestrijding kunnen verbeteren.

Mogen wij u eventueel later uitnodigen voor een persoonlijk gesprek? In dit gesprek kunnen we meer vragen stellen over de impact van het delict. Als wij u hiervoor mogen uitnodigen, stuur dan een e-mail naar [email address omitted].

Dit onderzoek gaat over de gevolgen van criminaliteit, die ingrijpend kunnen zijn. Voor emotionele steun, hulp in het strafproces of ondersteuning bij het vergoed krijgen van uw schade kunt u gaan naar www.slachtofferhulp.nl, of bellen naar 0900 - 01 01.

Appendix 4. Victim impact interactions – Chapter 5

The figures presented in this Appendix illustrate statistically significant interaction effects ($p < .01$) between crime type and another determinant across four impact types: internalizing problems, externalizing problems, financial impact, and damaged self-image. These statistically significant findings suggest that the influence of the other determining factor on the impact varies between victims of cybercrime and victims of traditional crime.

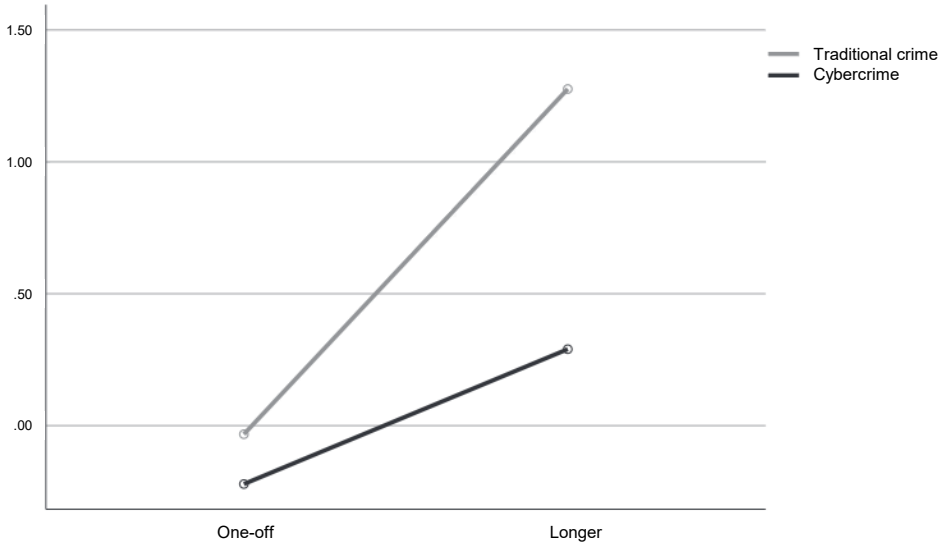


Figure A.4.1. Mean internalizing problems by crime type and duration.

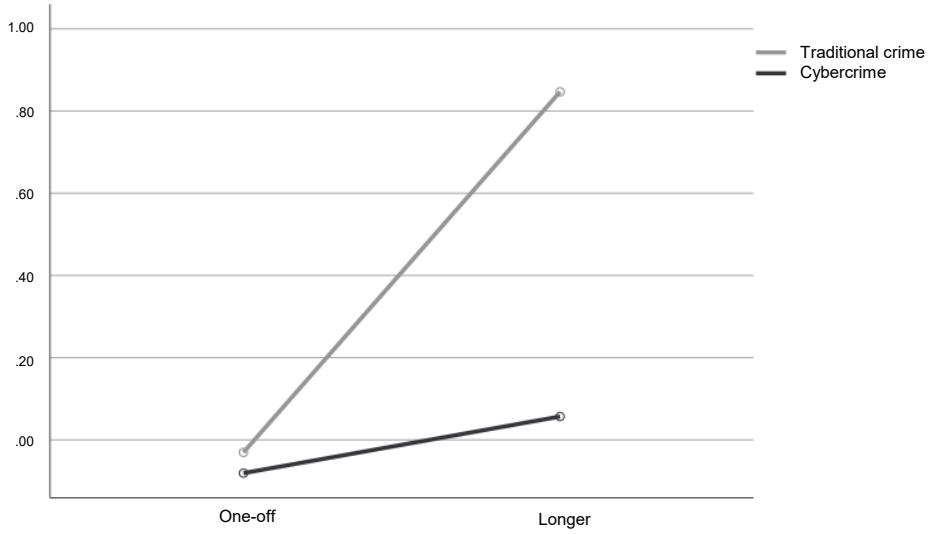


Figure A.4.2. Mean externalizing problems by crime type and duration.

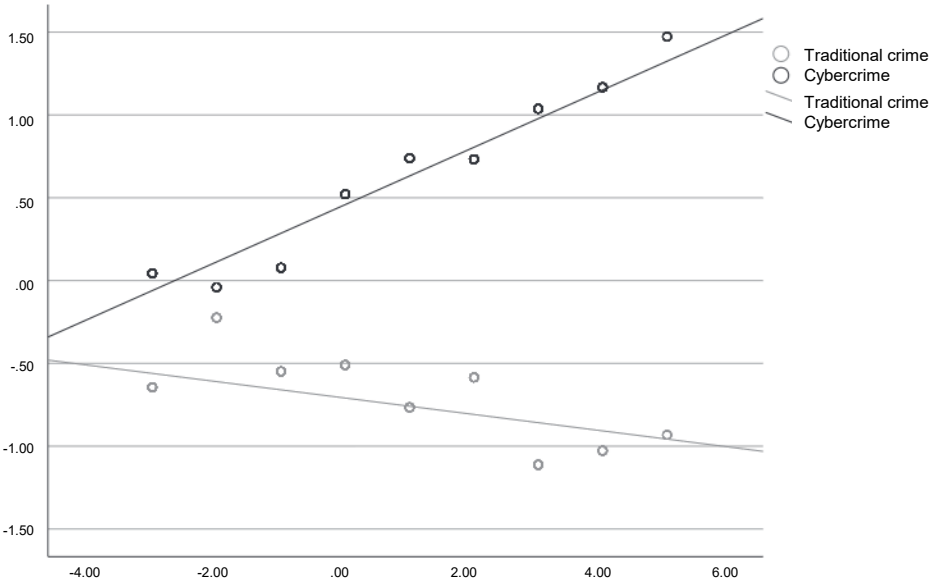


Figure A.4.3. Mean damaged self-image by crime type and financial damage.

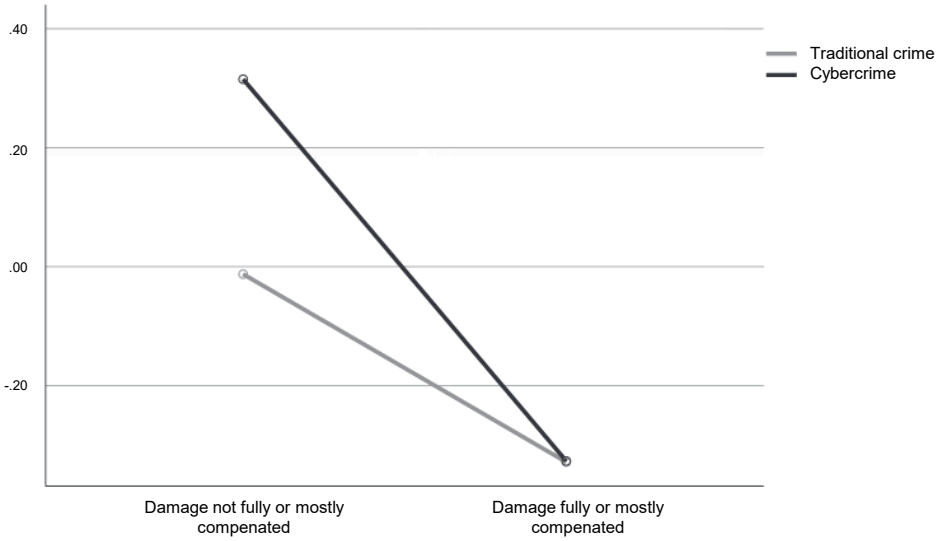


Figure A.4.4. Mean internalizing problems by crime type and damage compensation.

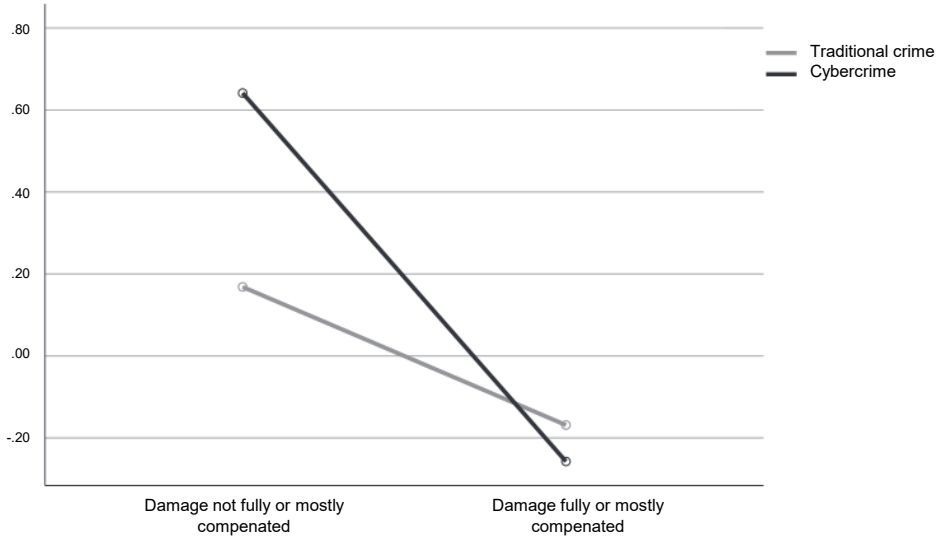


Figure A.4.5. Mean financial impact by crime type and damage compensation.

