ARTIKELEN

De slachtofferimpact van cybercrime versus traditionele criminaliteit: aanknopingspunten voor slachtofferzorg en preventieprioriteiten

Kimberly Bluhm, Jildau Borwell & Wouter Stol

In deze studie onderzoeken wij in hoeverre de gevolgen van slachtofferschap van cybercrime verschillen van die van traditionele criminaliteit, door deze twee typen criminaliteit expliciet tegen elkaar af te zetten. Door middel van enquêtes in twee gemeenten zijn de impact en behoeften van slachtoffers van beide typen criminaliteit in kaart gebracht. De resultaten suggereren dat er geen verschil is in impact tussen cybercrime en traditionele criminaliteit. De impact varieert hierbij per delict. Daarnaast verschillen bepaalde behoeften van cybercrimeslachtoffers van de behoeften van slachtoffers van traditionele criminaliteit. Lokale beleidsmakers kunnen hierop inspelen door cybercrime te prioriteren in hun nazorg- en preventiebeleid, en daarbij tegemoet te komen aan specifieke behoeften van cybercrimeslachtoffers.

1 Inleiding

Digitalisering biedt criminelen mogelijkheden om nieuwe delicten te plegen alsook mogelijkheden om oude delicten op een nieuwe manier te plegen (Jansen & Leukfeldt, 2018). Bijeengenomen gaat het om criminaliteit waarbij informatie- en communicatietechnologie (ICT) een wezenlijke rol speelt in de uitvoering van het delict (Domenie et al., 2013), hierna kortweg cybercrime.

Het slachtofferpercentage van traditionele criminaliteit neemt af, terwijl dat van cybercrime toeneemt en in slachtofferonderzoek zijn ze inmiddels op gelijke hoogte geraakt. In 2021 was 17% van de inwoners van Nederland slachtoffer van traditionele criminaliteit. Dit percentage lag voor cybercrime ook op 17% (CBS, 2022a). Cybercrime is zo gezien 'veel voorkomende criminaliteit' (VVC) en te verwachten is dat het binnen afzienbare tijd de traditionele criminaliteit in slachtofferpercentages voorbij streeft.

De politie lijkt echter bij de lokale politieteams, waar zij VVC behandelt, cybercrime niet hoog te prioriteren (Kleijer, 2020; Borwell et al., 2021a; Van Loenhout, n.g.). Ook bij gemeenten zien we niet veel meer dan een beginnende belangstelling voor cybercrime in lokaal veiligheidsbeleid (Stol & Bantema, 2020). Gezien de veiligheidsdriehoek hebben beide partijen een rol in de lokale aanpak van cybercrime.

Voor een adequate prioritering van cybercrime ten opzichte van traditionele criminaliteit, hebben politie en gemeenten naast kennis over prevalentie, ook kennis nodig over de gevolgen van cybercrime voor de slachtoffers. De vraag is dan of cybercrime andere gevolgen heeft voor slachtoffers dan traditionele criminaliteit. Ook is de vraag of de gevolgen per type cybercrime verschillen, zodat in cybercrimebeleid rekening kan worden gehouden met het type delict. In dit onderzoek zijn daarom, met behulp van data (surveyonderzoek) uit de gemeenten Groningen en Leeuwarden, slachtoffers van acht vormen van cybercrime en tien vormen van traditionele criminaliteit bevraagd over de gevolgen die het delict voor hen had. We kijken daarbij zowel naar de impact van het delict op slachtoffers als naar de behoeften van slachtoffers. De acht cybercrimes en tien traditionele criminaliteitsvormen worden in dit onderzoek overkoepelend 'cybercrimes' en 'traditionele criminaliteit' genoemd.

Cybercrime heeft unieke kenmerken die mogelijk invloed hebben op de gevolgen ervan, zoals de ongrijpbaarheid, schaalbaarheid en permanentie van veel cybercrimes (Borwell et al., 2021a). Aspecten als toenemende afhankelijkheid van het internet, de gevoelsmatige verbondenheid van mensen met hun apparaten en 'victim blaming' van speciaal cybercrimeslachtoffers kunnen ook een rol spelen bij de gevolgen van het delict. CBS-slachtofferonderzoek bevat aanwijzingen dat cybercrime en traditionele criminaliteit inderdaad verschillen qua impact. Slachtoffers van persoonsgerichte cybercrimes, zoals online stalking, online bedreiging en shamesexting, rapporteren vaker emotionele of psychische problemen dan slachtoffers van traditionele geweldsdelicten (CBS,2022a). Verder rapporteren slachtoffers van phishing en online verkoopfraude vaker financiële problemen dan slachtoffers van offline vermogensdelicten (CBS, 2022a).

Sommige studies suggereren dat slachtofferimpact na cybercrime gelijkwaardig aan of groter kan zijn dan de impact van traditionele criminaliteit (Holt & Bossler, 2008; CBS, 2022a). De gevolgen van cybercrime en traditionele criminaliteit voor slachtoffers werden in eerder onderzoek echter niet in een brede invulling van die twee, tegen elkaar afgezet. Er zijn studies die enkele soorten cybercrimes of enkele soorten impact na slachtofferschap van cybercrime vergelijken (bijv. Kerr et al., 2013), maar in deze studies zijn cybercrime en traditionele criminaliteit slechts beperkt ingevuld (weinig delictsvormen) en niet expliciet tegen elkaar afgezet, waardoor een brede vergelijking tussen cybercrime en traditionele criminaliteit ontbreekt (Borwell et al., 2021a).

Onderzoeken naar behoeften zijn voornamelijk gericht op slachtofferschap na traditionele criminaliteit (Kunst & Koster, 2015), of maken geen expliciete vergelijking tussen cybercrime en traditionele criminaliteit (Leukfeldt et al., 2018). De nazorg voor slachtoffers is momenteel voornamelijk gebaseerd op kennis over de impact en behoeften na slachtofferschap van traditionele criminaliteit. Die kunnen echter verschillen van de impact en behoeften na slachtofferschap van cybercrime. Het is daarom, nu de criminaliteit verschuift van offline naar online, voor slachtofferbeleid van belang om de twee soorten criminaliteit in bredere zin tegen elkaar af

te zetten en beter zicht te krijgen op of en zo ja hoe de impact en behoeften na cybercrime verschillen van de impact en behoeften na traditionele criminaliteit.

Kortom, of en hoe de digitalisering de slachtofferimpact van criminaliteit, waaronder behoeften van slachtoffers heeft beïnvloed, is nog onvoldoende duidelijk voor het ontwikkelen van lokaal slachtofferbeleid. Met het hier gepresenteerde onderzoek beogen we een bijdrage te leveren aan het invullen van deze kennisleemte door de twee soorten criminaliteit expliciet en met verschillende delictvormen tegen elkaar af te zetten.

