‘Veiliger offline dan online?’

Een studie naar burger- en politieperspectieven op slachtofferimpact en behoefte(voorziening) na slachtofferschap van cybercriminaliteit en traditionele criminaliteit in Noord-Nederland

---

Geschreven door:

Reijer J. Peters

2681965

Opleiding:	Master Bestuurskunde – Besturen van veiligheid
Onderwijsinstelling:	Vrije Universiteit (VU) Amsterdam
Eerste lezer:	Dr. Y. Eski
Tweede lezer:	Dr. S. Çanyaka

Amsterdam, 9 augustus 2021

Vrije Universiteit Amsterdam, 9 Augustus 2021

Voorwoord

Voor u ligt mijn masterthesis over de slachtofferimpact en behoefte(voorziening) van cybercriminaliteit en traditionele criminaliteit volgens burgers en politiemedewerkers uit Noord-Nederland. Deze thesis is geschreven ter afsluiting van de master Bestuurskunde met de specialisatie van Veiligheid aan de Vrije Universiteit te Amsterdam. Deze thesis is tot stand gekomen door een bijdrage te leveren aan het promotieonderzoek van PhD kandidaat J. Borwell. In haar promotieonderzoek wordt onderzocht hoe de impact van cybercriminaliteit op slachtoffers zich verhoudt tot de impact van traditionele criminaliteit, en wat dit betekent voor de rol van de politie. Dit onderzoek loopt tot december 2022.

Voordat u deze thesis verder leest, wil ik graag een dankwoord richten aan iedereen die betrokken was bij de totstandkoming van deze thesis. Allereerst wil ik mijn thesisbegeleider dr. Y. Eski bedanken voor zijn begeleiding, kritische blik en toewijding tijdens het afstudeertraject. Daarnaast wil ik graag J. Borwell in het bijzonder bedanken. Borwell heeft mij gedurende dit thesistraject ondersteunt in de rol van actieve thesisbegeleider namens het CyberScienceCenter (CSC). Ik wil haar dan ook graag bedanken voor alle begeleiding, feedback, het benaderen van ambtenaren (waaronder politiemedewerkers) buiten mijn netwerk en alle hulp die hier niet staat bijgeschreven. Verder wil ik ook de andere betrokken namens het CSC bedanken. Dr. J. Jansen in de rol van co-begeleider en prof. dr. W. Stol als co-begeleider en het bieden van dit interessante vraagstuk. Bedankt voor jullie deskundigheid en betrokkenheid tijdens de Microsoft Teams sessies. Tenslotte wil ik mijn dank uitspreken naar de respondenten die tijd hebben vrijgemaakt om mee te werken aan dit onderzoek.

Ik wens u veel leesplezier toe,

Reijer J. Peters
Zwammerdam, 9 augustus 2021

Samenvatting

De cijfers van het Centraal bureau voor de Statistiek (CBS) laten zien dat het slachtofferpercentage van cybercriminaliteit (13% in 2019) bijna gelijk is aan die van traditionele criminaliteit (14% in 2019). Traditionele criminaliteit lijkt volgens de cijfers steeds meer af te nemen, terwijl de cybercriminaliteit gelijk blijft of toeneemt per jaar (Centraal Bureau voor de Statistiek, 2020a). Steeds meer universiteiten, wetenschappelijke kennisinstituten en hogescholen houden zich daarom bezig met onderzoek naar cybercriminaliteit (NWO, 2020).

Vooralsnog is er weinig tot geen onderzoek gedaan naar de vergelijking van traditionele criminaliteit en cybercriminaliteit, waarbij er wordt gekeken naar de slachtofferimpact en behoefte(voorziening) na slachtofferschap volgens niet-slachtoffers. Deze niet-slachtoffers betekenen in dit onderzoek, de perspectieven van burgers en politiemedewerkers in de basisteams. Dit heeft geleid tot de volgende centrale onderzoeksvraag: "*Wat is volgens de basisteams van de politie en burgers uit Noord-Nederland de slachtofferimpact en de behoefte(voorziening) na slachtofferschap van cybercriminaliteit in vergelijking met traditionele criminaliteit?"*

Deze onderzoeksvraag wordt beantwoord aan de hand van vijf empirische deelvragen en drie hypothesen op basis van een vignettenstudie (kwantitatieve onderzoeksmethode). Uit de kwantitatieve gegevens van 593 respondenten (N = 593) is gebleken dat de slachtofferimpact en behoefte na slachtofferschap volgens burgers (N = 461) groter is bij cybercriminaliteit dan bij traditionele criminaliteit. Ook blijkt de slachtofferimpact volgens politiemedewerkers (N = 132) groter bij cybercriminaliteit dan bij traditionele criminaliteit. Over de behoeftevoorziening na slachtofferschap kan geen significante uitspraak worden gedaan, dit moet in vervolgonderzoek blijken.

Daarnaast zijn de uitkomsten van het onderzoek ook interessant om verder onderzoek te doen naar de betekenis hiervan voor het politiebeleid en de inrichting van de basisteams. Het beleid lijkt op dit moment de prioriteiten te leggen bij traditionele criminaliteit, terwijl cybercriminaliteit steeds dominanter lijkt te worden.

Inhoudsopgave

Figuren en tabellen

Lijst van afkortingen

AI	Artificial Intelligence
CBS	Centraal Bureau voor de Statistiek
COP	Coördinatie Operationeel Politiewerk
CSC	CyberScienceCenter
CVV	Centrum voor criminaliteitspreventie en veiligheid
HIC	High Impact Crimes
IoT	Internet of Things
NWO	Nederlandse Organisatie voor Wetenschappelijk onderzoek
OSN	Online sociale netwerken
PPTS	Posttraumatische stressstoornis

Afkortingen van statistische gegevens

α	Cronbach's Alpha
M	Mean (gemiddelde)
N	Steekproefgrootte
SD	Standard deviation (standaard deviatie)
t	De toets statistiek voor de t-toets

Hoofdstuk 1. Inleiding

1.1 Aanleiding

In de afgelopen twee decennia is cybercriminaliteit in veel lagen van de bevolking een steeds meer besproken onderwerp geworden (Yar & Steinmetz, 2019). De technologische ontwikkelingen heeft de mensheid in grote mate afhankelijk gemaakt van internet. Het *cybercrime landschap* is parallel gegroeid met software en opkomende technologieën, zoals *Artificial intelligence (AI)* en *Internet of Things (IoT)* (Tavares et al., 2020). Het gebruik van deze nieuwe technologieën in criminaliteit maakt fictie niet meer te onderscheiden van de werkelijkheid, zoals de deepfake-technologie (Kwok & Koh, 2020). Dit maakt het voor criminelen interessant om zich steeds meer bezig te houden met de ontwikkelingen op het gebied van cybercriminaliteit.

In 2019 werd in het rapport Cybersecuritybeeld Nederland vastgesteld dat Nederland kwetsbaar is voor digitale aanvallen, doordat we achterblijven in weerbaarheid. Deze weerbaarheid geldt voor bedrijven, maar ook voor burgers (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2019). In het rapport 'Veilig Online 2020' is deze weerbaarheid van digitale veiligheid gepeild bij de Nederlandse bevolking. De vier belangrijkste bevindingen uit dit onderzoek waren dat het merendeel van de respondenten aangaf: (1) dat ze hun eigen onlinegedrag een voldoende geven, (2) vinden dat zij goed op de hoogte zijn van hun online veiligheid, (3) schatten de kans dat ze schade ondervinden van online risico's laag in en (4) maken zich beperkt zorgen om hun online veiligheid (Ministerie van Economische Zaken, 2020).

Ondanks deze bevindingen blijkt uit de cijfers van de Nederlandse politie dat het criminaliteitsbeleid in 2020 sterk is beïnvloed door de coronapandemie. Het valt op dat de coronapandemie vooral heeft geleid tot een toename van cybercriminaliteit (127 procent). Een onderzoek in Engeland wijst uit dat deze toename mogelijk verklaard kan worden door de verschuiving van de dagelijkse activiteiten van miljoenen mensen. De verschuiving van een fysieke omgeving naar een online omgeving (Buil-Gil et al., 2020).

Op basis van de cijfers bij het Centraal bureau voor de Statistiek (CBS) lijkt de cybercriminaliteit elk jaar lichtelijk toe te nemen. Het slachtofferpercentage was 12 procent in 2012 en 13 procent in 2019 (CBS, 2020a). Er zijn nog geen cijfers bekend bij het CBS na 2019. De politie daarentegen toont dat het aantal geregistreerde cybermisdrijven in 2020 aanzienlijk is toegenomen. Dit aantal was 4.715 in 2019 en 10.770 in 2020 (Politie, 2021). De verwachting is dan ook dat het slachtofferpercentage in 2020 hoger zal liggen mede door de coronapandemie (Buil-Gil et al., 2020). Verder tonen de cijfers van het CBS dat de traditionele criminaliteit steeds meer afneemt. Het slachtofferpercentage van traditionele criminaliteit was 20 procent in 2012 en 14 procent in 2019 (CBS, 2020a).

Ook wordt er steeds meer wetenschappelijk onderzoek gedaan naar de impact van cybercriminaliteit (Kanayama, 2017; Jansen & Leukfeldt, 2017), zoals onderzoek naar slachtofferschap en daderschap (Weulen Kranenbarg et al., 2017; Lee, 2018). Daarnaast wordt in wetenschappelijk onderzoek de vergelijking gemaakt tussen traditionele criminaliteit en cybercriminaliteit (Graham e.a., 2019; Kranenbarg e.a., 2018, 2017; van de Weijer & Leukfeldt, 2017). Daarnaast zijn universiteiten, wetenschappelijke kennisinstituten en hogescholen bezig met cybercriminaliteit (NWO, 2020). Een onderzoeksinstituut dat zich bezighoudt met onderzoek naar cybercriminaliteit is het CyberScienceCenter (CSC): 'een multidisciplinaire samenwerking van wetenschappers die bijdragen aan de veiligheid in de gedigitaliseerde samenleving' (CyberScienceCenter, z.d.).