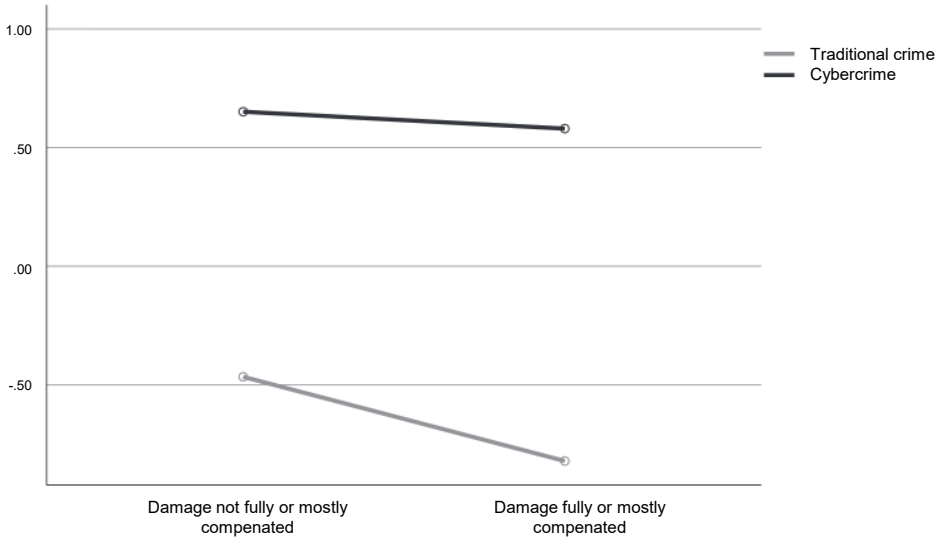


Figure A.4.6. Mean damaged self-image by crime type and damage compensation.

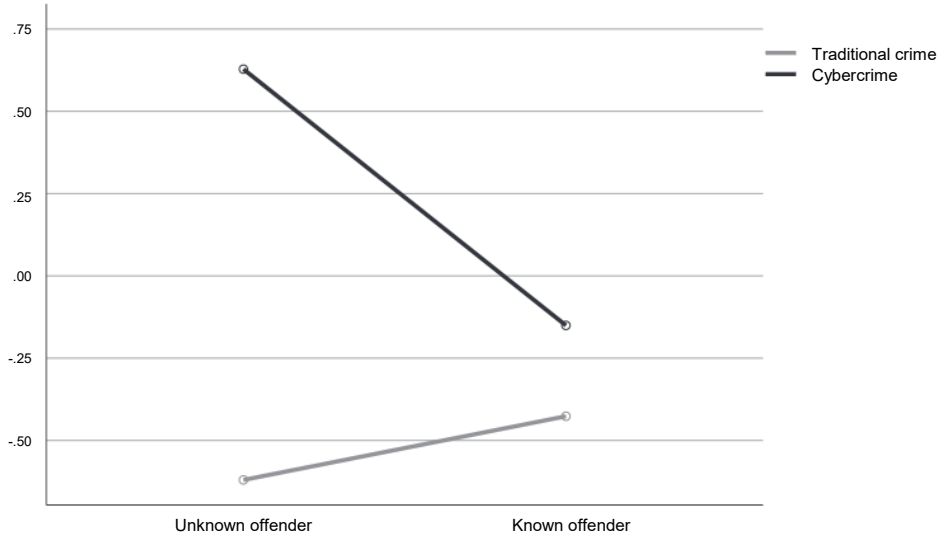


Figure A.4.7. Mean damaged self-image by crime type and known offender.

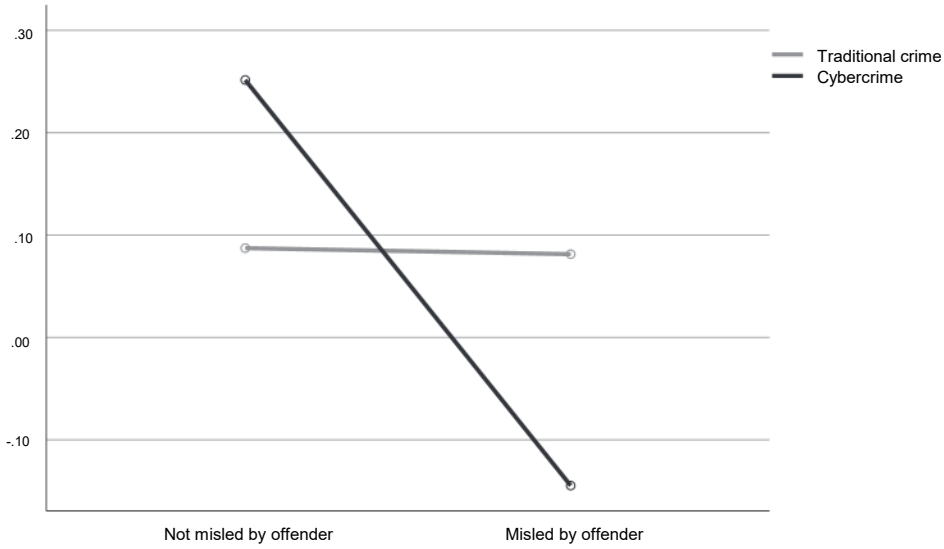


Figure A.4.8. Mean internalizing impact by crime type and misleading offender.

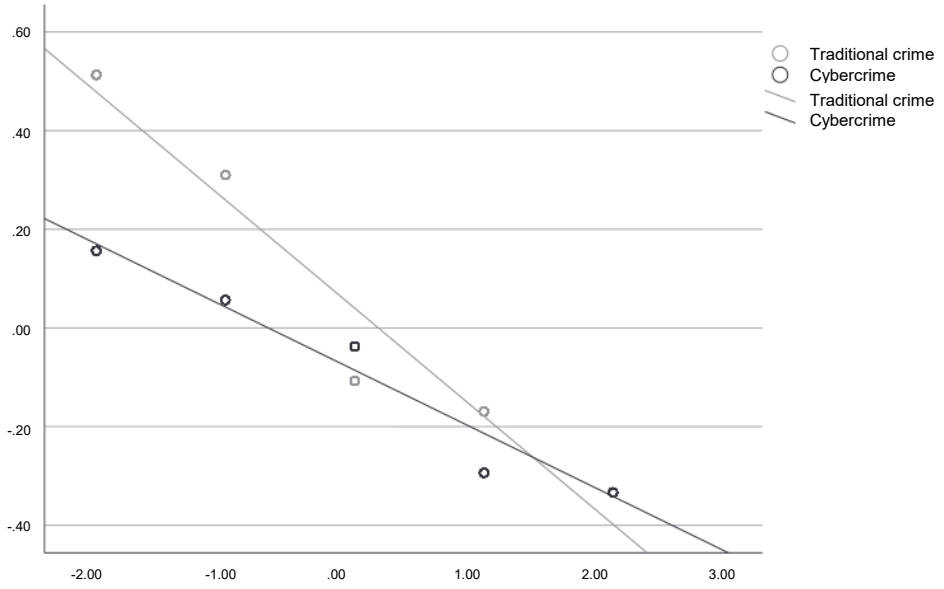


Figure A.4.9. Mean internalizing impact by crime type and self-efficacy.

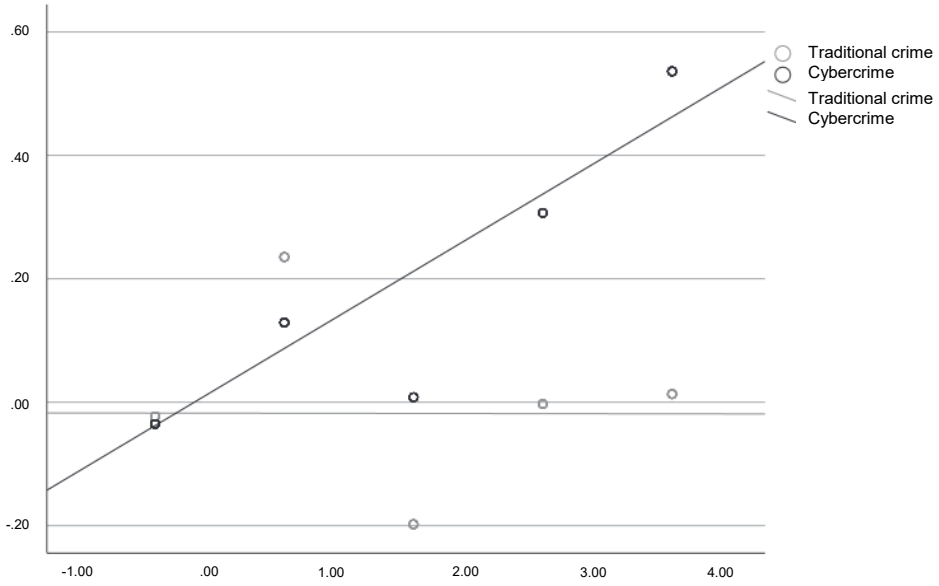


Figure A.4.10. Mean financial impact by crime type and psychological problems.