2 Vraagstelling en literatuurverkenning

De hoofdvraag in dit onderzoek luidt: *In hoeverre heeft cybercrime andere gevolgen voor slachtoffers dan traditionele criminaliteit?*

Om deze hoofdvraag te kunnen beantwoorden, zijn de volgende onderzoeksvragen geformuleerd, waarbij 'gevolgen' is onderverdeeld in impact en behoeften:

1 In hoeverre verschilt de slachtofferimpact van cybercrime van die van traditionele criminaliteit?
2 In hoeverre ervaren slachtoffers van verschillende cybercrimes verschillende impact?
3 In hoeverre hebben cybercrimeslachtoffers na het delict andere behoeften dan slachtoffers van traditionele criminaliteit?

In de literatuur worden verschillende impactvormen onderscheiden: 1) emotioneel/psychisch, 2) lichamelijk/fysiek, 3) sociaal/gedragsmatig en 4) financieel/materieel (Borwell et al., 2021b). Wij hanteren ook deze operationalisering.

We geven hierna een overzicht van het (schaarse) eerdere onderzoek waarin slachtoffergevolgen van cybercrime worden vergeleken met die van traditionele criminaliteit. We zochten op studies naar de impact of behoeften van cybercrime en studies die een vergelijking maken tussen cybercrime en traditionele criminaliteit.

2.1 Slachtofferimpact

Heinz et al. (2013) geven een overzicht van de emotionele impact van online oplichting met bankgegevens en een aantal traditionele delicten. Het onderzoek suggereert dat, afhankelijk van het type delict, de emotionele cybercrime-impact hoger dan wel lager is dan die van traditionele criminaliteit (Borwell et al., 2021a). Een studie van Kerr et al. (2013) focust op de impact van on- en offline fraude. Aan participanten (slachtoffers van online fraude en experts) is gevraagd in hoeverre zij online fraude op een andere manier zien dan offline fraude. Sommigen gaven aan dat de omvang van het delict zwaarder weegt dan het feit of het on- of offline plaatsvindt en dat de consequenties gelijk kunnen zijn. Anderen geven aan dat de impact van online fraude lager is dan van offline fraude, omdat het minder persoonlijk van aard is (Kerr et al., 2013).

Cross et al. (2016) onderzochten de financiële impact van online fraude. Zij vonden dat de ervaren financiële impact onder andere afhankelijk is van het schadebedrag en de financiële omstandigheden van het slachtoffer. Modic en Anderson (2015) richten zich in hun onderzoek op de financiële en emotionele impact van online fraude. Dit onderzoek suggereert dat mensen die slachtoffer zijn geworden van diverse typen online fraude financiële en emotionele impact ervaren.

De genoemde onderzoeken suggereren dat slachtoffers van cybercrime, afhankelijk van het type delict, verschillende typen impact kunnen ervaren en dat die kunnen verschillen van de impact van vergelijkbare traditionele delicten.

2.2 Slachtofferbehoeften

De studie van Ten Boom en Kuijpers (2008) biedt inzicht in de behoeften van slachtoffers na slachtofferschap van traditionele criminaliteit. Hierbij maken zij onderscheid in de volgende behoeftecategorieën: emotioneel, strafproces in ruime zin, informatie, praktisch, financieel en primair. Deze behoeften vormen tevens de basis voor het onderzoek van Leukfeldt et al. (2018), dat zich focust op de behoeften na slachtofferschap van cybercrime. Uit interviews volgt dat behoeften van cybercrimeslachtoffers voor een groot deel overeenkomen met die van slachtoffers van traditionele delicten. In het onderzoek komen drie behoeften voornamelijk naar voren bij cybercrimeslachtofferschap: 1) stoppen van het slachtofferschap, 2) straf en vergelding, en 3) anderen helpen om slachtofferschap te voorkomen. Ook hadden slachtoffers behoeften betreffende het verloop van het strafproces (Leukfeldt et al., 2018).

Bovengenoemde studies zijn gebaseerd op behoeften na slachtofferschap van zowel cybercrime als traditionele criminaliteit, al zijn deze behoeften niet tegen elkaar afgezet. Daarnaast is het mogelijk dat cybercrimeslachtoffers andere of aanvullende behoeften hebben dan de behoeften die in eerdere studies zijn bevraagd.

3 Methoden

In dit onderzoek gebruiken we data uit de Veiligheidsmonitor 2020 van de gemeente Groningen en uit de Leefomgeving-enquête 2019 van de gemeente Leeuwarden. In Groningen is gevraagd naar de impact van cybercrime en naar die van traditionele criminaliteit, én is gevraagd naar de behoeften van de slachtoffers van beide typen criminaliteit. In Leeuwarden is gevraagd naar de impact van cybercrime. Een weergave van slachtoffergevolgen van cybercrime baseren we op de data uit Groningen en Leeuwarden; een weergave van slachtoffergevolgen van traditionele criminaliteit baseren we op de data uit Groningen. Voor een hogere betrouwbaarheid van het onderzoek en vanwege de sterke punten in beide datasets, zijn beide datasets geanalyseerd en waar mogelijk samengevoegd.

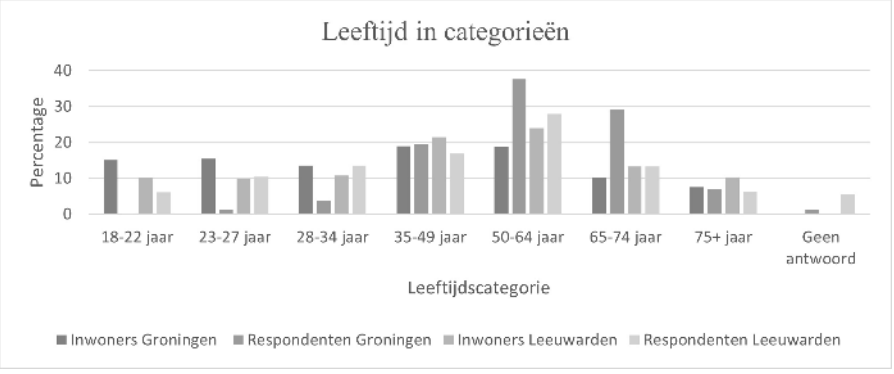
3.1 Participanten

Het totaal aantal participanten is 3462. Daarvan komen er 1682 uit de gemeente Groningen, waarvan 958 mannen (57,0%), 713 vrouwen (42,4%), 1 overig (0,1%),

doi: 10.5553/TvV/.000045

en 6 (0,4%) die geen sekse hebben opgegeven. Z-scores laten zien dat de groepen van 50-64 en 65-74 jaar oververtegenwoordigd zijn in deze gemeente en dat de groepen van 18-22, 23-27 en 28-34 jaar significant ondervertegenwoordigd zijn (p <0,01) (zie figuur 1).
Er zijn 1780 participanten uit de gemeente Leeuwarden, waarvan 850 mannen (47,8%), 860 vrouwen (48,3%), 1 anders (0,1%) en 69 (3,9%) die geen sekse hebben opgegeven.