Binnen dit onderzoeksinstituut houdt de onderzoeker, Borwell zich bezig met een onderzoek naar de slachtofferimpact van cybercriminaliteit in vergelijking met traditionele criminaliteit (verwacht 2022). Deze slachtofferimpact wordt in het onderzoek gemeten door vier impactvormen mee te nemen: (1) financieel/materieel, (2) psychologisch/emotioneel, (3) fysiek en (4) sociaal/gedragsmatig. Daarbij worden verschillende traditionele- en cybercriminaliteitsdelicten meegenomen en tegenover elkaar geplaats om deze vier impactvormen te meten. Deze slachtofferimpact meet Borwell bij slachtoffers van criminaliteit.

Het onderzoek van Borwell kan betrekking hebben op niet-slachtoffers, zoals het rapport 'Veilig Online 2020' dat onder burgers is gehouden. Dit betekent dat het dan gaat over de perceptie(s) van niet-slachtoffers op slachtofferschap. Het perspectief van burgers is hierbij van belang, omdat zij potentiële slachtoffers van criminaliteit zijn. Ook het rapport 'Veilig Online 2020' dat in 2019 is uitgevoerd, wijst uit dat burgers zich over het algemeen veilig 'online' voelen (Ministerie van Economische Zaken, 2020). Dit rapport is uitgevoerd vóór de coronapandemie en dus ook vóór de 127 procent toename van cybercriminaliteit. Dit is een aanleiding om het perspectief van burgers ten aanzien van slachtofferschap mee te nemen in dit onderzoek.

Daarnaast is het interessant om het perspectief van politiemedewerkers mee te nemen in dit onderzoek. Vooral de politiemedewerkers die werkzaam zijn in de voorste linie (de basisteams), omdat zij vaak het eerste aanspreekpunt zijn voor burgers en slachtoffers van criminaliteit. Ook is dit perspectief van belang voor de aanpak en rol van politiemedewerkers bij slachtofferschap.

Verder blijkt ook de behoefte en behoeftevoorziening na slachtofferschap sterk samen te hangen met de impact die het delict heeft gehad op het slachtoffer (Leukfeldt et al., 2018, p. 40). De behoefte die burgers hebben en in hoeverre de politie in deze behoeften denkt te kunnen voorzien. Ook dit is een aanleiding om de behoefte en behoeftevoorziening na slachtofferschap mee te nemen in dit onderzoek.

1.2 Doel- en vraagstelling

Dit onderzoek is een vergelijkend onderzoek, dan wel verkennend onderzoek naar de slachtofferimpact en behoefte(voorziening) na slachtofferschap van cybercriminaliteit in vergelijking met traditionele criminaliteit. In dit onderzoek wordt de nadruk gelegd op de perspectieven van burgers en politiemedewerkers in de basisteams.

Het doel van dit onderzoek is om inzicht te krijgen in de slachtofferimpact en behoefte(voorziening) na slachtofferschap volgens burgers en politiemedewerkers in de basisteams van cybercriminaliteit en traditionele criminaliteit. Vervolgens zullen deze inzichten met elkaar worden vergeleken. Dit betekent de vergelijking van cyber- en traditionele criminaliteit, maar ook de vergelijking van burgers en politiemedewerkers in de basisteams ten opzichte van deze criminaliteitsvormen. Daarmee onderscheidt dit onderzoek zich van eerder onderzoek.

De burgers die deelnemen aan dit onderzoek komen uit het burgerpanel Leeuwarden (Friesland, gemeente Leeuwarden) en de politiemedewerkers uit de basisteams komen uit de politiedistricten uit Noord-Nederland (Friesland, Groningen en Drenthe).

Dit leidt tot de volgende centrale onderzoeksvraag:

Wat is volgens de basisteams van de politie en burgers uit Noord-Nederland de slachtofferimpact en de behoefte(voorziening) na slachtofferschap van cybercriminaliteit in vergelijking met traditionele criminaliteit?

Om deze onderzoeksvraag te beantwoorden zijn de volgende theoretische- en empirische deelvragen opgesteld.

Theoretische deelvragen:

1. Wat wordt er in de literatuur verstaan onder de begrippen cybercriminaliteit en traditionele criminaliteit?
2. Welke delicten vallen volgens de literatuur onder cybercriminaliteit en traditionele criminaliteit en waarin verschillen deze vormen van elkaar?
3. Wat is er in de literatuur bekend over de impactvormen van cybercriminaliteit en traditionele criminaliteit en waarin verschillen deze vormen van elkaar?
4. Wat is er in de literatuur bekend over de behoeften na slachtofferschap van cybercriminaliteit en traditionele criminaliteit?
5. Wat is er in de literatuur bekend over de behoeftevoorziening na slachtofferschap van cybercriminaliteit en traditionele criminaliteit?

De antwoorden op de theoretische deelvragen zullen de basis vormen voor de antwoorden op de empirische deelvragen. Hieronder volgen de empirische deelvragen:

Empirische deelvragen:

1. Wat is volgens de burgers de slachtofferimpact van cybercriminaliteit en traditionele criminaliteit?
2. Wat zijn volgens de burgers de behoeften na slachtofferschap van cybercriminaliteit en traditionele criminaliteit?
3. Wat is volgens de basisteams van de politie de slachtofferimpact van cybercriminaliteit en traditionele criminaliteit?
4. In hoeverre kan de politie volgens de politiemedewerkers in de behoeften van slachtoffers voorzien?
5. Bestaan er verschillen in percepties tussen de basisteams van de politie en de burgers?

Deelvraag 5 wordt beantwoord aan de hand van de antwoorden op deelvraag 1 tot en met 4.

1.3 Relevantie

Wetenschappelijke relevantie

Er bestaan wetenschappelijke studies die iets zeggen over de slachtofferimpact van traditionele criminaliteit (Button et al., 2012; Campbell, 2008; Lamet & Wittebrood, 2009; Shapland & Hall, 2007; Ten Boom & Kuijpers, 2008). Ook bestaan er wetenschappelijke studies die iets zeggen over de slachtofferimpact van cybercriminaliteit (Borwell e.a., 2021; Button e. a., 2020; Kerr e. a., 2013, pp. 36-44; Leukfeldt e.a., 2018). In wetenschappelijke studies is nog nauwelijks onderzoek gedaan naar de vergelijking van de slachtofferimpact tussen cyber- en traditionele criminaliteit, zoals Borwell onderzoekt. Daarnaast is er nog geen onderzoek gedaan naar de vergelijking van de slachtofferimpact tussen cyber- en traditionele criminaliteit, waarbij er wordt gekeken naar het perspectief van burgers en politiemedewerkers. Dit onderzoek loopt daarmee voorop in de kennisontwikkeling naar de vergelijking van de slachtofferimpact tussen cyber- en traditionele criminaliteit en daarbij de vergelijking van burgers en politiemedewerkers.

Maatschappelijke relevantie

De Nederlandse overheid wil cybercriminaliteit onder andere bestrijden door meer onderzoek te doen naar het fenomeen (Rijksoverheid, 2020). Ondanks het plan om meer maatregelen te nemen voor de bestrijding van cybercriminaliteit zijn er nog steeds maatschappelijke vraagstukken over cybercriminaliteit. Eén van deze vraagstukken is om meer onderzoek te doen naar cybercriminaliteit in tijden van de coronapandemie (Ministerie van Justitie en

Veiligheid, 2020). In de aanleiding van dit hoofdstuk is de maatschappelijk relevantie al enigszins toegelicht met betrekking tot het meenemen van de perspectieven van burgers en politiemedewerkers in de basisteams. Daarop voortbordurend is het maatschappelijk relevant om deze perspectieven van burgers en politiemedewerkers niet alleen inzichtelijk te maken, maar ook met elkaar te vergelijken. Deze vergelijking kan iets zeggen over mogelijke verschillen die er bestaan tussen burgers en politiemedewerkers. Deze verschillen kunnen weer iets zeggen over de maatregelen die getroffen moeten worden door de Nederlandse overheid, dan wel de Nederlandse politie.

1.4 Leeswijzer

Het onderzoek bestaat uit vijf hoofdstukken. Het eerste inleidende hoofdstuk is zojuist behandeld. In het eerstvolgende hoofdstuk zal het theoretisch kader worden uiteengezet. Hierna volgt de methodologie in hoofdstuk drie. In hoofdstuk vier worden de onderzoeksresultaten gepresenteerd, gevolgd door de conclusie en discussie in hoofdstuk vijf.

Hoofdstuk 2. Theoretisch kader

Dit hoofdstuk bestaat uit zes paragrafen. In paragraaf 2.1 worden de begrippen cybercriminaliteit en traditionele criminaliteit nader beschouwd. In paragraaf 2.2 worden de delictsvormen van cyber- en traditionele criminaliteit beschreven. In paragraaf 2.3 worden de impactvormen beschreven van slachtofferschap. In paragraaf 2.4 en in paragraaf 2.5 is de behoeften en behoeftevoorziening na slachtofferschap toegelicht en het hoofdstuk sluit af in paragraaf 2.6 met een samenvattend theoretisch model.