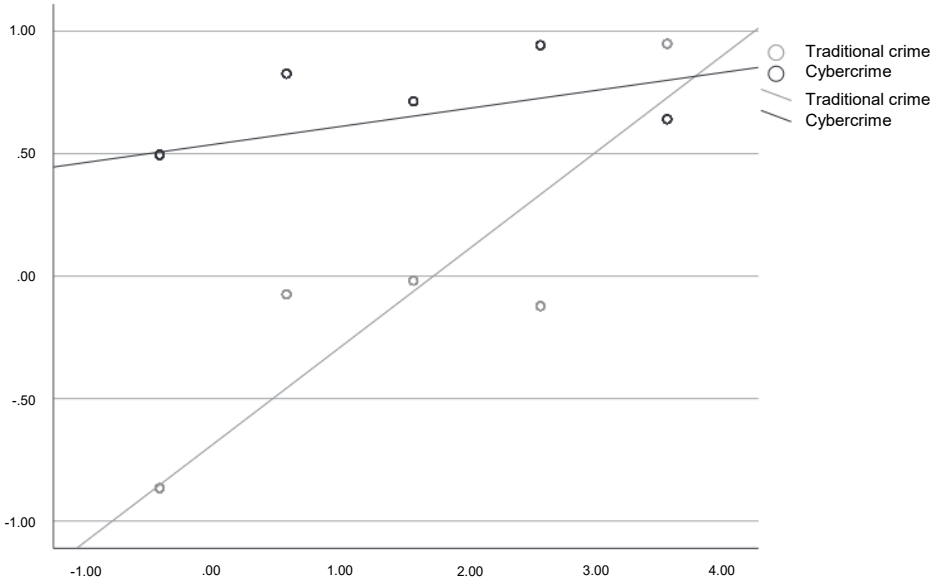


Figure A.4.11. Mean damaged self-image by crime type and psychological problems.

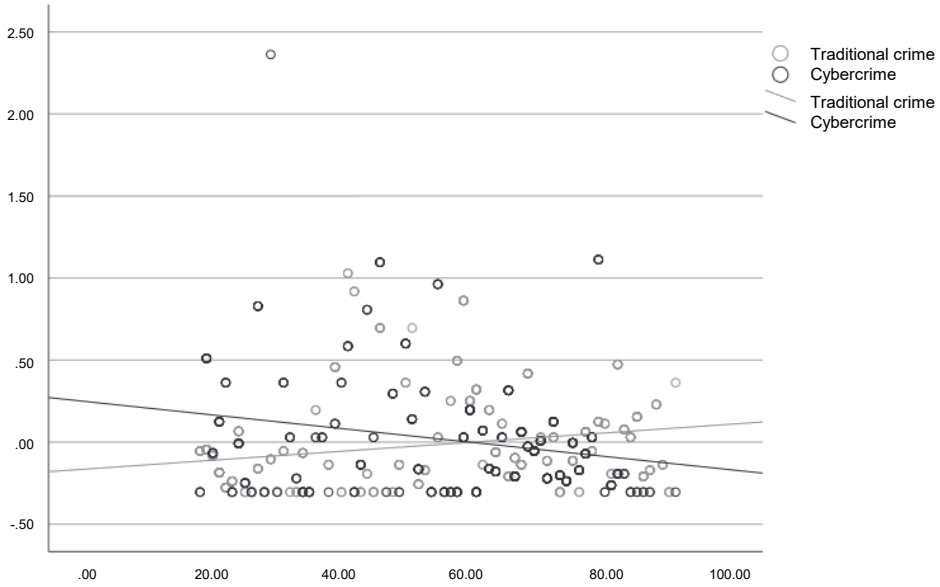


Figure A.4.12. Mean financial impact by crime type and age.[27]

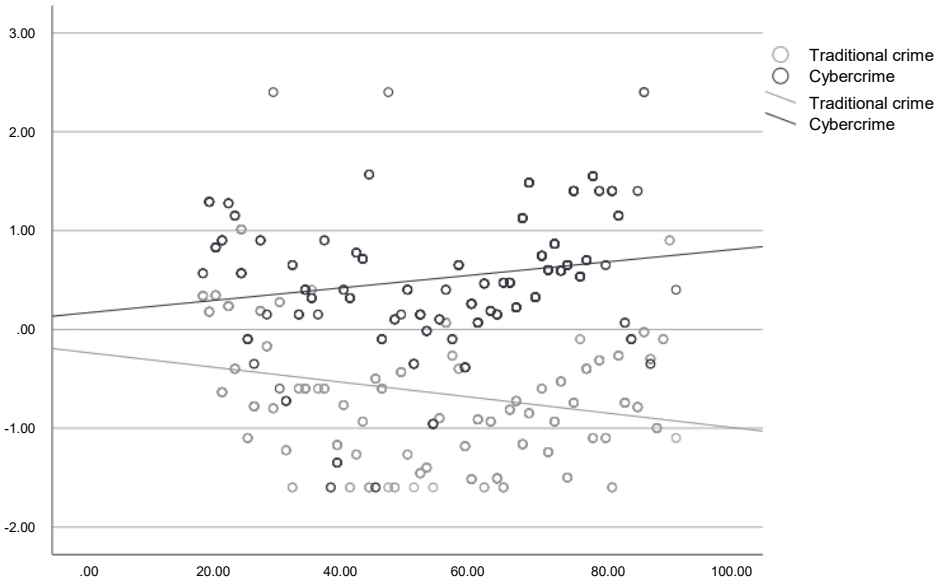
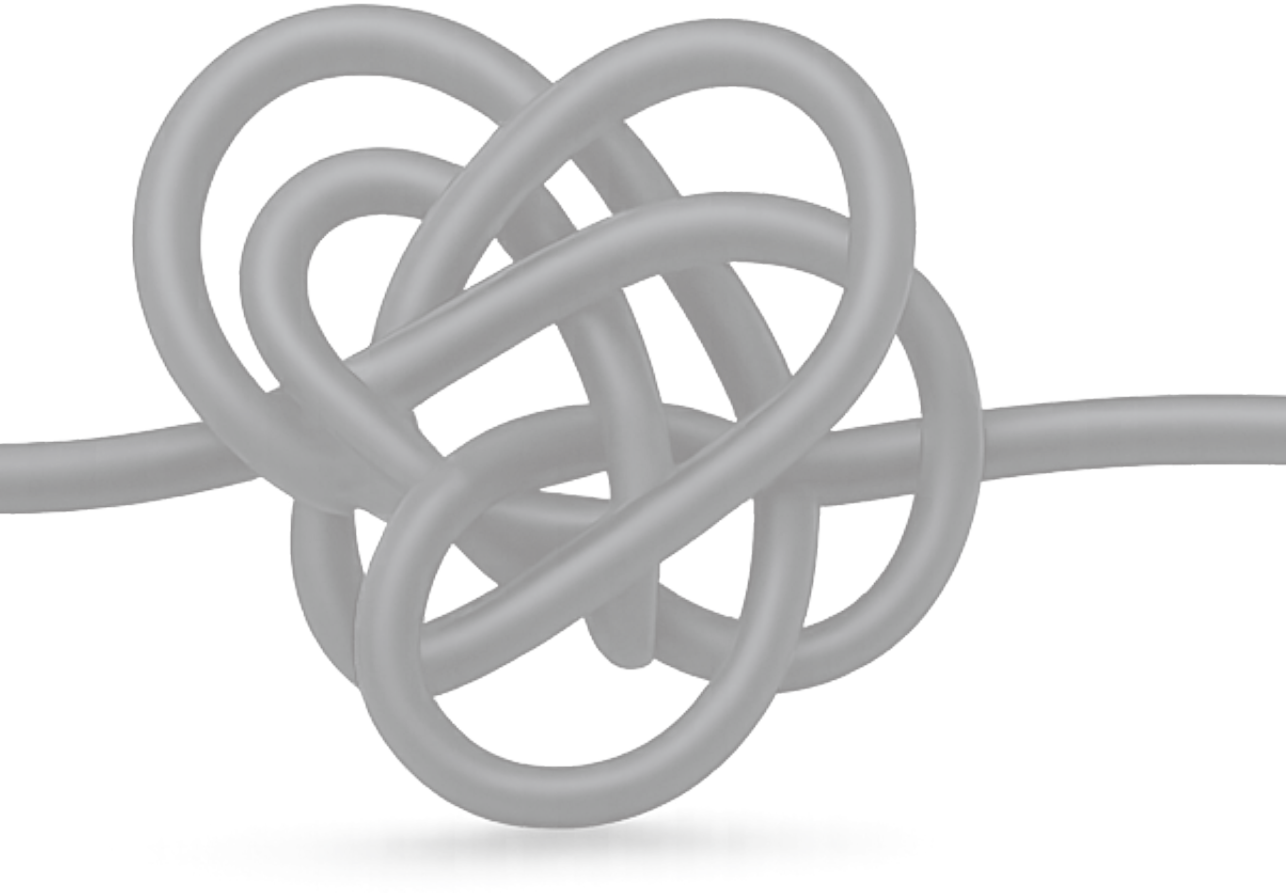


Figure A.4.13. Mean damaged self-image by crime type and age.[28]

[27] Non-centered variable displayed for graph interpretation.
[28] Non-centered variable displayed for graph interpretation.