***Figuur 1 Leeftijd in categorieën in Groningen en Leeuwarden**[*]*



* Aangepast overgenomen uit 'Inwoners naar leeftijd' door Leeuwarden in cijfers (2022) en 'Bevolking 2022' door gemeente Groningen (2022).

3.2 Operationalisatie

3.2.1 Slachtofferschap

Cybercrime. Eerst is aan participanten uit de gemeente Groningen middels een gesloten vraag (ja/nee) gevraagd of zij de afgelopen twaalf maanden persoonlijk slachtoffer zijn geworden van cybercrime. In Leeuwarden is die screeningsvraag niet gesteld. Aan participanten in beide gemeenten is gevraagd van welk type cybercrime zij slachtoffer waren. Participanten uit de gemeente Groningen konden hierbij één antwoordmogelijkheid selecteren, namelijk het laatst plaatsgevonden delict. Participanten uit de gemeente Leeuwarden konden bij ieder voorgelegd delict aangeven of zij in de afgelopen twaalf maanden wel of geen slachtoffer zijn geweest. Alle participanten kregen de opties: 1) oplichting bij het kopen van goederen of diensten via internet/e-mail/social media (*aan- en verkoopfraude)*; 2) afpersing of chantage via internet/e-mail/social media (*online afpersing*); 3) iemand die zonder toestemming gebruik heeft gemaakt van bankgegevens (*fraude bankgegevens*); 4) helpdeskfraude, waarbij iemand zich voordeed als helpdeskmedewerker (*helpdeskfraude*); 5) iemand die het mobiele-telefoon account overnam (*SIM-swapping*); 6) stalking via internet/e-mail/social media/telefoon (*online stalking*); 7) datingfraude, waarbij iemand slachtoffers financieel oplicht met als smoes dat het zou gaan om een liefdesrelatie of de weg daar-naar-toe (*online datingfraude*); en 8) hacken, waarbij iemand zich zonder toestemming en met opzet toegang heeft ver-

schaft tot de computer, het webwinkelaccount, de website of profielsite (*hacken*). Ook konden participanten zelf een cybercrimetype invullen. In Leeuwarden kregen participanten de vraag welk delict als laatste plaatsvond. De vervolgvragen gingen over dat delict. Van beide gemeenten beschikken we hiermee over gelijke informatie: of iemand slachtoffer is geworden van cybercrime en zo ja, wat het laatst plaatsgevonden delict was.

Traditionele criminaliteit. Eerst is aan Groningse participanten middels een gesloten vraag (ja/nee) gevraagd of zij in de afgelopen twaalf maanden slachtoffer zijn geweest van traditionele criminaliteit. De participanten kregen de opties: 1) inbraak in de woning (*woninginbraak*); 2) beroving van tas, portemonnee, telefoon of iets anders (*beroving*); 3) mishandeling, zoals slaan, schoppen of het gebruik van een mes (*mishandeling*); 4) bedreiging met geweld in de fysieke ruimte (*bedreiging*); 5) afpersing of chantage in de fysieke ruimte (*afpersing en chantage*); 6) stalking in de fysieke ruimte (*stalking*); 7) moedwillige vernieling of beschadiging van eigendommen zonder diefstal (*vernieling en vandalisme*); en 8) babbeltrucs, waarbij iemand aan de deur of op straat een smoes gebruikte voor een beroving (*babbeltruc*).

We includeerden participanten die aangaven slachtoffer te zijn geweest van een aan hen voorgelegd delict of van een door henzelf bij de optie 'anders namelijk' genoemd delict. Als uit de antwoorden bleek dat het ging om een 'poging tot' het delict, includeerden we deze niet.

3.2.2 Ervaren impact

Leeuwarders is middels een dichotome vraag (ja/nee) gevraagd naar de gevolgen die het recentste delict voor hen had: 1) emotionele/psychische gevolgen, zoals woede, angst, onzekerheid; 2) lichamelijke/fysieke gevolgen zoals slecht slapen en lichamelijke klachten; 3) sociale/gedragsmatige gevolgen zoals verlies aan vertrouwen, vermijden van het internet en problemen in relaties; 4) tijd die het voorval heeft gekost; en 5) financiële/materiële schade, zoals het kwijtraken van geld en niet meer/minder kunnen werken. Bij deze laatste categorie is ook gevraagd naar de schade in euro's en hoeveel is vergoed door de bank, verzekering of creditcardmaatschappij.

Groningers is middels een vijf-punts Likert-schaal, van 1 (gevolg niet ervaren) tot en met 5 (gevolg in sterke mate ervaren), gevraagd naar de gevolgen van het delict. Daarbij zijn de volgende stellingen voorgelegd: a) Ik blijf/bleef hier regelmatig aan terugdenken, het laat/liet me niet los; b) Ik maak/maakte me hier erg boos over; c) Ik was/ben hierdoor bang dat het vaker mis kan gaan; d) Ik sliep/slaap hierdoor slechter; e) Mijn eetlust of gewicht veranderde hierdoor; f) Ik had/heb hierdoor last van hoofdpijn; g) Ik vermeed/vermijd hierdoor bepaalde plaatsen/het internet; h) Ik had/heb hierdoor minder vertrouwen in andere mensen; i) Ik had/heb hierdoor problemen in mijn relaties (bijv. met familie, partner of vrienden); j) Ik ben hierdoor geld kwijtgeraakt aan het oplossen van door het delict veroorzaakte problemen; k) Ik heb hierdoor minder of niet kunnen werken; en l) Ik ben hierdoor in de financiële problemen geraakt.

doi: 10.5553/TvV/.000045

Om de data uit beide gemeenten samen te voegen, zijn de antwoorden uit de vijfpunts Likert-schaal van de gemeente Groningen gecodeerd naar dichotome antwoordmogelijkheden (1 = 'niet ervaren'; 2 tot en met 5 = 'ervaren'). Hierbij is ook de antwoordmogelijkheid 'niet van toepassing' gecodeerd als 'niet ervaren'. Daarnaast zijn de antwoordmogelijkheden van de vragen over impact van slachtofferschap van de gemeente Groningen te herleiden tot dezelfde categorieën als bij de gemeente Leeuwarden (tabel 1).