2.1 (Cyber)criminaliteit nader beschouwd

Cybercriminaliteit kent meerdere definities. De meeste gebruikte term in de literatuur is de Engelse/Amerikaanse variant; *cybercrime*. Daarnaast wordt ook wel eens de term computercriminaliteit gebruikt in de Nederlandse wetgeving, zoals de Wet Computercriminaliteit. In veelal Nederlandse literatuur en master thesissen wordt de term cybercriminaliteit gehanteerd (van der Bruggen, 2015). De Nationale politie bevestigt dat deze termen dezelfde definitie hebben en definieert cybercriminaliteit als volgt:

> *"Misdaad gepleegd met ICT, gericht op ICT. Het strafbare feit wordt gepleegd met een computer, smartphone, smartwatch of tablet, kortom alles waar een processor in zit. Cybercrime voorbeelden zijn hacking, DDoS-aanvallen, ransomware, virussen, malware, enzovoort"*[1]

Verder wordt ook de term 'online criminaliteit' gebruikt in de literatuur. Online criminaliteit is weer te onderscheiden in cybercriminaliteit en gedigitaliseerde criminaliteit (Leukfeldt et al., 2018). Onder cybercriminaliteit vallen delicten waarbij de ICT-structuur het doelwit is en waarbij ICT een rol speelt in de uitvoering, zoals hacking en DDos-aanvallen. Onder gedigitaliseerde criminaliteit vallen delicten waarbij ICT-structuur geen doelwit is maar waar ICT wel een rol speelt in de uitvoering, zoals fraude en stalking (Leukfeldt & Weulen Kranenbarg, 2017, p. 282). Deze definities worden in literatuur ook nog uitgewerkt tot andere termen (zie tabel 1).

Tabel 1. *Termen voor cybercriminaliteit en gedigitaliseerde criminaliteit*

Cybercriminaliteit	Gedigitaliseerde criminaliteit	Bron
Cybercriminaliteit in 'enge zin'	Cybercriminaliteit in 'brede zin'	(Van Erp et al., 2013, p. 328).
Cyber dependent crimes	Cyber enabled crimes	(Furnell et al., 2015)

[1]https://www.politie.nl/themas/cybercrime.html#:~:text=Hierbij%20gaat%20het%20om%20misdaad,%2C%20virussen%2C%20malware%2C%20enzovoort.

High-tech crimes	-	EuroPol[2]
Computer focused crimes	Computer-assisted crimes	(Furnell, 2002)

De definitie van de politie lijkt hiermee te vallen onder cybercriminaliteit en minder op de gedigitaliseerde criminaliteit (zie tabel 1). Traditionele criminaliteit laat zich in de literatuur niet makkelijk definiëren. In de tijd dat er nog geen ICT werd gebruikt in de criminaliteit waren er niet zoveel onderscheidingen te maken als tegenwoordig. De term criminaliteit is door de opkomst van andere soorten criminaliteit zoals cybercriminaliteit steeds meer veranderd naar termen als traditionele criminaliteit, klassieke criminaliteit of offline criminaliteit. Ook het CBS gebruikt voor dit soort delicten de term traditionele criminaliteit.[3]

In dit onderzoek wordt de term cybercriminaliteit gehanteerd, zoals in veelal Nederlandse literatuur (van der Bruggen, 2015). Onder deze term worden criminaliteitsdelicten verstaan waar zowel ICT-structuren een doelwit als geen doelwit zijn. De term traditionele criminaliteit wordt in dit onderzoek gehanteerd als het gaat over criminaliteitsdelicten zonder behulp van ICT-middelen. Deze delictsvormen worden in paragraaf 2.2 verder toegelicht.

2.2 Afbakening delictsvormen van cyber- en traditionele criminaliteit

In de vorige paragraaf werd de definitie gegeven van cyber- en traditionele criminaliteit. In dit onderzoek is ervoor gekozen om niet alle delicten van cyber- en traditionele criminaliteit toe te lichten, maar het te beperken tot de vier cybercriminaliteitsdelicten en vier traditionele criminaliteitsdelicten die Borwell meeneemt in haar onderzoek (zie tabel 2).

Tabel 2. *De vergelijking van delict typen*

	Cybercriminaliteitsdelict		Traditioneel criminaliteitsdelict
1	Bankhelpdeskfraude	Versus	Babbeltruc aan de deur
2	Hacken van online bankaccount	Versus	Woninginbraak
3	Beeld gerelateerd seksueel misbruik	Versus	Aanranding
4	Online bedreiging	Versus	Offline bedreiging

De paragraaf is daarbij onderverdeeld in vier sub-paragrafen. In sub-paragraaf 2.2.1 worden de delictsvormen van cybercriminaliteit toegelicht. In sub-paragraaf 2.2.2 worden de delictsvormen van traditionele criminaliteit toegelicht. Vervolgens wordt in sub-paragraaf 2.2.3

[2] Deze definitie wordt vooral gehanteerd door EuroPol – de https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/high-tech-crime
[3] https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime

de verantwoording en de vergelijking voor deze cyber- en traditionele delicten toegelicht. De paragraaf zal afsluiten met een deelconclusie in sub-paragraaf 2.2.4.

2.2.1 Delictsvormen (en slachtofferschap) cybercriminaliteit

De bankhelpdeskfraude is een vorm van online oplichting, waarbij de oplichter zich voordoet als een bankmedewerker. De oplichter belt naar zijn potentiële slachtoffer met een vals nummer. De oplichter gebruikt hierbij een truc om het originele nummer van de bank in het beeldscherm van het potentiële slachtoffer te tonen. Vervolgens zal de oplichter tijdens het telefoongesprek vertellen dat er verdachte transacties te zien zijn op de rekening van het potentiële slachtoffer en zal adviseren en mogelijk aandringen om het geld op de rekening te verplaatsen naar een zogenaamde 'veilige rekening'. In werkelijkheid is deze veilige rekening vaak de rekening van de oplichter. Volgens de politie komen vooral mensen boven de 50 in aanraking met dit delict (Politie, z.d.-b). Het exacte aantal slachtoffers van de bankhelpdeskfraude is niet bekend. Het is wel bekend dat de banken ABN AMRO, ING, Rabobank en de Volksbank in de periode 2018-2020 voor bijna 5,3 miljoen euro aan meldingen van de helpdeskfraude hebben ontvangen (NU.nl, 2020) Het ging hier om zo'n 4.831 meldingen, echter zitten hier ook meldingen tussen over andere *Tech Support Scams,* zoals de nephelpdesk van IT- of softwarebedrijven (Ministerie van Justitie en Veiligheid, 2021).

Het hacken van een online bankaccount wordt vaak gedaan door middel van *phishing*. Phishing is een 'schaalbare vorm van misleiding waarbij nabootsing wordt gebruikt om informatie van een doelwit te verkrijgen' (Lastdrager, 2014). De politie in Nederland lijkt de term *phishing* op de website abstracter op te vatten dan de politie in België. De politie in België maakt onderscheid in *phishing* (via e-mail*), smishing* (via sms) en *vishing* (via telefonische oproep) (Federale Politie, 2018). Bij al deze methodes wil de oplichter door misleiding informatie krijgen van het doelwit. Bij het hacken van een bankaccount stuurt de oplichter door middel van *smishing*, een sms namens de bank over bijvoorbeeld achterstallige betalingen. In het bericht zit vaak een link die het potentiële slachtoffer doorverwijst naar een valse website om de achterstallige betaling te verrichten. Deze valse website is vaak identiek aan de originele website van de bank. Als het potentiële slachtoffer zijn inloggegevens invult op deze valse website en probeert in te loggen, is het hacken van de bankaccount een feit. Vervolgens zal de oplichter razendsnel het geld van de rekening van het slachtoffer halen (Veiligbankieren, 2021). Het CBS houdt slachtofferpercentages bij over algemene termen, zoals identiteitsfraude (waaronder *phishing*) en hacken (CBS, 2020a). Het is niet bekend wat het exacte slachtofferpercentage is van het hacken van een bankaccount. Uit de statistieken van het CBS blijkt verder dat vooral de 'middelleeftijden' (tussen 25 – 65 jaar) slachtoffer zijn van identiteitsfraude en hacken (CBS, 2020c).

Beeld gerelateerd seksueel misbruik (*image-based sexual abuse)* is een nieuwe manifestatie van dergelijk online geweld. Het delict houdt in het maken of verspreiden van seksuele privébeelden zonder toestemming van de partij voor seksuele of niet-seksuele doeleinden (McGlynn & Rackley, 2017). Vrouwen zijn vaak het slachtoffer en mannen zijn vaak de dader van het delict (idem, pp. 537 – 538). Dit delict gaat over het schenden van persoonlijke en lichamelijke integriteit van het slachtoffer (idem, p. 545). De motieven van dit delict kunnen verschillen; wraak en ontladen van spanning zijn veel voorkomend (Naezer, 2019).

Online bedreigingen zijn sinds de komst van online sociale netwerken (OSN), zoals Facebook en LinkedIn, alleen maar toegenomen (Fire et al., 2014,). In dit onderzoek wordt een online bedreiging gezien als een *interpersonal threats* – bedreigingen uitgedrukt door een persoon naar een andere persoon (Spitzberg & Gawron, 2016, p. 50). Bij het CBS valt deze typering van online bedreiging onder het 'bedreigen met geweld'. Volgens het CBS was het slachtofferpercentage van bedreigingen met online geweld 0,6 procent in zowel 2012 als in 2019 (CBS, 2020a).