Samenvatting (summary in Dutch)

De impact van cybercrime ontrafeld: Inzicht in slachtofferervaringen en implicaties voor de politiepraktijk

Inleiding

Dit proefschrift gaat over de impact van cybercrime op de slachtoffers ervan. Een van de keerzijden van digitalisering is de opkomst van cybercrime. De vormen van criminaliteit die hieronder vallen hebben ingrijpende gevolgen voor slachtoffers, die minstens zo groot zijn als de gevolgen van traditionele criminaliteit, zo blijkt uit dit proefschrift. Toch lijken de politie, andere publieke en private organisaties en burgers deze impact vaak te onderschatten. Dit proefschrift laat, vanuit een slachtoffergerichte benadering, zien hoe slachtoffers de impact van cybercrime ervaren, welke behoeften daaruit voorkomen, en wat dit betekent voor de rol van de politie en partnerorganisaties. De ervaringen en percepties van slachtoffers staan centraal: hoe zij de ernst en gevolgen van het delict beleven, welke emoties en praktische problemen daaruit voortvloeien, en welke ondersteuning zij voor zichzelf nodig achten. Door de impact van cybercrime te vergelijken met traditionele criminaliteit, die impact te verklaren, en door onderscheid te maken tussen verschillende typen impact en vormen van slachtofferschap, biedt dit proefschrift vernieuwende en maatschappelijk betekenisvolle inzichten in de slachtofferimpact van cybercrime.

Opzet en doelen

De centrale onderzoeksvraag van dit proefschrift luidt: *Wat is de slachtofferimpact van cybercrime, en wat betekent dit voor de rol van de politie?* Om deze centrale vraag te beantwoorden zijn drie deelvragen opgesteld: 1) Hoe kan de slachtofferimpact van cybercrime en traditionele criminaliteit worden gemeten?; 2) Wat is de slachtofferimpact van cybercrime, en hoe verhoudt deze zich tot de slachtofferimpact van traditionele criminaliteit?; en 3) Wat betekent de slachtofferimpact van cybercrime voor de rol van de politie? Om de onderzoeksvragen te beantwoorden, combineert dit proefschrift meerdere onderzoeksmethoden en databronnen. Allereerst was er een verkennende fase waarbij expertinterviews, een systematische literatuurreview en een theoretische verkenning zijn uitgevoerd (Hoofdstuk 2). Vervolgens zijn bestaande gegevens uit een enquête onder 2.415 cybercrimeslachtoffers van het Centraal Bureau van de Statistiek geanalyseerd (Hoofdstuk 3 en 4). Daarna is voor dit proefschrift een slachtofferenquête opgezet die werd ingevuld door 910 slachtoffers van zowel cybercrimes als traditionele delicten (Hoofdstuk 5 en 6).

Deze opzet maakt het mogelijk om de impact en behoeften van slachtoffers te meten, verklarende factoren daarvoor te identificeren, en vergelijkingen te maken met traditionele criminaliteit. Daarnaast zijn de ervaringen van cybercrime- en traditionele

criminaliteitsslachtoffers bij het doen van aangifte of melding vergeleken. Er is steeds een breed spectrum aan criminaliteitsvormen meegenomen voor een zo volledig mogelijk beeld van de impact van cybercrime. In Hoofdstuk 3 en 4 is onderscheid gemaakt naar hacken, online vermogenscriminaliteit en online persoonsgerichte criminaliteit. In Hoofdstuk 5 en 6 is voor de vergelijking met traditionele criminaliteit een indeling gehanteerd van de volgende 'delictparen': inbraak (inbraak op online bankaccount en woninginbraak), oplichting (bankhelpdeskfraude en babbeltruc), bedreiging (online en offline bedreiging), en schending van de lichamelijke integriteit (beeldgerelateerd seksueel misbruik en aanranding).

Ook voor impacttypen is een breed scala aan gevolgen meegenomen, zodat bijvoorbeeld niet alleen financiële, maar ook psychologische en sociale aspecten in beeld komen. Daarnaast zijn verschillende theoretische raamwerken toegepast, zoals de shattered assumptions theory en de cyborg theorie, om de impact van cybercrimeslachtofferschap beter te begrijpen en te verklaren. Het proefschrift is exploratief en voornamelijk kwantitatief van aard, waarmee het fundamentele inzichten biedt in de impact, behoeften en ervaringen van cybercrimeslachtoffers. Met deze inzichten is niet alleen beoogd bij te dragen aan een empirisch beter begrip van cybercrimeslachtofferschap binnen de victimologie en criminologie, maar ook richting te geven aan politiebeleid en slachtofferzorg.

Slachtofferimpact van cybercrime

De slachtofferimpact van cybercrime is groot en kent verschillende facetten. Waar eerdere studies meestal een indeling hanteren in psychologische, fysieke, financiële en sociale impact, laat dit proefschrift zien dat deze categorieën in de context van cybercrime niet geheel passend of toereikend zijn om de impact op cybercrimeslachtoffers te vatten. Daarom zijn nieuwe indelingen gemaakt binnen het psychologische domein (Hoofdstuk 3 en 4), tussen de directe impact op het emotioneel welzijn en de impact op het online veiligheidsgevoel. Die laatste verwijst naar de mate waarin cybercrimeslachtoffers zich na het delict nog veilig voelen in de online omgeving. In Hoofdstuk 5 en 6 is een bredere impactindeling toegepast, waarin internaliserende problemen (zoals angst, depressie en psychosomatische klachten), externaliserende problemen (zoals boosheid, angst voor herhaling en wraakgevoelens), financiële impact (zoals aanzienlijke schade gelet op iemands financiële positie) en een beschadigd zelfbeeld (schaamte en zelfverwijt) als impactdimensies worden onderscheiden. Ook peritraumatische stress—de acute stressreactie tijdens het delict of de ontdekking daarvan (zoals shock, ontkenning of machteloosheid)—is afzonderlijk in beschou-

wing genomen, omdat deze van andere aard is dan de andere, meer langdurige effecten.

De mate van impact blijkt samen te hangen met kenmerken van het delict, het slachtoffer en de context. Persoonsgerichte cybercrime, zoals online bedreiging of stalking, tast het emotioneel welzijn relatief sterker aan, terwijl financiële cybercrime en hacken juist het online veiligheidsgevoel aantasten, zo blijkt uit Hoofdstuk 3 en 4. Slachtoffers die de dader kenden, alleen woonden, een lagere sociaaleconomische status hadden, of geen schadevergoeding ontvingen, rapporteerden meer impact op hun emotioneel welzijn. Oudere slachtoffers ervoeren juist meer impact op hun online veiligheidsgevoel. Ook omstandigheden zoals een langere duur van het slachtofferschap of het hacken van apparaten (in plaats van accounts) vergroten de psychologische impact.

De vergelijking met traditionele criminaliteit (Hoofdstuk 5 en 6) laat zien dat cybercrimeslachtoffers evenveel of zelfs meer psychosociale schade ervaren. Zo is de aantasting van het zelfbeeld (schaamte en zelfverwijt) bij cybercrime groter dan bij traditionele delicten (behalve bij bedreiging, waar geen significante verschillen werden gevonden), en heeft financiële cybercrime meer peritraumatische stress tot gevolg dan traditionele financiële criminaliteit. De internaliserende en externaliserende problemen zijn vergelijkbaar voor cybercrime en traditionele criminaliteit, en de financiële impact was juist bij woninginbraak hoger dan bij inbraak op een online bankaccount. De mate van impact wordt beïnvloed door factoren zoals directe financiële schade, psychische problemen voorafgaand aan het delict, lager opleidingsniveau, lagere zelfeffectiviteit, de recentheid van het delict, victim blaming, en neutralisatie of ontkenning door het slachtoffer zelf.

Concluderend blijkt dat de impact van cybercrime minstens zo groot is als die van traditionele criminaliteit. De ondersteuning door politie en andere instanties sluit daar nog niet altijd op aan, zoals wordt beschreven in het vervolg van deze samenvatting.

Slachtofferbehoeften en meldingservaringen

De behoeften van slachtoffers variëren afhankelijk van het type delict, de delictkenmerken, de ervaren impact, en persoonlijke en sociale factoren, zo blijkt uit dit proefschrift. Slachtoffers van financiële cybercrime gaven aan sterkere behoeften te hebben aan praktische ondersteuning, zoals duidelijke hulproutes, financiële compensatie en preventieadvies, dan slachtoffers van financiële traditionele criminaliteit. Daarnaast rapporteerden zij sterkere emotionele en sociale behoeften, zoals erkenning van het delict en het voorkomen van slachtofferschap bij anderen, dan slachtoffers

van de traditionele tegenhangers. Daarentegen hadden slachtoffers van traditionele persoonsgerichte delicten sterkere behoeften op emotioneel vlak dan slachtoffers van persoonsgerichte cybercrime, zoals het delen van gevoelens en serieus genomen worden als slachtoffer, evenals behoefte aan opsporing en vervolging van de dader. Leeftijd, geslacht, ervaren financiële schade en peritraumatische stress blijken de belangrijkste voorspellers van slachtofferbehoeften.