Tabel 1 Categorieën impact Groningen en Leeuwarden

Categorie impact gemeente Leeuwarden	**Items gemeente Groningen**
Emotionele/psychische impact	– (a) Ik blijf/bleef hier regelmatig aan terugdenken, het laat/liet me niet los – (b) Ik maak/maakte me hier erg boos over – (c) Ik was/ben hierdoor bang dat het vaker mis kan gaan
Lichamelijke/fysieke impact	– (d) Ik sliep/slaap hierdoor slechter – (e) Mijn eetlust of gewicht veranderde hierdoor – (f) Ik had/heb hierdoor last van hoofdpijn
Sociale/gedragsmatige impact	– (g) Ik vermeed/vermijd hierdoor bepaalde plaatsen/het internet – (h) Ik had/heb hierdoor minder vertrouwen in andere mensen – (i) Ik had/heb hierdoor problemen in mijn relaties
Financiële impact	– (j) Ik ben hierdoor geld kwijtgeraakt aan het oplossen van door het delict veroorzaakte problemen – (k) Ik heb hierdoor minder of niet kunnen werken – (l) Ik ben hierdoor in de financiële problemen geraakt

3.2.3 Behoeften

Aan Groningers is gevraagd welke behoeften zij hadden na hun slachtofferschap van cybercrime of traditionele criminaliteit. Dit is middels een vijfpunts Likert-schaal gemeten, van 1 (geen behoefte) tot en met 5 (sterke behoefte). De volgende behoeften zijn aan participanten voorgelegd: 1) Opsporing van de dader; 2) Informatie over het politieonderzoek (uitgesloten indien niet gemeld bij de politie); 3) Compensatie voor de geleden schade; 4) Serieus genomen worden als slachtoffer; 5) Emotionele steun, iemand om mee te praten; 6) Tips om toekomstig slachtofferschap te voorkomen; 7) Voorkomen dat andere mensen slachtoffer worden van hetzelfde delict; 8) Praktische hulp bij het oplossen van door het delict ontstane problemen; 9) Straf voor de dader; en 10) Duidelijkheid over hoe het delict heeft kunnen plaatsvinden.

Uit een principale factoranalyse blijkt dat 'opsporing van de dader' (cybercrime: 0,85; traditionele criminaliteit: 0,89) en 'straf voor de dader' (cybercrime: 0,78; traditionele criminaliteit: 0,66) laden op één component bij zowel cybercrime (Eigenwaarde >1; Kaiser-Meyer-Olkin = 0,856; Bartlett's toets $p < 0{,}01$) als traditionele criminaliteit (Eigenwaarde > 1; Kaiser-Meyer-Olkin = 0,834; Bartlett's toets $p < 0{,}01$) Deze twee behoeften worden hierna samengenomen als 'vergelding'.

3.3 Slachtofferschap in de gemeenten

Tabel 2 geeft een overzicht van het slachtofferschap per delict-type. In Groningen is niet specifiek gevraagd naar *fietsendiefstal*, maar dit kwam dermate vaak naar voren bij 'anders namelijk …' dat deze categorie is toegevoegd.

Tabel 2 Slachtofferschap cybercrime en traditionele criminaliteit

Delict cybercrime	Groningen N (%)	Leeuwarden N (%)	Delict traditionele criminaliteit	Groningen N (%)
Aan- en verkoopfraude	41 (2,4%)	103 (5,8%)	Vernieling en vandalisme	26 (1,5%)
Online afpersing	16 (1,0%)	38 (2,2%)	Fietsendiefstal	10 (0,6%)
Helpdeskfraude	13 (0,8%)	88 (5,0%)	Woninginbraak	8 (0,5%)
Hacken	12 (0,7%)	45 (2,5%)	Mishandeling	5 (0,3%)
Fraude bankgegevens	8 (0,5%)	34 (1,9%)	Bedreiging	4 (0,2%)
Online stalking	3 (0,2%)	60 (3,4%)	Afpersing en chantage	4 (0,2%)
Online datingfraude	3 (0,2%)	8 (0,4%)	Stalking	2 (0,1%)
SIM-swapping	2 (0,1%)	15 (0,8%)	Babbeltruc	2 0,1%)
			Beroving	1 (0,1%)

3.4 Statistische toetsing

Omdat het een exploratief onderzoek betreft, is telkens getoetst met een significantieniveau van $p < 0.05$. Een mogelijke verklaring voor de lagere slachtofferpercentages voor cybercrime in Groningen is dat wanneer participanten hadden aangegeven slachtoffer te zijn geweest, hen geen mogelijkheid is geboden om meerdere delicten te selecteren. Participanten uit de gemeente Leeuwarden konden bij alle delicten aangeven of zij wel of niet slachtoffer zijn geweest. Een andere, mogelijke verklaring voor de lagere slachtofferpercentages in Groningen is dat slachtoffers hun ervaren delict niet als cybercrime of traditionele criminaliteit zagen en bij de vraag over slachtofferschap 'nee' hebben ingevuld. Gevolg is dat zij de afzonderlijke delicten niet aangeboden kregen. Overigens tonen gemeenten ook bij eenzelfde onderzoeksmethode verschillende slachtofferpercentages (CBS, 2022b). Het waarom van verschillen tussen gemeenten valt echter buiten het bestek van dit onderzoek.

- *Deelvraag 1: impact van cybercrime versus impact van traditionele criminaliteit*

Bij de eerste deelvraag is gebruik gemaakt van een *t*-toets, zodat de gemiddelde impact van Groningse cybercrime-slachtoffers vergeleken kan worden met de gemiddelde impact van slachtoffers van traditionele criminaliteit.

Er zijn relatief veel slachtoffers van *aan- en verkoopfraude* (tabel 2). De (emotionele) impact van *aan- en verkoopfraude* is relatief laag (CBS, 2022a), wat mogelijk invloed

heeft op de gemiddeld ervaren impact van cybercrime. Daarom zijn drie toetsen uitgevoerd, namelijk vergelijkingen tussen traditionele criminaliteit en: 1) alle cybercrimes; 2) alle cybercrimes uitgezonderd *aan- en verkoopfraude* (bedoeld om een evenwichtige verdeling van delicten over te houden); en 3) *aan- en verkoopfraude*.

- *Deelvraag 2: impact van cybercrimedelicten onderling vergeleken*

Met een combinatie van de data uit Groningen en Leeuwarden is een vergelijking gemaakt tussen de impact van de verschillende cyberdelicten. *Online dating-fraude* en *SIM-swapping* zijn hierbij uitgesloten vanwege de lage *N*. Hierbij is een chi-kwadraat toets gebruikt. Vervolgens zijn *adjusted residuals* gebruikt om significante afwijkingen in de delicten te onderscheiden.

- *Deelvraag 3: behoeften bij cybercrime versus behoeften bij traditionele criminaliteit*

Bij de derde deelvraag is gebruik gemaakt van een *t*-toets, waarbij per soort behoefte de gemiddelden van cybercrimeslachtoffers zijn vergeleken met de gemiddelden van slachtoffers van traditionele criminaliteit. We gebruiken hiervoor de data uit Groningen (in Leeuwarden is niet naar behoeften gevraagd). Net als bij de eerste deelvraag is de toets uitgevoerd over drie groepen: 1) alle cybercrimes; 2) alle cybercrimes uitgezonderd *aan- en verkoopfraude*; en 3) *aan- en verkoopfraude*. Bij de behoefte 'compensatie voor geleden schade' zijn alleen participanten met financiële impact meegenomen, wat een te lage *N*-waarde oplevert voor de tweede en derde toets. Daarom is voor deze behoefte alleen een vergelijking gemaakt tussen cybercrimeslachtoffers en slachtoffers van traditionele criminaliteit.