2.2.2 Delictsvormen (en slachtofferschap) van traditionele criminaliteit

De babbeltruc aan de deur is een truc van (offline) oplichterij, waarbij de oplichter(s) vaak via een smoes het huis van het potentiële slachtoffer wil betreden. De oplichter(s) doen zich bij deze babbeltruc veelal voor als nepmedewerkers van een organisatie, bijvoorbeeld een thuiszorgmedewerker. Als de oplichters (vaak meerdere personen) binnen zijn getreden leidt de ene oplichter het slachtoffer vaak af, zodat de andere de spullen of geld uit het huis kan halen (Politie, z.d.-a). Uit een onderzoek van KBO-PCOB, een organisatie die zich inzet voor senioren (ouder dan 55), blijkt 1 op de 4 senioren aan te geven dat ze weleens zijn geconfronteerd met de babbeltruc (KBO-PCOB, 2019). Het exacte aantal slachtoffers van de babbeltruc is niet bekend. Het is wel bekend dat vooral senioren vaak geconfronteerd worden met dit delict (CVV, 2021). Dit bevestigt ook een onderzoeksrapport van de politie (Politieacademie, 2014).

Een woninginbraak valt volgens het Ministerie van Veiligheid en Justitie onder de zogenoemde *High Impact Crimes* (HIC). Dit houdt in dat het delict een grote impact heeft op het slachtoffer en de directe omgeving (Opstelten, 2013). Het CBS onderscheidt poging tot inbraak en inbraak. In dit onderzoek wordt alleen de inbraak meegenomen. In 2012 lag het slachtofferpercentage van inbraak op 1,2 procent, in 2019 was dit 0,6 procent (CBS, 2020b). Verder blijkt uit onderzoek dat de leeftijdscategorieën van slachtoffers van een woninginbraak uiteenlopen (Knijf, 2011).

Aanranding wordt binnen de politie gezien als een vorm van seksueel misbruik. Seksueel misbruik betekent dat iemand is gedwongen tot seksuele handelingen. Wanneer het

gaat om het binnendringen van het lichaam wordt dit in de wet benoemd als verkrachting (art. 242 Sr)[4]. De overige gedwongen seksuele handelingen zijn toe te wijzen binnen de wet als aanranding. In de wet staat aanranding beschreven als: '*Hij die door geweld of andere feitelijkheid of bedreiging met geweld of een andere feitelijkheid iemand dwingt tot het plegen of dulden van ontuchtige handelingen, wordt, als schuld aan feitelijke aanranding van de eerbaarheid'* (art. 246 Sr)[5]. Bij het CBS valt de definitie van aanranding onder 'geweld met seksuele bedoeling'. Volgens het CBS was het slachtofferpercentage van geweld met seksuele bedoeling 0,1 procent in zowel 2012 als in 2019. Vooral vrouwen zijn slachtoffer en mannen de dader van het delict (CBS, 2020a). De motieven van de dader bij dit delict kunnen gaan over boosheid en wraak, ervaren van macht of bevrediging van geslachtsdriften (NOS, 2017).

Offline bedreigingen worden in dit onderzoek gezien als mondelinge of schriftelijke bedreigingen. Ook in dit onderzoek worden deze bedreigingen beschouwd als *interpersonal threats* (Spitzberg & Gawron, 2016, p. 50). Volgens het CBS was het slachtofferpercentage van offline bedreigingen 1,6 procent in 2012 en 1,3 procent in 2019 (CBS, 2020a).

2.2.3 Delict vergelijkingen

De vier cyberdelicten (sub-paragraaf 2.2.1) en de vier traditionele delicten (sub-paragraaf 2.2.2) worden in dit onderzoek gekoppeld aan een delict vergelijking, zoals weergegeven in tabel 2. Dit betekent dat een cyberdelict wordt vergeleken met een traditioneel delict. De delict 'paren' die zijn gemaakt worden in deze sub-paragraaf toegelicht.

A. Bankhelpdeskfraude versus babbeltruc aan de deur

De bankhelpdeskfraude en de babbeltruc aan de deur maken gebruik van de zogenoemde *social engineering* technieken. Deze techniek is gericht op de psychologische manipulatie van mensen om iets te doen of te dulden om informatie afhandig te maken. De techniek valt onder de noemer 'oplichting' (Drew en Cross, 2015, p. 192). Daarnaast is het dadermotief bij de delicten financieel gericht. Het zijn vaak ouderen die benaderd en slachtoffer worden van deze delicten (CVV, 2021).

B. Hacken van een online bankaccount versus woninginbraak

Het hacken van een online bankaccount en woninginbraak vallen onder de noemer 'inbraak' (Leukfeldt et al., 2018). Ook bij deze vergelijking is het dadermotief financieel gericht. In

4 Artikel 242 Wetboek van Strafrecht

5 Artikel 246 Wetboek van Strafrecht

tegenstelling tot de bankhelpdeskfraude is de dader bij het hacken van een bankaccount zelf de persoon die het geld overmaakt.

C. Beeld gerelateerd seksueel misbruik versus aanranding

Beeld gerelateerd seksueel misbruik en aanranding gaan over de schending van persoonlijke en lichamelijke integriteit. Daarnaast hebben deze delicten geen financieel motief, maar een motief van wraak (Naezer, 2019; NOS, 2017). Ook zijn bij beide delictsvormen vaak vrouwen de slachtoffers en mannen de daders (CBS, 2020a; McGlynn & Rackley, 2017).

D. Online versus offline bedreiging

Online en offline bedreigingen kunnen interpersoonlijke bedreigingen zijn (Spitzberg & Gawron, 2016, p. 50). Daarnaast is de modus operandi (“handschrift van de crimineel”) bij beide delicten vaak hetzelfde. Het enige verschil is dat offline bedreigingen zich afspelen in een offline wereld en de online bedreigingen in een online wereld.

2.2.4 Deelconclusie

In dit onderzoek worden alleen de delicten meegenomen, zoals ze zijn beschreven in paragraaf 2.2. In sub-paragraaf 2.2.3 zijn de delict vergelijkingen onder bepaalde noemers geplaatst. Deze noemers met de daarbij horende delict vergelijking is weergegeven in tabel 3.

Tabel 3. *De noemers van de traditionele criminaliteitsdelicten en cybercriminaliteitsdelicten*

Traditioneel criminaliteitsdelict:	Cybercriminaliteitsdelict:	Onder de noemer van:
Babbeltruc	Bankhelpdeskfraude	Oplichting
Woninginbraak	Hacken van een online bankaccount	Inbraak
Aanranding	Beeld gerelateerd seksueel misbruik	Schending van lichamelijke integriteit
Offline bedreiging	Online bedreiging	Interpersoonlijke bedreiging

2.3 Impactvormen van slachtofferschap

In deze paragraaf zullen verschillende impactvormen van slachtofferschap van cybercriminaliteit en traditionele criminaliteit worden beschreven. Deze impactvormen zijn te onderscheiden in: financieel/materiaal (sub-paragraaf 2.3.1), psychologisch/emotioneel (sub-paragraaf 2.3.2), fysiek (sub-paragraaf 2.3.3) en gedragsmatig/sociaal (sub-paragraaf 2.3.4). Deze impactvormen zijn geselecteerd, omdat het in wetenschappelijke literatuur over slachtofferschap gebruikelijk is om deze impactvormen te meten als het gaat over slachtofferschap van criminaliteit (Shapland & Hall, 2007; Lamet en Wittebrood, 2009; Kerr et

al., 2013; Jansen & Leukfeldt, 2017; Button et al., 2020; Leukfeldt et al., 2018; Borwell et al., 2021). Deze paragraaf zal eindigen met een deelconclusie en hypothese (sub-paragraaf 2.3.5).

2.3.1 Financiële/materiële impact

De financiële gevolgen van slachtofferschap worden vaak uitgedrukt in termen van directe en indirecte kosten (Jansen & Leukfeldt, 2017; Lamet en Wittebrood, 2009; Miller et al., 1996). Directe kosten hebben betrekking op de waarde van beschadigde of gestolen eigendommen. Ook medische kosten kunnen vallen onder directe kosten (Lamet en Wittebrood, 2009, p. 13). Deze directe kosten zijn bij de delicten over inbraak en oplichting sneller aan te wijzen dan bij delicten over schending van lichamelijke integriteit en interpersoonlijke bedreiging. De delicten kunnen daarentegen wel te maken hebben met indirecte kosten. Deze indirecte kosten kunnen bij alle delicten uit tabel 3 bestaan uit medische kosten en/of inkomensderving (Lamet & Wittebrood, 2009; Shapland & Hall, 2007; Cohen, 1988). Deze medische kosten worden gemaakt als het slachtoffer ten gevolge van het delict bijvoorbeeld psychische klachten krijgt en de dokter moet bezoeken. De inkomensderving gaat over de situatie waar het slachtoffer ten gevolge van het delict bijvoorbeeld door psychische klachten niet of tijdelijk niet kan werken.

Uit onderzoek blijkt dat de financiële impact afhankelijk is van de financiële situatie van het slachtoffer (Leukfeldt et al., 2018, p. 12). Ook blijkt dat het effect van geldverlies versterkt wordt als de kans klein is dat het slachtoffer het financiële verlies terugkrijgt (Kerr et al., 2013, p. 36). Er is nog geen wetenschappelijk onderzoek gedaan naar de vergelijking van de financiële impact van slachtofferschap tussen cybercriminaliteit en traditionele criminaliteit.
Er is wel onderzoek gedaan naar cybercriminaliteit die de financiële impact en de emotionele impact (zie ook paragraaf 2.3.2) met elkaar vergelijkt (Kerr. et al., 2013; Modic & Anderson, 2015). Een onderzoek over internet fraude laat zien dat respondenten de emotionele impact ernstiger beschouwen dan de financiële impact (Modic & Anderson, 2015, p. 102). Ander onderzoek naar online fraude beweert juist dat de financiële impact het meest significant is (Kerr et al., 2013, p. 36).