Wat betreft de ervaringen bij het doen van melding of aangifte, zijn er weinig verschillen tussen de slachtoffers van cybercrime en traditionele criminaliteit. Slachtoffers van beeldgerelateerd seksueel misbruik gaven vaker aan voldoende informatie en preventieadvies te hebben ontvangen dan slachtoffers van (offline) aanranding, en zij rapporteerden minder vaak dat de politiebehandeling de impact van het delict heeft vergroot. Wel moet in acht worden genomen dat cybercrimeslachtoffers mogelijk lagere verwachtingen van de politie hebben, zichzelf meer verantwoordelijk voelen voor hun slachtofferschap, en dat slachtoffers die geen aangifte konden doen of werden weggestuurd door de politie niet in de steekproef zaten. Ook blijft de algemene tevredenheid over het aangifteproces beperkt, en gaven slachtoffers die online aangifte deden lagere scores op meerdere aspecten van het proces dan slachtoffers die persoonlijk contact hadden met de politie. Dit wijst erop dat de digitalisering van het aangifteproces momenteel onvoldoende aansluit bij de behoeften van slachtoffers.

Aanbevelingen voor beleid en praktijk

Uit de bevindingen volgen zes aanbevelingen die van belang zijn voor beleid en praktijk, in het bijzonder voor de politie en andere organisaties die in contact staan met slachtoffers van cybercrime. Dit vraagt om afstemming tussen de betrokken partijen, waarbij de politie een regie- of aanjaagrol kan vervullen.

Aanbeveling 1: Behandel slachtoffers van cybercrime als slachtoffers van "High Impact Crime"

Overweeg om cybercrime te classificeren als een vorm van "High Impact Crime" (HIC), aangezien de impact ervan vaak vergelijkbaar is met of zelfs groter is dan die van traditionele HIC-feiten, zoals woninginbraak. Prioriteer op die manier de bestrijding van cybercrime en maak meer middelen vrij voor slachtofferpreventie en -ondersteuning.

Aanbeveling 2: Stem slachtofferondersteuning af op het type cybercrime en de kenmerken ervan

De impact van cybercrime varieert per delict en wordt mede bepaald door situationele factoren en modus operandi. Slachtofferondersteuning dient daarom afgestemd te worden op de aard van het delict, met expliciete aandacht voor zowel het emotioneel welzijn als het online veiligheidsgevoel. Maatwerk, snelle opvolging en passende schadevergoeding is daarbij cruciaal.

Aanbeveling 3: Geef prioriteit aan preventie en ondersteuning voor cybercrimeslachtoffers die extra kwetsbaar lijken voor het ervaren van hoge impact

Sommige groepen blijken extra kwetsbaar voor het ervaren van ernstige gevolgen van bepaalde cybercrimes, waaronder mensen met een lagere sociaaleconomische status, ouderen, alleenwonenden, herhaald slachtoffers, en mensen met bestaande psychische problemen. Bij preventie en ondersteuning kan daarom specifieke aandacht worden gegeven aan deze doelgroepen. Denk hierbij aan gerichte bewustwordingscampagnes en slachtoffernotificatie (secundaire preventie), en intensievere ondersteuning na slachtofferschap voor herstel en om herhaald slachtofferschap te voorkomen (tertiaire preventie).

Aanbeveling 4: Besteed aandacht aan de praktische en emotionele behoeften van slachtoffers van financiële cybercrime

Slachtoffers van financiële cybercrime hebben sterkere praktische en emotionele behoeften dan slachtoffers van financiële traditionele criminaliteit. Deze slachtoffers zijn veelal niet alleen financieel benadeeld, maar ook misleid en aangetast in hun zelfbeeld. De respons van politie en ketenpartners moet daarom niet enkel gericht zijn op juridische afhandeling of schadevergoeding, maar ook op psychosociale en praktische ondersteuning.

Aanbeveling 5: Prioriteer zelfbeeldherstel van cybercrimeslachtoffers en voorkom secundaire victimisatie

Cybercrime tast vaak het zelfbeeld van slachtoffers aan; bij hen is er meer schaamte en zelfverwijt dan bij slachtoffers van traditionele criminaliteit. Professionals kunnen bijdragen aan zelfbeeldherstel door erkenning te geven aan wat slachtoffers is overkomen, en door victim blaming en stigma tegen te gaan (bijvoorbeeld via bewust taalgebruik en publiekscampagnes). Contact met slachtoffers moet zorgvuldig en empathisch verlopen om secundaire victimisatie te voorkomen.

Aanbeveling 6: Evalueer en verbeter aangifteprocessen om beter tegemoet te komen aan de impact en behoeften van cybercrimeslachtoffers

Bij contact met cybercrimeslachtoffers is menselijkheid en maatwerk van belang. Het verdient aanbeveling om het proces van internetaangifte te evalueren en waar mogelijk aan te passen, bijvoorbeeld door slachtoffers in staat te stellen om op andere wijze de aangifte te voltooien. Ook kunnen pilots worden uitgevoerd ter verbetering van het aangifteproces bij cybercrime, zodat beter tegemoet kan worden gekomen aan de impact en behoeften van slachtoffers.

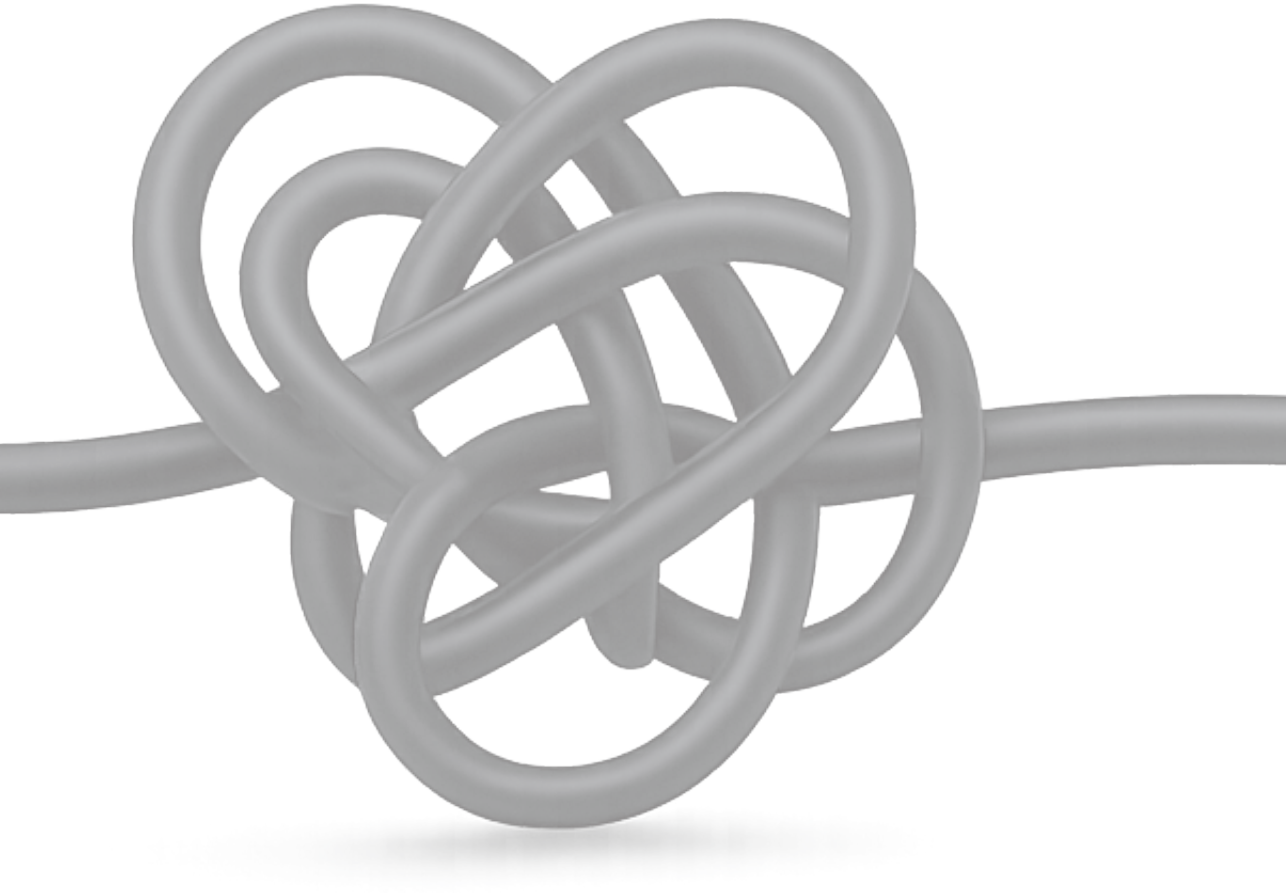
Beperkingen en vervolgonderzoek

Hoewel dit proefschrift belangrijke en vernieuwende inzichten oplevert over de impact van cybercrime en de betekenis daarvan voor de rol van de politie, kent het enkele beperkingen. Het onderzoek is grotendeels kwantitatief van aard, waardoor de onderliggende mechanismen achter slachtofferimpact en -behoeften niet volledig zijn blootgelegd. Daarnaast zijn relatief veelvoorkomende en minder technisch complexe vormen van cybercrime onderzocht, terwijl minder voorkomende fenomenen—zoals slachtofferschap in de metaverse—of technischer delicten—zoals malware—buiten beschouwing zijn gebleven. Daarnaast zijn de studies in Hoofdstuk 5 en 6 beperkt tot slachtoffers die zich bij de politie hebben gemeld. Slachtoffers die om uiteenlopende redenen geen aangifte hebben gedaan, bleven daarmee buiten beeld. Ook is er, mede door de focus op vergelijkingen met traditionele criminaliteit, weinig aandacht besteed aan cybercrime-specifieke impact en behoeften. Een andere beperking is het ontbreken van longitudinale gegevens, waardoor de ontwikkeling van impact over de tijd slechts beperkt in kaart is gebracht. Toekomstig onderzoek zou zich daarom kunnen richten op kwalitatieve verdieping van cybercrimeslachtofferervaringen, op slachtoffers die geen melding of aangifte hebben gedaan, en op cybercrime-specifieke behoeften zoals hulp bij het herstellen van digitale schade. Daarbij is het belangrijk dat vervolgonderzoek gelijke tred houdt met de technologische ontwikkelingen, aangezien de aard van cybercrime en de modus operandi van de daders voortdurend veranderen.