4 Resultaten

4.1 Impact cybercrime versus impact traditionele criminaliteit

Allereerst vergelijken we de impact van alle cybercrimes samen met die van traditionele criminaliteit (tabel 3). Er is een significant verschil bij emotionele/psychische impact: $t(154) = -1{,}907$; $p = 0{,}03$. De score van cybercrime ($M = 2{,}27$; $SD = 0{,}93$) is *lager* dan die van traditionele criminaliteit ($M = 2{,}55$; $SD = 0{,}81$). Bij lichamelijke/fysieke impact is eveneens een significant verschil: $t(108) = 1{,}968$; $p = 0{,}03$. Ook hier is de score van cybercrime ($M = 0{,}65$; $SD = 1{,}02$) *lager* dan die van traditionele criminaliteit ($M = 1{,}02$; $SD = 1{,}23$). Er zijn geen significante verschillen in sociale/gedragsmatige impact: $t(154) = -0{,}605$; $p = 0{,}27$ en financiële impact: $t(106) = -1{,}604$; $p = 0{,}06$.

Vervolgens vergelijken we de impact van cybercrime, exclusief *aan- en verkoopfraude*, met die van traditionele criminaliteit. Er zijn geen significante verschillen in emotionele/psychische impact: $t(113) = -1{,}134$; $p = 0{,}13$, lichamelijke/fysieke impact: $t(113) = -1{,}091$; $p = 0{,}14$, sociale/gedragsmatige impact: $t(113) = 0{,}222$; $p = 0{,}41$ en financiële impact: $t(113) = -1{,}427$; $p = 0{,}08$.

Tot slot vergelijken we de impact van *aan- en verkoopfraude* met die van traditionele criminaliteit. Er is een significant verschil in emotionele/psychische impact:

$t(99) = -2{,}236$; $p = 0{,}02$. De score van *aan- en verkoopfraude* ($M = 2{,}15$; $SD = 0{,}91$) is lager dan die van traditionele criminaliteit ($M = 2{,}55$; $SD = 0{,}81$). Ook bij lichamelijke/fysieke impact is een significant verschil: $t(98) = -2{,}580$; $p = 0{,}01$ en ook hier is de score van *aan- en verkoopfraude* ($M = 0{,}46$; $SD = 0{,}92$) lager dan die van traditionele criminaliteit ($M = 1{,}02$; $SD = 1{,}23$). Er is geen significant verschil in sociale/gedragsmatige impact: $t(99) = -1{,}461$; $p = 0{,}15$ en financiële impact: $t(99) = -1{,}411$; $p = 0{,}16$.

Tabel 3 ***t-toets impact traditionele criminaliteit en cybercrime***

Impact	***M* cybercrime (*SD*)**	***N***	***M* cybercrime *zonder aan- en verkoopfraude* (*SD*)**	***N***	***M* cybercrime *aan- en verkoopfraude* (*SD*)**	***N***	***M* traditionele criminaliteit (*SD*)**	***N***
Emotioneel/ psychisch	2,27 (0,93)*	96	2,36 (0,95)	55	2,15 (0,91)*	41	2,55 (0,81)	60
Lichamelijk/ fysiek	0,65 (1,02)*	96	0,78 (1,07)	55	0,46 (0,92)*	41	1,02 (1,23)	60
Sociaal/ gedragsmatig	0,98 (1,05)	96	1,13 (1,07)	55	0,78 (0,99)	41	1,08 (1,05)	60
Financieel	0,57 (0,86)	96	0,56 (0,96)	55	0,59 (0,71)	41	0,83 (1,06)	60

* $p < 0{,}05$

4.2 Impact cybercrimedelicten onderling vergeleken

Hierna vergelijken we de impact van de verschillende cybercrimes onderling met elkaar (tabel 4). We bespreken alleen de significante bevindingen.

Een X^2-toets toont significante verbanden tussen drie typen impact en het delict: 1) emotionele impact: $X^2(1) = 8{,}83$; $p < 0{,}01$; 2) lichamelijke impact: $X^2(1) = 4{,}81$; $p = 0{,}02$; en 3) financiële impact: $X^2(1) = 39{,}19$; $p < 0{,}01$ en $X^2(1) = 4{,}48$; $p = 0{,}03$.

De *adjusted residuals* laten zien dat significant minder slachtoffers van *aan- en verkoopfraude* lichamelijke impact ervaren dan slachtoffers van andere delicten. Daarnaast ervaren significant minder slachtoffers van helpdeskfraude emotionele impact dan slachtoffers van andere delicten. Ten slotte ervaren significant meer slachtoffers van *aan- en verkoopfraude* financiële impact, terwijl minder slachtoffers van *afpersing of chantage*, ten opzichte van de andere delicten, deze impact ervaren.

Tijdschrift voor Veiligheid 2022 (21) 3-4
doi: 10.5553/TvV/.000045

Tabel 4 *X^2-toets vergelijking impact cyberdelicten met adjusted residuals (% wel genoemd)*

Delict **Impact**	***aan- en verkoop-fraude* (% wel ge-noemd)**	***N***	***Afper-sing of chantage* (% wel ge-noemd)**	***N***	***Fraude bankge-gevens* (% wel ge-noemd)**	***N***	***Help-desk fraude* (% wel ge-noemd)**	***N***	***Online stalking* (% wel ge-noemd)**	***N***	***Hacken* (% wel ge-noemd)**	***N***
Emotioneel	−0,4 (58,1%)	117	−0,3 (54,5%)	44	−0,8 (60,0%)	30	−3,0 (40,9%)	66	0,7 (61,9%)	42	−1,0 (50,0%)	42
Lichamelijk	−2,2 (11,1%)	117	−0,7 (13,6%)	44	−0,6 (13,3%)	30	−0,8 (13,6%)	66	−1,0 (11,9%)	42	1,7 (26,2%)	42
Sociaal	−1,3 (29,9%)	117	−1,3 (22,7%)	44	−0,1 (30,0%)	30	−1,9 (21,2%)	66	−1,0 (23,8%)	42	−1,8 (42,9%)	42
Tijd	−0,1 (19,7%)	76	−0,3 (17,9%)	28	1,4 (22,7%)	22	−1,8 (11,3%)	53	1,0 (25,6%)	39	1,5 (30,0%)	30
Financieel	6,3 (58,1%)	117	−2,1 (22,7%)	44	0,7 (43,3%)	30	−1,9 (27,3%)	66	−1,2 (28,6%)	42	−1,6 (26,2%)	42

4.3 Behoeften bij cybercrime versus behoeften bij traditionele criminaliteit

In deze paragraaf vergelijken we de behoeften van cybercrimeslachtoffers met die van slachtoffers van traditionele criminaliteit (tabel 5).