Op basis van de literatuur in deze deelparagraaf kan geen conclusie worden getrokken of de financiële impact op slachtoffers groter zal zijn voor cybercriminaliteit of voor traditionele criminaliteit. Ook laten de twee onderzoeken naar financiële en emotionele impact zien dat er verschillende uitkomsten zijn qua significantie (Kerr. et al., 2013; Modic & Anderson, 2015). Deze emotionele impact wordt in de volgende deelparagraaf verder toegelicht.

2.3.2 Psychologische en emotionele impact

De psychologische en emotionele impact van slachtofferschap kan worden onderscheiden in korte termijn impact en lange termijn impact (Jansen & Leukfeldt, 2017). Op korte termijn kunnen slachtoffers bijvoorbeeld leiden aan een shock en verlies van vertrouwen in de samenleving. Bij traditionele criminaliteitsdelicten kan dit bijvoorbeeld gaan over vertrouwen in de lokale gemeenschap of in relatie tot een sociale groep of plaats waar het misdrijf is gepleegd (Shapland & Hall, 2007). Bij cybercriminaliteitsdelicten kan dit bijvoorbeeld gaan over vertrouwen in bepaalde instanties waar ze onderdeel van zijn en het vertrouwen in andere mensen (Kerr et al., 2013). Een slachtoffer kan zijn vertrouwen in de bank bijvoorbeeld verliezen bij de bankhelpdeskfraude of het hacken van online een bankaccount. De shock heeft meestal een korttermijneffect (dagen of weken), terwijl het verlies van vertrouwen jaren kan duren. Daarnaast zijn er ook andere psychologische effecten zoals angst, boosheid en depressie. Boosheid komt vooral op korte termijn voor en angst en depressie kunnen langer duren (Shapland & Hall, 2007).

De emotionele en psychologische gevolgen van slachtofferschap kunnen zich ook uiten in schaamte, verdriet, stress, eenzaamheid, woede en gevoel van onveiligheid (Cross et al., 2016). Uit een rapport van slachtoffers van computermisbruik in het Verenigd Koningrijk blijkt dat de meeste slachtoffers van computermisbruik voornamelijk last hebben van stress (75 procent). Daarna volgen ongerustheid (70 procent), angst (52 procent), verlegenheid/schaamte/zelfbeschuldiging (51 procent), woede (48 procent) en isolatie (43 procent) (Button et al., 2020, p. 9). In sommige gevallen kunnen deze emotionele reacties leiden tot een posttraumatisch stressstoornis (PTSS) (Lamet & Wittebrood, 2009, p. 13).

Er bestaan studies die de psychologische effecten (zoals depressie) van traditionele- en cyberslachtofferschap vergelijken. Deze studies gaan vooral over de vergelijking van traditioneel- en cyberpesten onder jongeren. Uit deze studies blijkt cyberslachtofferschap een sterkere associatie te hebben met depressieve symptomen, meer dan bij traditioneel slachtofferschap (Price et al., 2013; Bonanno & Hymel, 2013: Perren et al., 2010). Op basis van deze bevinding naar depressie symptomen zou kunnen worden gesteld dat de psychologische en emotionele impact van slachtofferschap groter lijkt bij cybercriminaliteit dan bij traditionele criminaliteit. Hierbij moet wel rekening worden gehouden dat niet elke vorm van pesten te maken heeft met criminaliteit.

2.3.3 Fysieke impact

De fysieke impact van slachtofferschap is bij cybercriminaliteit anders dan bij traditionele criminaliteit. Bij cybercriminaliteit bestaat er een fysieke afstand tussen het slachtoffer en dader. De directe fysieke impact van een cybercriminaliteit is hierdoor minder waarschijnlijk

dan bij traditionele criminaliteit (Kerr et al., 2013). De indirecte fysieke impact kan daarentegen wel voorkomen bij cybercriminaliteit, zoals huidproblemen, slaapgebrek, hoofdpijn en gewichtsverlies. Dit wordt in de literatuur doorgaans gezien als de psychologische impact van criminaliteit, omdat het een gevolg is van slachtofferervaring (Dinisman & Moroz, 2017; Kerr et al., 2013; Lamet & Wittebrood, 2009). De fysieke en psychologische/emotionele gevolgen zijn daardoor ook vaak met elkaar verweven (Shapland & Hall, 2007). In het rapport van Button et al. (2020) blijkt dat slachtoffers van computermisbruik voornamelijk last hebben van slaapproblemen (53 procent), paniek- of angst gerelateerde ziekte (45 procent), depressie (43 procent), stress-gerelateerde ziekte (42 procent) en veranderingen in eetlust, gewichtsverlies en gewichtstoename (38 procent) (2020, p. 9).

De fysieke impact van slachtofferschap bij traditionele criminaliteitsdelicten kunnen gaan over lichamelijk letsel dat direct in verband staat aan het misdrijf zelf, zoals bij een mishandeling. Daarnaast kunnen slachtofferervaringen ook leiden tot gezondheidsproblemen (Lamet & Wittebrood, 2009, p. 13). Een studie naar de effecten van traditionele criminaliteit op de mentale gezondheid van studenten in het Verenigd Koningrijk laat de volgende statistieken zien: slaapproblemen (32,2 procent), angst of gestrest voelen (62,1 procent), depressie (14,4 procent), paniekaanvallen (13,8 procent), gebrek aan vertrouwen (35,3 procent) (Morrall et al., 2010, pp. 825-826).

De vergelijkingen die gemaakt kunnen worden tussen de onderzoeken van Button et al. (2020) en Morrall et al. (2010) zijn de indirecte fysieke klachten over slaapproblemen, depressie en paniekaanvallen. Hieruit blijkt dat de indirecte fysieke impact onder slachtoffers groter is bij cybercriminaliteit dan bij traditionele criminaliteit.

2.3.4 Gedragsmatig/sociaal impact

De gedragsmatige en sociale impact van slachtofferschap kan verweven zijn met de psychologische en emotionele impact van slachtofferschap. Uit onderzoek blijkt dat online fraude een aanzienlijke impact heeft op de persoonlijke relaties van een slachtoffer (Kerr et al., 2013). Door een gevoel van schaamte of zelfbeschuldiging te ervaren kan het slachtoffer zich sociaal gaan isoleren (Kerr et al., 2013, p. 40). Bijvoorbeeld als het slachtoffer niet op zijn werk durft te vertellen dat hij slachtoffer is geworden van online fraude, omdat hij bang is voor de percepties van zijn collega's. Wanneer ook geld een rol speelt in dit voorbeeld is de financiële impact van slachtofferschap hier ook in verweven. Ook kan de gedragsmatige en sociale impact van slachtofferschap verweven zijn met de fysieke impact van slachtofferschap. Bijvoorbeeld als het slachtoffer door lichamelijk letsel minder sociale activiteiten kan of wil ondernemen. Verder blijkt uit onderzoek dat ook de plek waar het misdrijf heeft plaatsgevonden of de context waarin het misdrijf plaatsvond wordt vermeden (Shapland &

Hall, 2007). Daarnaast kunnen ook werkeloosheid, verhuizing en scheidingen het gevolg zijn van levensstijlaanpassingen (Lamet & Wittebrood, 2009, p. 13; Shapland & Hall, 2007, p. 178).

2.3.5 Deelconclusie en hypothese 1

De vergelijkingen van de impactvormen van cybercriminaliteit en traditionele criminaliteit zijn niet altijd één op één te verhouden, zoals de onwaarschijnlijke directe fysieke impact bij cybercriminaliteit (Kerr et al., 2013). Daarnaast lijkt er in de literatuur ook weinig onderzoek te zijn gedaan naar de impactvormen op de delicten die worden meegenomen in dit onderzoek. Om die reden is er gekeken naar andere delicten, zoals naar cyber- en traditioneel pesten (zie paragraaf 2.3.2). Op basis van de informatie in deze paragraaf over de psychologische/emotionele en indirecte fysieke impact lijkt de impact bij cybercriminaliteit groter dan bij traditionele criminaliteit. Dit heeft geleid tot de volgende hypothese die getoetst zal worden in dit onderzoek:

Hypothese 1: *De slachtofferimpact van cybercriminaliteit wordt hoger gepercipieerd dan de slachtofferimpact van traditionele criminaliteit.*

2.4 Behoeften na slachtofferschap

Volgens Leukfeldt et al. (2018) hangt de slachtofferbehoeften sterk samen met de impact die het delict heeft gehad op het slachtoffer (2018, p. 40). Uit de studie van Ten Boom en Kuijpers (2008) blijkt dat de behoeften voortkomen uit de ervaren gevolgen van een delict (2018, p. 17). In sub-paragraaf 2.4.1 zal de behoefte na slachtofferschap worden beschreven in relatie tot cybercriminaliteit en in sub-paragraaf 2.4.2 in relatie tot traditionele criminaliteit. Deze paragraaf zal eindigen met een deelconclusie en hypothese (sub-paragraaf 2.4.3).