Slotbeschouwing

Cybercrime is geen 'licht' delict. De psychologische, financiële en sociale schade voor slachtoffers is groot en doet niet onder voor die van traditionele criminaliteit. Voor de politie en andere betrokken instanties is het van belang een goed begrip te hebben

van wat slachtoffers daadwerkelijk doormaken om hen effectief te kunnen ondersteunen. Dit proefschrift levert daaraan een bijdrage door een uitgebreide analyse van de impact van cybercrime, een vergelijking met traditionele delicten, en de vertaling van bevindingen naar concrete aanbevelingen voor politie en ketenpartners. Het biedt daarmee belangrijke inzichten voor meer slachtoffergericht beleid en politiewerk op het gebied van cybercrime. In een tijd waarin technologie verder doordringt tot ons dagelijks leven, moet ook de aandacht voor cybercrimeslachtoffers meebewegen: mensgericht, responsief en afgestemd op de dynamiek van het digitale tijdperk.



Summary

Unravelling the impact of cybercrime: Understanding victim experiences and implications for police practice

Introduction

This dissertation concerns the impact of cybercrime on its victims. One of the downsides of digitization is the rise of cybercrime. This dissertation reveals that cybercrimes have profound consequences for victims that are at least as severe as the consequences of traditional crime. Yet the police, other public and private organizations and citizens often seem to underestimate this impact. This dissertation shows, from a victim-centered approach, how victims experience the impact of cybercrime, what needs arise from it, and what this means for the role of the police and their partner organizations. The experiences and perceptions of victims are central: how they experience the severity and consequences of the crime, what emotions and practical problems arise from it, and what support they consider necessary for themselves. By comparing the impact of cybercrime with traditional crime, explaining that impact, and distinguishing between different types of impact and forms of victimization, this dissertation offers innovative and socially meaningful insights into the victim impact of cybercrime.

Design and goals

The central research question of this dissertation is: *What is the victim impact of cybercrime, and what does this mean for the role of the police?* To answer this central question, three sub-questions were developed: 1) How can the victim impact of cybercrime and traditional crime be measured?; 2) What is the victim impact of cybercrime, and how does it compare to the victim impact of traditional crime?; and 3) What implications does the victim impact of cybercrime have for the role of the police? To answer the research questions, this dissertation combines multiple research methods and data sources. First, there was an exploratory phase in which expert interviews, a systematic literature review, and a theoretical exploration were conducted (Chapter 2). Subsequently, existing data from a survey of 2,415 cybercrime victims by Statistics Netherlands were analyzed (Chapters 3 and 4). A victim survey was then developed for this dissertation, which was completed by 910 victims of both cybercrimes and traditional crimes (Chapters 5 and 6).

This design allows for the measurement of victims' impact and needs, identification of explanatory factors, and comparisons with traditional crime. In addition, the experiences of cybercrime and traditional crime victims when filing a police report were compared. Throughout, a broad spectrum of crime types was included to offer a comprehensive understanding of the impact of cybercrime. Chapters 3 and

4 distinguish between hacking, online property crime, and online person-centered crime. In Chapters 5 and 6, for the comparison with traditional crime, the following 'crime pairs' were discerned: burglary (hacking of online bank account and residential burglary), scams (bank helpdesk fraud and doorstep deception), threat (online and offline threat), and violation of physical integrity (image-based sexual abuse and sexual assault).

Also for impact types, a wide range of consequences was included, ensuring that, for example, not only financial but also psychological and social aspects are captured. In addition, various theoretical frameworks were applied, such as the shattered assumptions theory and the cyborg theory, to better understand and explain the impact of cybercrime victimization. The dissertation is exploratory and primarily quantitative in nature, thereby offering fundamental insights into the impact, needs and experiences of cybercrime victims. These insights are intended not only to contribute to an empirically better understanding of cybercrime victimization within victimology and criminology, but also to inform police policy and victim care.

Victim impact of cybercrime

The victim impact of cybercrime is substantial and multi-faceted. Whereas previous studies generally apply a classification into psychological, physical, financial, and social impact, this dissertation shows that these categories are not entirely suitable or sufficient in the context of cybercrime to capture the impact on cybercrime victims. Therefore, new classifications were developed within the psychological domain (Chapters 3 and 4), distinguishing between the direct impact on emotional well-being and the impact on online sense of security. The latter refers to the extent to which cybercrime victims still feel safe in the online environment after the crime. In Chapters 5 and 6, a broader impact classification was applied, in which internalizing problems (e.g., anxiety, depression and psychosomatic complaints), externalizing problems (e.g., anger, fear of recurrence and feelings of revenge), financial impact (e.g., significant damage given one's financial position) and damaged self-image (shame and self-blame) are distinguished as impact dimensions. Peritraumatic stress—the acute stress response during the offense or its discovery (such as shock, denial, or helplessness)—was also included separately, as it is of a different nature than the other, more enduring effects.

The degree of impact is related to characteristics of the offense, the victim and the context. Person-centered cybercrime, such as online threat or stalking, has a relatively stronger effect on emotional well-being, while financial cybercrime and

hacking more strongly affect online sense of security, as shown in Chapters 3 and 4. Victims who knew the offender, lived alone, had lower socioeconomic status, or did not receive financial compensation reported greater impact on their emotional well-being. In contrast, older victims experienced more impact on their sense of online safety. Conditions such as longer duration of victimization or hacking of devices (rather than accounts) were also related to greater psychological impact.

The comparison with traditional crime (Chapters 5 and 6) shows that cybercrime victims experience as much or even more psychosocial harm. For example, damage to self-image (shame and self-blame) is greater for cybercrime than for traditional crimes (except in the case of threat, where no significant differences were observed), and financial cybercrime leads to more peritraumatic stress than financial traditional crime. Internalizing and externalizing problems are comparable for cybercrime and traditional crime, and the financial impact was found to be greater for residential burglary than for hacking of an online bank account. The degree of impact is influenced by factors such as direct financial loss, psychological problems prior to the offense, lower education level, lower self-efficacy, the recency of the offense, victim blaming, and neutralization or denial by the victim.

In conclusion, the impact of cybercrime appears to be at least as great as that of traditional crime. Support provided by the police and other agencies does not yet always match this, as described in the remainder of this summary.

Victim needs and reporting experiences

Victims' needs vary depending on crime type, crime characteristics, experienced impact, and personal and social factors, as this dissertation shows. Victims of financial cybercrime reported stronger needs for practical support—such as clear support routes, financial compensation, and prevention advice—than victims of traditional financial crime. They also reported stronger emotional and social needs, such as acknowledgment of the offense and the prevention of victimization in others, than victims of traditional counterparts. In contrast, victims of traditional person-centered crime had stronger emotional needs than victims of person-centered cybercrime, such as sharing feelings, being taken seriously as a victim, and a greater need for investigation and prosecution of the offender. Age, gender, experienced financial loss and peritraumatic stress emerged as the main predictors of victim needs.

In terms of the experiences of reporting to the police, there are few differences between victims of cybercrime and traditional crime. Victims of image-based sexual abuse more often indicated that they had received sufficient information and preven-

tion advice than victims of (offline) sexual assault, and they reported less frequently that the police response had increased the impact of the offense. However, it should be noted that cybercrime victims may have lower expectations of the police, feel more responsible for their victimization, and that victims who were unable to file a report or were turned away by the police were not in the sample. Overall satisfaction with the reporting process also remains limited, and victims who reported online rated multiple aspects of the process lower than those who had personal contact with the police. This suggests that the digitization of the reporting process currently fails to adequately meet the needs of victims.

Recommendations for policy and practice

Six recommendations follow from the findings that are important for policy and practice, particularly for the police and other organizations that engage with cybercrime victims. This calls for coordination between the parties involved, with the police taking a coordinating or driving role.

Recommendation 1: Treat cybercrime victims as victims of "High-Impact Crime"
Consider classifying cybercrime as a form of "High-Impact Crime" (HIC), as its impact is often comparable to or even greater than that of traditional HIC offenses, such as residential burglary. In doing so, prioritize the fight against cybercrime and allocate more resources to victim prevention and support.