We kijken, net als in paragraaf 4.1, eerst naar alle cybercrime samen, daarna naar cybercrime zonder *aan- en verkoopfraude* en tot slot naar *aan- en verkoopfraude*.

Over alle cybercrimes gezien verschillen de behoeften van slachtoffers op drie punten van die van slachtoffers van traditionele criminaliteit. Bij cybercrime scoren de slachtoffers significant lager op 'informatie krijgen over het politieonderzoek' ($t(113) = -3{,}048$; $p < 0{,}01$) en 'serieus worden genomen als slachtoffer' ($t(154) = -3{,}097$; $p < 0{,}01$) - twee behoeften die zijn te zien als persoonlijke belangen van het slachtoffer. Ze scoren juist significant hoger op 'voorkomen dat anderen slachtoffer worden' ($t(154) = 2{,}522$; $p < 0{,}01$). Dit beeld wijzigt enigszins wanneer we *aan- en verkoopfraude* apart nemen.

Slachtoffers van cybercrime zonder *aan- en verkoopfraude* scoren in vergelijking met slachtoffers van traditionele criminaliteit significant lager op de behoefte 'vergelding': $t(113) = -2{,}184$; $p = 0{,}02$) en 'informatie krijgen over het politieonderzoek' ($t(108) = -4{,}738$; $p < 0{,}01$) . Ze scoren daarentegen significant hoger op 'duidelijkheid krijgen over hoe het delict heeft kunnen gebeuren' ($t(113) = 3{,}349$; $p < 0{,}01$).

Slachtoffers van *aan- en verkoopfraude* scoren significant hoger dan slachtoffers van traditionele criminaliteit op de behoeften 'vergelding': ($t(97) = 1{,}727$; $p = 0{,}04$) en 'voorkomen dat anderen slachtoffer worden' ($t(99) = 3{,}734$; $p < 0{,}01$). De zo-even genoemde behoeften die we kunnen zien als persoonlijke belangen, komen bij deze groep slachtoffers niet meer zo naar voren.

Dat slachtoffers van cybercrime hoger scoren op 'voorkomen dat anderen slachtoffer worden' is dus vooral toe te rekenen aan slachtoffers van *aan- en verkoopfraude*. Daarentegen zien we dat de slachtoffers van *aan- en verkoopfraude*, in vergelijking met slachtoffers van traditionele criminaliteit, niet opvallend laag scoren op de drie behoeften die we aanduidden als persoonlijke belangen van het slachtoffer ('informatie krijgen over het politieonderzoek', 'compensatie voor geleden schade' en 'serieus worden genomen als slachtoffer'). De verschillen met slachtoffers van traditionele criminaliteit zijn dus vooral gerelateerd aan slachtoffers van cybercrime zonder *aan- en verkoopfraude*.

Samengevat typeren slachtoffers van *aan-en verkoopfraude* zich, in vergelijking met slachtoffers van traditionele criminaliteit, door een hoge score op 'vergelding' en vooral 'voorkomen dat anderen slachtoffer worden'. Slachtoffers van cybercrime zonder *aan- en verkoopfraude* typeren zich, op vergelijkbare wijze gezien, door een lage score op 'vergelding', 'informatie over het politieonderzoek', 'compensatie voor geleden schade' en 'serieus worden genomen als slachtoffer', en juist een hoge score op 'duidelijkheid over hoe het delict heeft kunnen plaatsvinden'.

Tijdschrift voor Veiligheid 2022 (21) 3-4
doi: 10.5553/TvV/.000045

Tabel 5 Verschil in behoeften

Behoeften	*M* cybercrime (*SD*)	*N*	*M* cybercrime zonder *aan- en verkoopfraude* (*SD*)	*N*	*M* cybercrime *aan- en verkoop-fraude* (*SD*)	*N*	*M* traditionele criminaliteit (*SD*)	*N*
Vergelding[a]	6,92 (3,27)	96	5,95 (3,51)*	55	8,22 (2,38)*	41	7,28 (3,05)	60
Informatie over het politie-onderzoek	1,50 (1,89)**	96	0,87 (1,58)**	55	2,34 (1,97)	41	2,53 (2,16)	60
Compensatie voor geleden schade[b]	1,81 (1,99)	96	X		X		2,67 (1,87)	60
Serieus worden genomen als slachtoffer	1,89 (1,96)**	96	1,51 (1,91)**	55	2,39 (1,92)	41	2,87 (1,87)	60
Emotionele steun; iemand om mee te praten	1,60 (1,59)	96	1,85 (1,81)	55	1,27 (1,16)	41	1,67 (1,50)	60
Tips om toekomstig slachtoffer-schap te voorkomen	1,81 (1,66)	96	1,87 (1,68)	55	1,73 (1,66)	41	1,57 (1,36)	60
Voorkomen dat anderen slachtoffer worden	3,31 (1,86)**	96	2,95 (2,00)	55	3,80 (1,55)**	41	2,57 (1,69)	60

Tabel 5 *(Vervolg)*

Behoeften	*M* cybercrime (*SD*)	*N*	*M* cybercrime zonder *aan- en verkoopfraude* (*SD*)	*N*	*M* cybercrime *aan- en verkoop-fraude* (*SD*)	*N*	*M* traditionele criminaliteit (*SD*)	*N*
Praktische hulp bij het oplossen van door het delict ontstane problemen	1,94 (1,79)	96	1,80 (1,84)	55	2,12 (1,72)	41	1,93 (1,65)	60
Duidelijkheid over hoe het delict heeft kunnen plaatsvinden	2,72 (1,91)	96	3,16 (1,81)**	55	2,12 (1,89)	41	2,03 (1,80)	60

* $p < 0{,}05$; ** $p \leq 0{,}01$

[a] Samengevoegde variabelen na factoranalyse

[b] Alleen getoetst met participanten met financiële impact

5 Conclusie en discussie

Dit artikel richt zich op de verschillen in impact en behoeften na slachtofferschap van cybercrime en traditionele criminaliteit.

5.1 Conclusie

Onderzoeksvraag 1:In hoeverre verschilt de slachtofferimpact van cybercrime van die van traditionele criminaliteit?

De impact die slachtoffers van cybercrime ervaren lijkt niet significant te verschillen van de impact die slachtoffers van traditionele criminaliteit ervaren. Aan- en verkoopfraude heeft hierbij een aanzienlijke invloed op de gemiddeld ervaren impact, aangezien het veel voorkomt en de impact relatief laag is. Voornamelijk wanneer aan- en verkoopfraude wordt uitgesloten, suggereren de resultaten dat er geen verschil is in emotionele/psychische, lichamelijke/fysieke, sociale/gedragsmatige en financiële impact tussen slachtoffers van cybercrime en traditionele criminaliteit.