2.4.1 Cybercriminaliteit

Volgens Leukfeldt et al. (2018) is er weinig empirisch onderzoek verricht naar de behoeften van slachtofferschap van cybercriminaliteit (2018, p. 86). In het onderzoek van Leukfeldt et al. (2018) is er een top drie slachtofferbehoeften opgesteld van online delicten. De eerste behoefte is het stoppen van slachtofferschap, zoals het langdurig contact tussen slachtoffer en dader bij fraudedelicten (2018, p. 88). De tweede behoefte is het straf- en vergeldingsproces, zoals informatievoorziening over de voortgang van het strafproces en dat de dader wordt gestraft (2018, pp. 90-95). De derde behoefte is het helpen van anderen. Dit houdt in dat ze vooral willen voorkomen dat anderen slachtoffer worden van het delict (2018, p. 90).

Onderzoek naar identiteitsfraude binnen cybercriminaliteit toont dat slachtoffers met name behoefte hebben aan herstel na afloop van het delict (Van der Meulen et al., 2012) en aangifte/melding willen doen (Harrell en Langton, 2013). Een onderzoek naar interpersoonlijke delicten laat zien dat slachtoffers liever het contact met de dader willen vermijden. De slachtoffers hebben de behoeften dat de politie de dader aanhoudt (Cassidy, et al., 2013; Slonje e.a. 2012; Worsley e.a., 2017).

Cross et al. (2016) hebben onderzoek gedaan naar de behoefte van slachtoffers van online fraude. Uit het onderzoek blijkt dat het besluit om aangifte te doen door slachtoffers voortkomt uit de behoefte aan vergelding of de wens dat er een onderzoek wordt gestart om de dader te straffen. Daarnaast blijkt uit dit onderzoek dat ook slachtoffers behoeften hebben aan een eenduidig antwoord op hun verzoek om hulp (2016 p. 11).

2.4.2 Traditionele criminaliteit

Ten Boom en Kuijpers (2008) hebben een studie verricht naar de behoeften van slachtoffers van traditionele criminaliteit. Zij hebben op basis van 33 kernpublicaties over slachtofferbehoeften een aantal clusters opgesteld. Dit zijn de zes clusters: emotioneel, stafproces in ruime zin, informatie, praktisch, financieel en primair (2008, p. 10). Deze clusters komen grotendeels overeen met eerdere onderzoeken naar slachtofferbehoeften (Maguire, 1991; Wemmers 2006). Volgens Leukfeldt et al. (2018) is het aannemelijk dat behoefte van slachtoffers niet drastisch is veranderd op basis van andere studies na 2008 (2018, p. 35). In het onderzoek van Leukfeldt et al. (2018) is ook de traditionele slachtofferbehoefte meegenomen. Uit de interviews met respondenten blijkt dat de behoeften van beide soorten criminaliteit grotendeels overeenkomen (p.118).

2.4.3 Deelconclusie en hypothese 2

De behoeften na slachtofferschap van cyber- en traditionele criminaliteit is in het onderzoek van Leukfeldt et al. (2018) wel meegenomen, maar niet tegen elkaar afgezet. Hierdoor blijft het onduidelijk of de behoefte na slachtofferschap groter is voor cybercriminaliteit of traditionele criminaliteit. Echter concluderen Leukfeldt et al. (2018) aan het eind van het onderzoek dat de behoeften bij cybercriminaliteit groter kan zijn dan die bij traditionele criminaliteit (2020, p. 122). Op basis van deze uitspraak is de tweede hypothese opgesteld die getoetst zal worden in dit onderzoek:

Hypothese 2: *Volgens burgers zijn de behoeften na slachtofferschap groter bij cybercriminaliteit dan bij traditionele criminaliteit.*

2.5 Behoeftevoorziening na slachtofferschap

In deze paragraaf wordt de behoeftevoorziening na slachtofferschap beschreven. In sub-paragraaf 2.5.1 zal de behoeftevoorziening na slachtofferschap worden beschreven in relatie tot cybercriminaliteit en in sub-paragraaf 2.5.2 in relatie met traditionele criminaliteit. Deze paragraaf zal eindigen met een deelconclusie en hypothese (sub-paragraaf 2.5.3).

2.5.1 Cybercriminaliteit

Uit het onderzoek van Cross et al. (2016) blijkt dat slachtoffers van cybercriminaliteit veelal teleurgesteld zijn door het gebrek aan actie van politie en justitie over het gebrek informatievoorziening van politie/justitie als er wel tot opsporing is overgegaan. Dit zou resulteren in een groot gevoel van onrechtvaardigheid bij slachtoffers. Daarnaast blijkt ook dat slachtoffers van het kastje naar de muur worden verwezen door bijvoorbeeld de politie, dat leidt tot een toename van stress. Slachtoffers hebben de wens om vooral duidelijke informatie te ontvangen over wat ze kunnen verwachten van politie en justitie.

Uit het onderzoek van Leukfeldt et al. (2018) blijkt ook dat slachtoffers de politie vaak als eerste aanspreekpunt zien, afhankelijk van het type delict. Een aantal slachtoffers in dit onderzoek geeft aan dat ze worden weggestuurd en daardoor geen aangifte kunnen doen. Ook hebben slachtoffers het gevoel dat ze niet serieus worden genomen door politiemedewerkers (2018, p. 94). Verder blijkt ook uit onderzoek dat mensen het bij cybercriminaliteit minder waarschijnlijk achten dat de politie een dader zal opsporen dan bij traditionele criminaliteit (Graham et al., 2019).

2.5.2 Traditionele criminaliteit

In de studie van Ten Boom en Kuijpers (2008) is ook gekeken naar de behoeftevoorziening na slachtofferschap. Bij de zes clusters (emotioneel, stafproces in ruime zin, informatie, praktisch, financieel en primair) is ook gekeken welke partijen, personen of instanties slachtoffers zien als verantwoordelijke partij voor het bevredigen van hun behoeften. De partijen die zij meenemen zijn: de politie, politie en justitie, slachtoffer, de dader of overige personen/instanties (2008, p. 10).

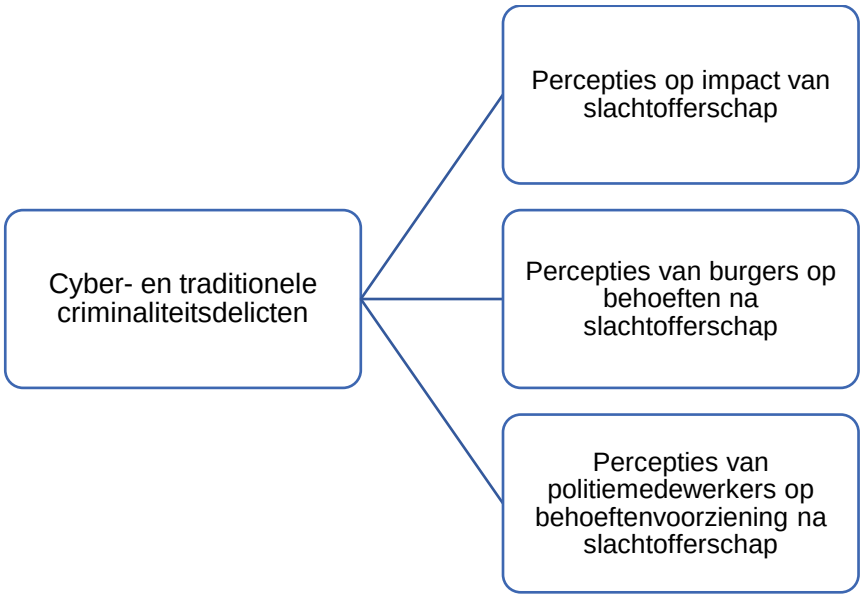
2.5.3 Deelconclusie en hypothese 3

Volgens de respondenten uit het onderzoek van Leukfeldt et al. (2018) hebben politiemedewerkers onvoldoende kennis van online delicten en worden deze in tegenstelling tot offline delicten vaak als complex gezien. Hierdoor worden mensen vaker in de behoefte voorzien bij traditionele criminaliteit dan bij cybercriminaliteit (pp. 118-120). Dit leidt tot de volgende derde hypothese die getoetst zal worden in dit onderzoek:

***Hypothese 3**: Volgens politiemedewerkers zijn de behoeftevoorzieningen na slachtofferschap groter bij traditionele criminaliteit dan bij cybercriminaliteit.*

2.6 Conclusie theoretisch kader

Kort samengevat, in dit onderzoek wordt onderscheidt gemaakt tussen cybercriminaliteitsdelicten en traditionele criminaliteitsdelicten (zie paragraaf 2.1 en 2.2) Deze delicten worden gebruikt om de percepties op impactvormen van slachtofferschap (zie paragraaf 2.3), percepties op behoeften na slachtofferschap (zie paragraaf 2.4) en percepties op behoeftevoorziening na slachtofferschap (zie paragraaf 2.5) te onderzoeken. Dit leidt tot het volgende overzicht:



Figuur 1. *Overzicht theoretisch kader*

Hoofdstuk 3. Methodologie

In dit hoofdstuk wordt de onderzoeksmethodologie van deze thesis uiteengezet. Dit hoofdstuk is opgedeeld in zeven paragrafen. In paragraaf 3.1 wordt de aard van het onderzoek toegelicht. Vervolgens wordt in paragraaf 3.2 ingegaan op de onderzoekspopulatie. In paragraaf 3.3 wordt de manier van dataverzameling toegelicht, waarna in paragraaf 3.4 de manier van dataverwerking volgt. In paragraaf 3.5 wordt de betrouwbaarheid en validiteit beschreven, waarna de ethische uitdagingen in paragraaf 3.6 volgen. Het hoofdstuk sluit af met een conclusie in paragraaf 3.7.