Recommendation 2: Tailor cybercrime victim support to the type of cybercrime and its characteristics
The impact of cybercrime varies by crime type and is partly determined by situational factors and modus operandi. Victim support should therefore be adapted to the nature of the offense, with explicit attention to both emotional well-being and the sense of online safety. Tailored support, timely follow-up, and appropriate compensation are crucial in this regard.

Recommendation 3: Prioritize prevention and support for cybercrime victims most vulnerable to severe impact
Certain groups appear especially vulnerable to experiencing severe consequences from specific types of cybercrime, including individuals with lower socioeconomic status, older adults, people living alone, repeat victims, and those with pre-existing psycho-

logical issues. Prevention and support efforts should therefore pay specific attention to these target groups. This may include targeted awareness campaigns and victim notification (secondary prevention), as well as more intensive post-victimization support aimed at recovery and preventing repeat victimization (tertiary prevention).

Recommendation 4: Address the practical and emotional needs of financial cybercrime victims

Victims of financial cybercrime have stronger practical and emotional needs than victims of financial traditional crime. These victims are often not only financially harmed, but also deceived and affected in their self-image. The response of the police and their partner organizations should therefore not be limited to legal processing or compensation, but should also include psychosocial and practical support.

Recommendation 5: Prioritize self-image restoration for cybercrime victims and prevent secondary victimization

Cybercrime often affects victims' self-image; they experience more shame and self-blame than victims of traditional crime. Professionals can contribute to self-image recovery by acknowledging what victims have experienced and by countering victim blaming and stigma (for example, through mindful language use and public awareness campaigns). Contact with victims should be handled with care and empathy to prevent secondary victimization.

Recommendation 6: Evaluate and adapt reporting processes to meet cybercrime victims' impact and needs

When interacting with cybercrime victims, a human-centered approach and tailored support are essential. It is recommended to evaluate the online reporting process and adapt it where possible—for instance, by enabling victims to complete their report through alternative means. Pilot projects can also be conducted to improve the cybercrime reporting process to better meet the impact and needs of victims.

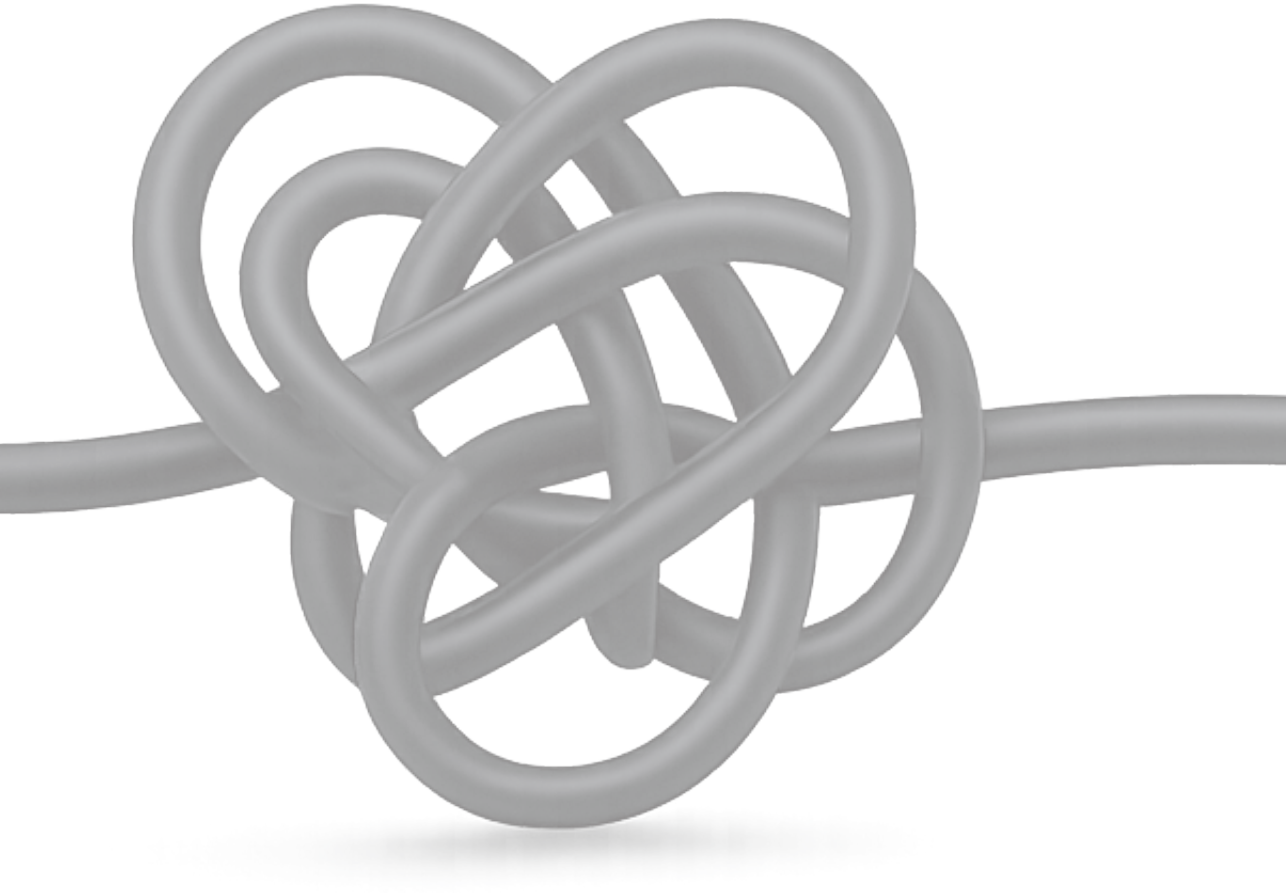
Limitations and follow-up research

While this dissertation yields important and innovative insights into the impact of cybercrime and its implications for the role of the police, it also has several limitations. The study is largely quantitative in nature, which means that the underlying mechanisms behind victim impact and needs have not been fully uncovered. In addition,

relatively common and less technically complex forms of cybercrime have been examined, while less common phenomena—such as victimization in the metaverse—or more technical offenses—such as malware—have been mostly excluded from the scope of this dissertation. In addition, the studies in Chapters 5 and 6 are limited to victims who reported to the police. Victims who, for various reasons, did not report the crime thus were not included. Furthermore, due to the focus on comparisons with traditional crime, relatively little attention has been paid to cybercrime-specific forms of impact and needs. Another limitation is the absence of longitudinal data, which limited the ability to capture the development of impact over time. Future research could therefore focus on qualitative deepening of cybercrime victim experiences, on victims who did not report to the police, and on cybercrime-specific needs such as assistance with digital recovery measures. In doing so, it is important that follow-up studies keep pace with technological developments, as the nature of cybercrime and the modus operandi of offenders are constantly evolving.

Final considerations

Cybercrime is not a 'minor' offense. The psychological, financial, and social harm to victims is substantial and no less serious than that caused by traditional crime. For the police and other relevant institutions, it is essential to have a thorough understanding of what victims actually go through in order to support them effectively. This dissertation contributes to this through a comprehensive analysis of the impact of cybercrime, a comparison with traditional offenses, and the translation of findings into concrete recommendations for the police and their partner organizations. In doing so, it provides important insights for more victim-oriented policy and police practice in the field of cybercrime. In a time when technology is increasingly permeating our daily lives, attention to cybercrime victims must evolve accordingly: human-centered, responsive, and attuned to the dynamics of the digital age.



Dankwoord
(acknowledgments in Dutch)

In december 2018 leek vier jaar eindeloos lang en ruim voldoende om een proefschrift af te ronden. Inmiddels zijn we meer dan zes jaar verder, en kijk ik terug op een intensief en leerzaam proces dat voorbij vloog. Het combineren van onderzoek en politiewerk was soms ingewikkeld, omdat ik me nu eenmaal niet volledig op beide kon toeleggen. Tegelijkertijd was het een uitkomst om te werken binnen de organisatie waar mijn onderzoeksonderwerp zich afspeelt. De relevantie werd herkend door collega's uit het veld van online criminaliteit, maar ook daarbuiten. Toch is het allerminst vanzelfsprekend dat zo'n onderzoek niet in een la belandt. Ik ben iedereen dankbaar die het belang ervan zag, het steunde en actief hielp uitdragen.

Eigenlijk begon het bij René Bakker, die me tegen het einde van mijn politieopleiding overtuigde om géén vrijstelling voor de scriptie aan te vragen. Ik vond onderzoek doen immers leuk, en wie weet tot welke onderwerpen, contacten en ontwikkelingen het zou leiden. Dat werden slachtofferschap van online criminaliteit, Wouter Stol en Jurjen Jansen als extra begeleiders, twee publicaties en uiteindelijk het idee voor mijn promotietraject. Mijn politiewerk wilde ik niet opgeven, maar dankzij een creatieve constructie—met dank aan het Programma Digitalisering en Cybercrime, de Eenheid Noord-Nederland, de Open Universiteit en NHL Stenden Hogeschool—kon ik van start. Wouter en Jurjen: veel dank voor jullie vertrouwen, betrokkenheid en prettige begeleiding. Jullie waren er als het nodig was, maar lieten mij het traject vormgeven in mijn eigen tempo en stijl. Wouter, jouw lange onderzoeks- en politie-ervaring en creative ideeën hielpen me om het onderzoek richting te geven en in breder perspectief te plaatsen. Jurjen, jouw nuchtere en kritische blik, je ervaring in het onderzoeksveld en als iets recenter gepromoveerde waren van grote waarde voor mijn promotietraject.