Onderzoeksvraag 2: In hoeverre ervaren slachtoffers van cybercrimes de verschillende typen impact?

Significant minder slachtoffers van aan- en verkoopfraude ervaren lichamelijke impact dan slachtoffers van andere delicten. Daarnaast ervaren minder slachtoffers van helpdeskfraude emotionele impact dan slachtoffers van andere delicten. Mogelijk hebben participanten een poging tot helpdeskfraude ook benoemd als slachtofferschap; dit is met de huidige data niet te achterhalen. Vervolgonderzoek zou daarom onderscheid moeten maken tussen een poging tot en daadwerkelijk slachtofferschap. Daarnaast ervaren significant meer slachtoffers van aan- en verkoopfraude financiële impact, terwijl minder slachtoffers van afpersing of chantage deze impact ervaren. Waarschijnlijk heeft dit te maken met de aard van de delicten, waarbij aan- en verkoopfraude te maken heeft met financieel gewin, terwijl afpersing of chantage ook ergens anders op gericht kan zijn. Ten slotte, minder slachtoffers van aan- en verkoopfraude ervaren lichamelijke impact ten opzichte van slachtoffers van andere delicten.

Onderzoeksvraag 3: In hoeverre hebben cybercrimeslachtoffers andere behoeften dan slachtoffers van traditionele criminaliteit?

Slachtoffers van alle in dit onderzoek betrokken cybercrimes samengenomen hebben minder behoefte aan informatie over het politieonderzoek en serieus worden genomen als slachtoffer dan slachtoffers van traditionele criminaliteit. Mogelijk heeft dit te maken met lagere verwachtingen van slachtoffers over de acties van de politie na aangifte (Leukfeldt et al., 2018). Slachtoffers van cybercrime hebben daarentegen wel meer behoefte aan het voorkomen dat anderen slachtoffer worden. Dit kan zijn veroorzaakt door de lagere prioritering van cybercrime door de politie (Borwell et al., 2021a), waardoor slachtoffers elkaar hiervoor willen behoeden. Een andere verklaring is dat cybercrimeslachtoffers geregeld niet weten hoe het delict is gepleegd (zie hierna) en ze willen dat anderen hiervan ook op de hoogte zijn.

Wanneer aan- en verkoopfraude wordt uitgesloten, is de behoefte aan vervolging en informatie over het onderzoek lager bij cybercrimeslachtoffers dan bij slachtoffers van traditionele criminaliteit. Mogelijk wordt dit veroorzaakt doordat slachtoffers moeilijkheden ondervinden bij het doen van aangifte en niet op de gewenste manier geholpen worden. Hierdoor hebben ze geen (hoge) verwachtingen van opsporing van de dader (Leukfeldt et al., 2018). Daarentegen hebben slachtoffers van cybercrime meer behoefte aan duidelijkheid over hoe het delict heeft kunnen plaatsvinden. Een mogelijke verklaring is dat slachtoffers het idee hebben dat cybercrime hen nogmaals kan overkomen door de ongrijpbaarheid hiervan (Borwell et al., 2021a), en om deze reden willen begrijpen wat er gebeurd is, zodat ze toekomstig slachtofferschap kunnen voorkomen. Daarnaast weten slachtoffers van deze delicten, ten opzichte van slachtoffers van aan- en verkoopfraude, door de complexiteit van de delicten vaak niet hoe het delict heeft kunnen plaatsvinden. Een andere verklaring is dat 'weten hoe het is gebeurd', inzicht kan verschaffen in de eigen rol bij de voltooiing van het delict. Dit kan helpen bij het verwerken ervan en het voorkomen van toekomstig slachtofferschap.

Wanneer aan- en verkoopfraude afzonderlijk wordt vergeleken met traditionele criminaliteit, blijkt dat slachtoffers van dit delict meer behoefte hebben aan vervolging van de dader en voorkomen dat anderen slachtoffer worden dan slachtoffers van traditionele criminaliteit. Een mogelijke verklaring is dat de slachtoffers van aan- en verkoopfraude vaak enige gegevens van de dader hebben en willen dat de politie daarmee iets doet. Een andere reden kan zijn dat wanneer een onderzoek wordt gestart om de dader op te sporen en te straffen, slachtoffers perspectief krijgen om een schadevergoeding te eisen van de dader (Leukfeldt et al., 2018). Bij aan- en verkoopfraude was relatief vaak sprake van financiële impact, wat in lijn ligt met deze verklaring.

5.2 Discussie

Cybercrime komt vaak voor en wordt (ook) vaak door Nederlandse daders gepleegd, en dient daarom ook lokaal te worden bestreden, met belangrijke rollen voor basisteams van de politie en voor gemeenten. Die zijn daarop nog matig ingespeeld. Voor een adequate aanpak hebben zij, onder andere, kennis nodig over de impact van cybercrime op slachtoffers en over behoeften die de slachtoffers naderhand hebben. Dit kan helpen voor adequatere slachtofferzorg en voor preventiebeleid, omdat men kan focussen op weerbaarheid tegen de delicten met de grootste impact.

Uit de resultaten komt naar voren dat wanneer cybercrime wordt afgezet tegen traditionele criminaliteit (met uitsluiting van aan- en verkoopfraude), de ervaren impact van de twee soorten criminaliteit niet lijkt te verschillen. Daarmee lijkt de impact van cybercrime tevens niet onder te doen voor die van traditionele criminaliteit, al is beleid van politie en gemeenten voor deze twee typen criminaliteit niet in balans. Momenteel worden cybercrimes namelijk niet gezien als 'high impact crime' (HIC). Traditionele high impact crimes zijn delicten waarvan de impact op slachtoffers groot is en mogelijk ook invloed hebben op de directe omgeving (Van

Tijdschrift voor Veiligheid 2022 (21) 3-4
doi: 10.5553/TvV/.000045

Dijk &Van Soomeren, 2021). Hierbij gaat het om woninginbraken, straatroven en overvallen. Waar cybercrime en traditionele criminaliteit een vergelijkbare impact hebben, zouden politie en gemeenten cybercrime in hun slachtofferzorg meer kunnen prioriteren, wat kan resulteren in een passender nazorg voor cybercrimeslachtoffers. Het is mogelijk dat de impact van verschillende cyberdelicten en traditionele criminaliteitsdelicten onderling verschillen (Borwell et al., 2021a). In het huidige onderzoek is onderzocht hoe de ervaren impact na slachtofferschap van een aantal cybercrimedelicten onderling verschilt. Vervolgonderzoek kan uitwijzen in hoeverre de impact van delicten, zowel cybercrime als traditionele criminaliteit, onderling verschilt en welke typen impact worden ervaren bij welke delicten.