3.1 Aard van het onderzoek

Het vergelijkend onderzoek is grotendeels exploratief van aard. Een exploratief onderzoek houdt in dat er een verkennend onderzoek wordt gedaan naar een onderwerp of probleem waar geen of zeer weinig kennis over beschikbaar is (Van Thiel, p. 27). Een verkennend onderzoek naar perspectieven van burgers en politiemedewerkers in de basisteams ten aanzien van de slachtofferimpact en behoefte(voorziening) na slachtofferschap. Het onderzoek is vergelijkend, omdat de vergelijking wordt gemaakt tussen cybercriminaliteit en traditionele criminaliteit. Daarnaast wordt ook de vergelijking gemaakt tussen meerdere groepen, namelijk de burgers en politiemedewerkers in de basisteams. Het vergelijkend onderzoek heeft ook een toetsende aard, omdat er vooraf verwachtingen (hypothesen) zijn geformuleerd die zijn opgesteld op basis van bestaande theorieën, dan wel informatie (ibid.). Het toetsende gedeelte bestaat uit drie hypothesen die niet de gehele onderzoeksvraag dekken, omdat er nog veel kennis ontbreekt in de bestaande theorieën. Om die reden heeft het onderzoek een combinatie van een exploratieve en toetsende aard.

Het onderzoek gebruikt een kwantitatieve onderzoeksmethode met een empirisch-analytische wetenschapsopvatting. Dit betekent dat kennis op een objectieve manier wordt verkregen, door empirische waarneming en systematisch onderzoek (2020, pp. 42-45). Deze kennis wordt verkregen door middel van een vragenlijst met daarbij een vignetmethode. De vignetmethode voegt een korte beschrijving of casus toe aan de gebruikelijke vragenlijst, van een persoon of situatie die relevant geachte informatie bevat (Veenma, 2004, p. 4). De vignetmethode is toegepast in dit onderzoek, omdat deze methode het mogelijk maakt om opvattingen te analyseren van respondenten die niet of nauwelijks bekend zijn met slachtofferschap van criminaliteitsdelicten. Ook wordt de informatie van respondenten relevanter geacht, wanneer zij allemaal dezelfde beschrijving of casus van een persoon of situatie voorgelegd krijgen (empirisch-analytisch).

3.2 Onderzoekspopulatie

3.2.1 Selectie van respondenten

De onderzoekspopulatie is gekozen door middel van een doelgerichte selecte steekproef. Dit houdt in dat er een selectie is gemaakt van de steekproef op bepaalde kenmerken. Het doel richt zich om informatie te halen dáár waar deze zit (Verhoeven, 2014, p. 191). Voor dit onderzoek betekent dat er doelgericht selectief is gekozen voor burgers en politiemedewerkers uit politiedistricten in Noord-Nederland. In hoofdstuk 1 (zie paragraaf 1.1) is de aanleiding om deze twee groepen mee te nemen al grotendeels toegelicht. Het burgerpanel in Leeuwarden en de politiedistricten in Noord-Nederland zijn uiteindelijk geselecteerd, omdat hier de netwerken lagen van de contactpersonen[6] binnen het CSC. Daarnaast is er voor gekozen om de steekproef binnen Noord-Nederland te houden, omdat er dan een betrouwbare en valide vergelijking kan worden gemaakt tussen de perspectieven van burgers en politiemedewerkers in de basisteams. In totaal hebben 593 respondenten de vragenlijst volledig ingevuld. Tabel 4 toont de beschrijvende statistieken van de respondenten in dit onderzoek.

Tabel 4*. Beschrijvende statistieken van aantal respondenten, basisteam, geslacht en gemiddelde leeftijd.*

	Burgerpanel Leeuwarden	Politie Noord-Nederland
	Aantal (N)	**Aantal (N)**
Respondenten:		
Respons	605	237
Afgehaakt tijdens invullen	144	102
Volledig ingevuld	461	132
Basis team in district:		
District Fryslân		41 (31,1%)
Groningen		65 (49,2%)
Drenthe		25 (18,9%)
Anders, namelijk …		1 (0,8%)
Totaal		132 (100%)
Geslacht:		
Man	241 (52,3%)	75 (56,8%)
Vrouw	166 (36%)	48 (36,4%)
Beide	40 (8,7%)	9 (6,8%)
Anders	14 (3,0%)	-
Totaal	461 (100%)	132 (100%)
Gemiddelde leeftijd:	58 (SD* = 13,90)	46 (SD* = 12)

**SD = standaard deviatie*

[6] PhD kandidaat J. Borwell, prof. dr. W. Stol en dr. J. Jansen

3.2.2 Voorbereiding en werving

2419 leden van het burgerpanel Leeuwarden en 2368 politiemedewerkers uit de basisteams in district Noord-Nederland zijn benaderd door middel van een uitnodigingsbrief. Het sturen van een uitnodigingsbrief is gebruikelijk bij het werven van respondenten voor deelname aan een vragenlijst (Hennink et al., 2020, p. 91). Voor dit onderzoek zijn twee verschillende uitnodigingsbrieven opgesteld met als doel een zo hoog mogelijk responspercentage te krijgen. Er is gekozen voor een informele uitnodigingsbrief aan de politiemedewerkers in de basisteams (zie bijlage 1.1) Volgens Borwell (achtergrond binnen de politie) zouden politiemedewerkers de brief eerder lezen bij een informele schrijfstijl dan bij een formele schrijfstijl. De verwachting is dat burgers daarentegen eerder formele brieven lezen en ontvingen dus een formele uitnodigingsbrief toegestuurd (zie bijlage 1.2).

De inhoud van de uitnodigingsbrief is belangrijk voor het aantal mensen dat deelneemt aan de vragenlijst (Erdogan & Baker, 2002; Sauermann & Roach, 2012). In de uitnodigingsbrief staat informatie over de achtergrond en doel van het onderzoek, de instructie om deel te nemen, de inhoud van de vragen, de geschatte duur en de waarborging van de persoonlijke gegevens. Ook was het mogelijk voor genodigden om vragen te stellen via een mailadres.

De vragenlijsten voor de politiemedewerkers zijn uitgezet via Borwell, omdat zij toegang heeft tot de systemen van de politie. De vragenlijsten konden hierdoor in naam van de politie intern worden uitgezet naar diverse politiedistricten in Noord-Nederland. Het verspreiden van vragenlijsten uit naam van de politie, zou op deze manier kunnen leiden tot een hogere respons vanuit politiemedewerkers, dan wanneer het uitzetten was gebeurd uit naam van een student. De vragenlijsten voor de burgers zijn uitgezet via een contactpersoon[7] van Borwell bij de gemeente Leeuwarden. Ook hier zou het verspreiden van vragenlijsten uit naam van de gemeente kunnen leiden tot een hogere respons, vanuit het burgerpanel, dan uit naam van een student.

Daarnaast hebben 4575[8] uitgenodigden één week na het uitzetten van de uitnodigingsbrief een herinneringsmail ontvangen, omdat dit mogelijk zou leiden tot een responsverhoging van 20 tot 40 procent (Dillman, 1999). 212 genodigden uit één basisteam in Drenthe heeft geen herinneringsmail ontvangen, omdat zij volgens het Coördinatiepunt Operationeel Politiewerk (COP) werden overspoeld met mails. Uiteindelijk is het voltooiingspercentage[9] van politiemedewerkers uitgekomen op 5,6 procent[10] en bij het

[7] Adviseur statistiek en onderzoek bij Gemeente Leeuwarden
[8] 2419 + (2368 – 212) = 4575
[9] Mensen die de vragenlijst volledig hebben ingevuld (zie ook tabel 4).
[10] 132/ 2368*100% = 5,6%

burgerpanel op 19 procent[11]. De betekenis van deze percentages wordt vervolgd in paragraaf 3.5.

3.3 Proces van dataverzameling

3.3.1 Softwareprogramma

Dit onderzoek is afgenomen met behulp van het softwareprogramma “Enalyzer” binnen de gemeente Leeuwarden (Analyzer, z.d.). De gemeente heeft dit softwareprogramma beschikbaar gesteld voor dit onderzoek. Dit softwareprogramma heeft het mogelijk gemaakt om een onbeperkt aantal respondenten te analyseren en een onbeperkt aantal vragen mee te nemen in de opzet. Daarnaast was er ook de mogelijkheid om een professioneel design te ontwerpen (idem). Deze design-aspecten van de vragenlijst hebben invloed op een hogere respons (Dillman et al., 1998).

Uiteindelijk zijn er twee aparte ‘links’ opgesteld één link voor het burgerpanel met de impact en behoeftevragen en één link voor de politiemedewerkers met de impact en behoeftevoorzieningsvragen (zie ook sub-paragraaf 3.3.3). Het was technisch niet mogelijk om dit uit te voeren met één link. De links zijn uitgezet over een periode van ongeveer drie weken (28 juni 2021 tot 19 juli 2021).

3.3.2 Pilot

De vragenlijst is twee keer voorgelegd in een pilotstudie. Een pilotstudie is een vooronderzoek waarbij aspecten zoals de haalbaarheid en de meetinstrumenten worden getest (Hassan et al., 2006; In, 2017; Van Thiel, 2020). De eerste keer werd dat gedaan binnen het netwerk van de onderzoeker en contactpersonen van dit onderzoek, en de tweede keer binnen het onderzoeksteam ‘Cybersafety’ van het CyberScienceCenter (CSC, z.d.), waarvan de contactpersonen deel uitmaken[12]. Het doel van de pilotstudies was om de methodologische kwaliteit van dit onderzoek te verhogen en te waarborgen. Deze testen zijn in dit onderzoek uitgevoerd in verband met de haalbaarheid, het gebruik van de meetinstrumenten en de logica van de casus-vraagstelling verhouding (Hassan et al., 2006; In, 2017; Van Thiel, 2020). De pilots zijn uitgevoerd over de periode van 27 mei 2021 tot 28 juni 2021.