Mijn dank gaat ook uit naar de klankbordgroep vanuit de politie, in de eerste plaats opdrachtgever Theo van der Plas. Dank voor je betrokkenheid en je vertrouwen in de manier waarop we het onderwerp hebben benaderd. Ook dank aan Nienke Groenhagen, Richard Nijeboer, en Oscar Dros (later Janny Knol en Maarten de Laat) voor jullie scherpe blik op de relevantie voor de politiepraktijk, en jullie inzet om de inzichten van het onderzoek naar de praktijk te vertalen.

Speciale dank ook aan alle respondenten die op verzoek van 'de politie' mijn vragenlijst invulden en waardevolle, vaak heel persoonlijke informatie deelden.

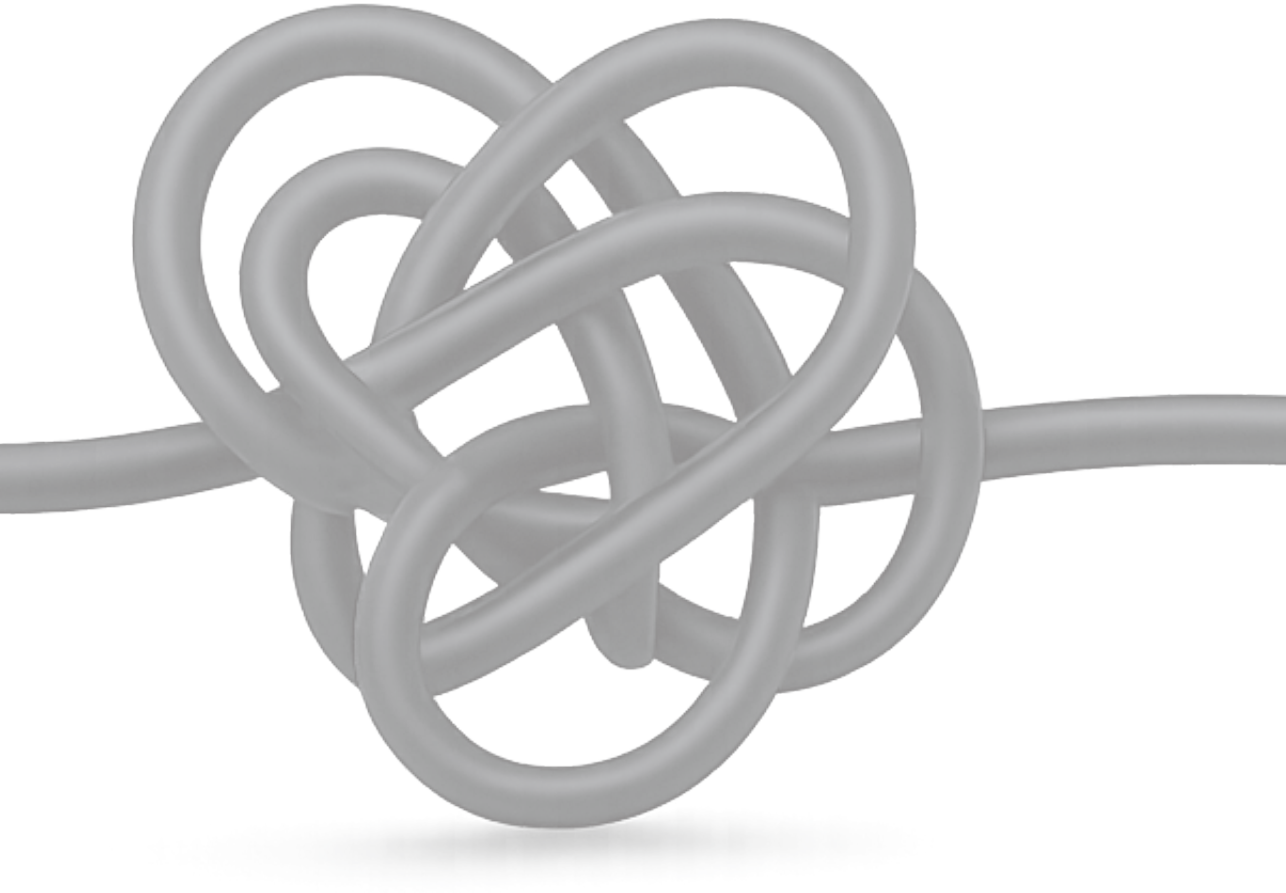
Verder bedank ik de collega's van NHL Stenden Hogeschool (onderzoeksgroep Cybersafety) voor het bieden van een werkplek en een fijne start van dit traject, en voor jullie blijvende interesse en betrokkenheid. Ook dank aan het promovendinetwerk van de OU, de politiepromovendi en niet in de laatste plaats het intervisieclubje: jullie hebben mij geïnspireerd, gespiegeld en verder geholpen. Het Team Cybercrime

Noord-Nederland, met Radmer voorop, dank ik voor het begrip voor mijn beperkte beschikbaarheid en het blijven zien van de meerwaarde van mijn onderzoek, ook als ik vaak afwezig was en nog steeds veel buiten het 'boeven vangen' om bezig ben. Veel dank ook aan Rutger en de anderen van het lectoraat Cybercrime & Cybersecurity van de Haagse Hogeschool voor de kans om me als nog niet gepromoveerde 'postdoc' in online daderschap te verdiepen, zonder de slachtoffers compleet te hoeven loslaten. Ook COPS/THTC, Wouter en de anderen: dank dat ik zo in het team werd opgenomen, en voor de waardering voor mijn onderzoekswerk.

Ook dank aan alle collega's binnen en buiten de politie die het onderzoek verder hielpen; sommigen in het bijzonder. Esther Schut-Lip voor de hulp bij de toestemmingsaanvragen en verspreiding van resultaten, en de studenten van de Politieacademie voor hun hulp bij het benaderen van respondenten. Peter Hagenaars, Ruben van Well en Aad Lensen waren van grote betekenis voor de zichtbaarheid van het onderzoek. Net als Sander Hoed en Remko Leeneman, met wie het wederzijds promoten rondom 'Digitaal ter plaatse' goed samenviel. Het VAK hielp om de bevindingen toegankelijker te presenteren. Dank ook aan de collega's van de Portefeuille Dienstverlening, en aan de Integrale Aanpak Online Fraude voor het breder onder de aandacht brengen en benutten van mijn onderzoeksresultaten in de praktijk. En aan iedereen die mijn onderzoek verder een podium gaf via presentaties, congressen, podcasts, media of vakbladen: veel dank.

Jerien en Ian, bedankt voor jullie betrokkenheid en eindeloze interesse, en dat jullie tussendoor ook nog testpersoon wilden zijn. Dank ook aan mijn vrienden en vriendinnen die ik tijdens de nodige afleiding en ontspanning niet te veel heb willen vermoeien met de inhoud, maar ik heb altijd jullie steun, trots en waardering gevoeld. Jindra, dank ook voor je hulp bij het testen. Danique en Yvonne, fijn hoe jullie dit traject begrepen vanuit de organisatie en onze gedeelde ervaringen. Bedankt dat jullie me ook tijdens de verdediging bijstaan. En natuurlijk Halewijn—dankjewel voor je steun, je positieve kijk op mijn onderzoek, dat je me af en toe uit de werkmodus haalde, en voor het meedenken over alles van Lasso's tot internaliserende en externaliserende kwesties.

Voor iedereen die me onderweg heeft gesteund of geholpen, ook zonder hier genoemd te zijn: bedankt voor het mogelijk maken van dit proefschrift.



Curriculum vitae

Jildau Borwell (1988) obtained a Master's degree in Sociology from the University of Groningen in 2011, specializing in Crime and Safety. She subsequently completed a Bachelor's degree in police studies at the Dutch Police Academy, graduating in 2017 with a thesis on the personality traits of online fraud victims. Following her police education, Jildau worked as an analyst in the Analysis & Research team of the Intelligence Division (DRIO) within the North Netherlands Police Unit, further specializing in cybercrime. Since 2019, she has served as a senior cybercrime analyst in the unit's Team Cybercrime, contributing to the police's cyber intelligence capabilities.

From December 2018 until the completion of her PhD, Jildau was affiliated as an external PhD candidate with the Open University of the Netherlands, NHL Stenden University of Applied Sciences, and the Dutch Police Academy. Her PhD research—on the impact of cybercrime on victims and its implications for the role of the police—culminated in this dissertation and has yielded both academic and practical contributions.

Since January 2024, Jildau has been working as a postdoctoral researcher in the Cybercrime & Cybersecurity research group at The Hague University of Applied Sciences. In this role, she conducts research on offender pathways into and out of cybercrime and acts as a liaison for national and international law enforcement partners, primarily for the Cyber Offender Prevention Squad of the Netherlands Police's High Tech Crime Unit.

Jildau aims to continue combining police practice with academic research in the field of cybercrime.

Open Universiteit

NHL STENDEN hogeschool

POLITIE