De resultaten suggereren dat slachtoffers van cybercrime in mindere mate behoefte hebben aan onder andere vergelding en informatie over het politieonderzoek. Opsporing van de daders van cybercrimes kan ook lastig zijn door de anonimiteit en grenzeloosheid van cyberdelicten (Leukfeldt et al., 2018; Borwell et al., 2021a). Daarentegen hebben slachtoffers meer behoefte aan duidelijkheid over hoe het delict heeft kunnen plaatsvinden. Mogelijk kunnen gemeenten en politie beleidsmatig meer focussen op het voorzien in duidelijkheid over het plaatsgevonden delict voor slachtoffers, wat ook de weerbaarheid vergroot, en daarmee de kans op toekomstig slachtofferschap verkleint.

Daarnaast kunnen slachtoffers van cybercrime mogelijk andere behoeften hebben dan die in dit onderzoek aanbod kwamen, bijvoorbeeld het offline halen van beelden of documenten. Vervolgonderzoek is gewenst om te bepalen of slachtoffers van cybercrime mogelijk andere behoeften hebben dan de behoeften die in dit onderzoek bevraagd zijn. Aandacht voor aanvullende behoeften kan bijdragen aan de verbetering van de nazorg van cybercrimeslachtoffers.

Bij de data-analyse is naar voren gekomen dat een aantal participanten een poging tot een cyberdelict heeft omschreven bij slachtofferschap en daarbij impact heeft ervaren. Hierbij ging het voornamelijk om het delict phishing. Voor dit onderzoek zijn deze respondenten uitgesloten. Volgens Junger et al. (2022) heeft 41,7% van de Nederlanders van 16 jaar of ouder in 2020 een fraude-poging meegemaakt. Ook hier ging het voornamelijk om phishing. Een deel daarvan (20,6%) heeft hierop gereageerd, al heeft dit niet in alle gevallen geleid tot slachtofferschap. Door de lage *N* en omdat dit buiten de scope van het onderzoek valt, is de impact van slachtoffers bij een poging in dit onderzoek niet nader onderzocht. Echter, vanwege het feit dat slachtoffers aangaven impact te hebben ervaren na een poging en de prevalentie van een poging tot een fraudedelict, is vervolgonderzoek gewenst waarin de ervaren impact na een poging tot cybercrime centraal staat.

5.3 Beperkingen

Deze studie is gebaseerd op bevolkingsonderzoeken in de gemeenten Groningen en Leeuwarden en is mogelijk niet representatief voor heel Nederland. Bij de participanten in Groningen zijn de leeftijdsgroepen van 18-22, 23-27, 28-34, 50-64, en 65-74 jaar bovendien over- of ondervertegenwoordigd. De resultaten moeten dus met enige voorzichtigheid worden bezien. Deze studie is een eerste aanzet tot een

brede vergelijking tussen gevolgen na slachtofferschap van cybercrimes en traditionele criminaliteit. De dataset van 3.462 participanten bevat niet genoeg slachtoffers om alle delictsoorten apart uit te lichten en onderling met elkaar te vergelijken. Ook zijn meer behoeften en elementen van impact denkbaar dan hier aan bod kwamen. Ten slotte hebben Groningers, door de screeningsvraag, hun ervaren delict mogelijk niet beschouwd als cybercrime of traditionele criminaliteit, waardoor zij niet voor de afzonderlijke delicten slachtofferschap hebben kunnen aangeven. Vervolgonderzoek zal dan ook gericht moeten zijn op het verfijnen van de gepresenteerde bevindingen.

Literatuur

Boom, A. ten, K.F. Kuijpers & M.H. Moene (2008) *Behoeften van slachtoffers van delicten een systematische literatuurstudie naar behoeften zoals door slachtoffers zelf geuit*. Den Haag: Boom Juridische uitgevers.

Borwell, J., J. Jansen & W. Stol (2021a) Comparing the victimization impact of cybercrime and traditional crime. *Journal of Digital Social Research*, *3*(3), 85-110. doi. org/10.33621/jdsr.v3i3.66

Borwell, J., J. Jansen & W. Stol (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. doi.org/10.1177/0894439320983828

CBS (2022a) *De percentages slachtofferschap cybercrime verschillen namelijk ook per gemeente bij één meetmethode, bijvoorbeeld 9,6% in meierijstad en 17,7% in roosendaal*. https:// opendata.cbs.nl/#/CBS/nl/data¬set/82464¬NED¬/table?ts=¬1659017777315

CBS (2022b). *Veiligheidsmonitor 2021*. Den Haag: CBS.

Cross, C. (2018) Victims' motivations for reporting to the 'fraud justice network'. *Police Practice and Research*, *19*(6), 550-564. doi.org/10.1080/15614263.2018.1507891

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

Dijk, B. van & P. van Soomeren (2021) *Basisboek ProHIC*. Den Haag: Boom criminologie.

Domenie, M.M.L., E.R. Leukfeldt, J.A. van Wilsem, J. Jansen & W. Stol (2013) *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit*. Den Haag: Boom Lemma Uitgevers.

Gemeente Groningen (2022) *Bevolking 2022*. https://groningen.buurtmonitor.nl// jive?workspace_guid=257e93b4-b163-40a6-ba1e-34fe829874ce+

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

Holt, T.J. & A.M. Bossler (2008) Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1-25. doi. org/10.1080/01639620701876577

Holt, T.J. & A.M. Bossler (2013) An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*(1), 20-40. doi.org/10.1080/01639625.2013.822209

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

Junger, M., B. Veldkamp & L. Koning (2022) *Fraudevictimisatie in Nederland*. Enschede: Universiteit Twente.

Kerr, J., R. Owen, C.M. Nicholls & M. Button (2011) *Research on sentencing online fraud offences*. Sentencing Council.

Kleijer, P. (2020) *De aanpak van gedigitaliseerde criminaliteit binnen het basisteam*. Apeldoorn: Politieacademie.

Leeuwarden in cijfers (2022) *Inwoners naar leeftijd 2022*. https://leeuwarden.incijfers.nl/Jive?workspace_guid=0946c246-54eb-4485-9406-bbdd0607fedf

Leukfeldt, R., R. Notté & L. Koning (2016) *Slachtofferschap van online criminaliteit*. Den Haag: WODC.

Loenhout, B. van (n.n.g.) *Politie georganiseerd digitaal*. Apeldoorn: Politieacademie.

Modic, D. & R. Anderson (2015) It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy*, *13*(5), 99-103. doi.org/10.1109/msp.2015.107

Stol, W.Ph. & W. Bantema (2020) Stadsbestuur en digitale veiligheid. Een analyse van beleidsplannen. In: M. Malsch & J.W. Sap (red.), *Orde en verwarring in de stad* (pp. 363-385). Den Haag: Boom criminologie.