De respondenten gaven in de eerste en tweede pilotversie aan dat de vragenlijst te lang duurde. Het advies was om de vragenlijst maximaal tien minuten te laten duren. Dit betekende dat de vragenlijst moest worden ingekort. De mogelijkheden hiervoor waren het (1) aantal vragen per vignet verminderen, (2) het aantal vignetten verminderen of (3) de vignetten

[11] 461/ 2419*100% = 19%

[12] M. Berkenpas – junior onderzoeker, S. Ebbers – PhD-researcher, S. Westers – docent/onderzoeker, J. Kerstens – Associate lector Politie, Partners en digitalisering, R.M. Zuurveen – afstudeercoördinator integrale veiligheid

verdelen over de respondenten. Uiteindelijk is ervoor gekozen om het aantal vignetten te verminderen, omdat alle vragen noodzakelijk waren om een betrouwbare en valide meting te maken en het responspercentage per vignet zo hoog mogelijk te houden.

In de definitieve versie is ervoor gekozen om vier vignetten in plaats van acht vignetten voor te leggen aan de respondenten (Veenma, 2010). De vier vignetten die zijn meegenomen in dit onderzoek zijn: (1) woninginbraak versus (2) hacken van een online bankaccount en (3) aanranding versus (4) beeld gerelateerd seksueel misbruik. Voor deze combinatie van delicten is gekozen, omdat er dan zowel financiële als een niet-financiële delict motieven worden getoetst. Daarnaast is voor beeld gerelateerd seksueel misbruik gekozen, omdat het nooit is vergeleken met een offline vorm van criminaliteit, zoals aanranding. Beeld gerelateerd seksueel misbruik wordt in de vragenlijst omschreven als het delict 'wraakporno', deze term is een sub variant van beeld gerelateerd seksueel misbruik en is gebruikt om het delict in te kaderen, de definitie van het delict blijft hetzelfde (Ten Voorde, 2017, p. 411).

3.3.3 Operationalisering

De vragenlijst is opgedeeld in een algemene vragenlijst en vier verschillende vignetten (zie bijlage 2). De algemene vragenlijst bestaat uit totaal 10 vragen voor de burgers en uit 13 vragen voor de politiemedewerkers. Deze vragen gaan over persoonsgegevens, zoals geslacht, leeftijd, opleiding en eerdere ervaring met criminaliteit. De politiemedewerkers hebben een paar extra vragen, zoals functie en locatie van het basisteam. Er is voor gekozen om deze algemene vragenlijst aan het eind van de vragenlijst te plaatsen, omdat de gegevens uit de vignetten belangrijker worden geacht bij mogelijke uitval van respondenten.

De casussen van de cyber- en traditionele delicten zijn zoveel mogelijk op elkaar afgestemd om zo nauwkeurig mogelijk de verschillen te meten. Dit betekent dat de persoon, het geldbedrag en het niet verzekerd zijn in een delict vergelijking overeenkomen (zie bijlage 2.2). Na de casus volgen er 21 gesloten vragen opgedeeld in (deel 1) 11 impactsvragen en (deel 2) 10 behoeftevragen of (deel 3) 10 behoeftevoorzieningsvragen. De behoeftevragen worden gesteld aan de respondenten uit het burgerpanel en de behoeftevoorzieningsvragen worden gesteld aan de politiemedewerkers in de basisteams. Bij alle 21 vragen kunnen de respondenten kiezen uit een vijfpunt likert-waarschijnlijkheidsmeetschaal (1 = zeer onwaarschijnlijk, 5 = zeer waarschijnlijk). Deze verdeling van de 21 vragen ziet er volgt uit:

Deel 1.

De impactvragen zijn opgedeeld in de psychologisch/emotionele, fysieke en gedragsmatig/sociale en de financieel/materiele vragen. In dit eerste deel staat de volgende vraag centraal:

“Hoe waarschijnlijk is het volgens u dat *[naam van de persoon in de casus]* door dit delict *[impact vraag]* ervaart?”

De indeling van deze eerste 11 vragen ziet er als volgt uit:

Tabel 5. *Verdeling impactvragen*

Impactvormen:	Nr.	Vraag:
Psychologisch/emotioneel	1.	Depressieve klachten
	2.	Boosheid
	3.	Afname van zelfvertrouwen
	4.	Angst om nog eens slachtoffer te worden van hetzelfde delict
	5.	Gevoelens van schuld en schaamte
Fysiek	6.	Slaapproblemen
	7.	Paniek- of angst gerelateerde lichamelijke klachten
Gedragsmatig/sociaal	8.	Een afname van vertrouwen in andere mensen
	9.	Vermijdingsgedrag
Financieel/materieel	10.	Minder of niet meer werkt
	11.	Financiële schade had om gevolgen van het delict op te lossen

Noot. Het worden vragen wanneer ze in de centrale vraag worden geplaatst, dus bij vraag 1: “Hoe waarschijnlijk is het volgens u dat [naam van de persoon in de casus] door dit delict [depressieve klachten] ervaart?”

Deel 2.

De behoeftevragen zijn onder te verdelen in de volgende clusters van Boom en Kuipers (2008) (zie ook paragraaf 2.4.2). In dit tweede deel staat de volgende vraag centraal:

“Hoe waarschijnlijk is het volgens u dat *[naam van de persoon in de casus]* door dit delict behoefte heeft aan *[behoeftevraag]*?”

Tabel 6. *Verdeling behoefte- en behoeftevoorzieningsvragen*

Clusters:	Nr.	Vraag:
Financieel	1.	Financiële compensatie voor de geleden schade
Emotioneel	2.	Emotionele steun
Informatie	3.	Duidelijkheid over hoe het delict heeft kunnen plaatsvinden
	6.	Informatie over het eventuele politieonderzoek
Strafproces	4.	Aanhouding van de dader
	5.	Contact met de politie
	9.	Serieus genomen als slachtoffer door instanties zoals de politie
Primair	7.	Tips om toekomstig slachtofferschap te voorkomen
	8.	Meehelpen te voorkomen dat anderen mensen slachtoffer worden van hetzelfde delict
Praktisch	10.	Hulp bij het oplossen van door het delict ontstane praktische problemen

Noot. Het worden vragen wanneer ze in de centrale vraag worden geplaatst, dus bij vraag 1: “Hoe waarschijnlijk is het volgens u dat *[naam van de persoon in de casus]* door dit delict behoefte heeft aan *[financiële compensatie voor de geleden schade]*?”

Deel 3.

De behoeftevoorzieningsvragen zijn dezelfde vragen als de behoeftevragen uit het tweede deel. Dit betekent dat deze vragen op dezelfde manier zijn opgedeeld in de clusters van Boom en Kuipers (2008). In dit derde deel staat de volgende vraag centraal:

“Hoe waarschijnlijk denkt u dat de politie *[naam van de persoon in de casus]* in deze behoefte *[behoeftevraag uit deel 2]* kan voorzien?”

3.4 Dataverwerking

Voor dit onderzoek is gebruikt gemaakt van het softwareprogramma IBM SPSS Statistics 26 (IBM, z.d.). De resultaten uit de vragenlijst zijn in dit programma verwerkt. De data-analysemethodes die zijn gebruikt in dit onderzoek zijn vooral de descriptieve analyses om de gemiddelden te berekenen. Daarnaast zijn er ook betrouwbaarheidsanalyses uitgevoerd om gemiddelden samen te voegen. Dit betekent dat de gemiddelde impactvormen en behoefte(voorziening) resultaten zijn getoetst met de Cronbach’s Alpha om te bepalen of deze gemiddelde per delict en per vorm intern consistent zijn (Hoe et al., 2015). Verder is ook de Paired Samples Test (T-test) uitgevoerd om te bepalen of de hypothesen significant zijn. Deze test voer je uit als twee of meer groepen met elkaar vergelijkt (Mara & Cribbie, 2012). In dit onderzoek betekent dat het vergelijken van de groepen; cybercriminaliteit tegenover traditionele criminaliteit. De dataverwerking heeft plaatsgevonden na het proces van dataverzameling wat plaats vond tussen 19 juli 2021 tot 31 juli 2021.

3.5 Betrouwbaarheid en validiteit

In kwantitatief onderzoek heeft de betrouwbaarheid betrekking op de consistentie van het meten van een concept. Er zijn drie prominente factoren die bepalen of een meting betrouwbaar is; (1) interne consistentie of homogeniteit, (2) stabiliteit en (3) inter-onderzoeker betrouwbaarheid (Bryman et al. 2012; Heale & Twycross, 2015). De interne consistentie houdt in de mate waarin items op een schaalmaat construeren. In dit onderzoek wordt de interne consistentie gemeten door middel van de Cronbach’s Alpha. Wanneer de Cronbach Alpha’s hoger is dan 0,7 zijn de items intern consistent en dus betrouwbaar (Bryman et al. 2012, p. 170; Heale & Twycross, 2015, p. 67). De stabiliteit houdt in de consistentie van de resultaten bij herhaalde metingen met hetzelfde instrument. In dit onderzoek wordt dit gewaarborgd door de onderzoekstappen zo nauwkeurig mogelijk te beschrijven. Het onderzoek inclusief de vragenlijst zijn zo opgesteld dat het onderzoek kan worden gerepliceerd voor

vervolgonderzoek (Bryman et al., 2012; Heale & Twycross, 2015; Van Thiel, 2020). De inter-onderzoeker betrouwbaarheid houdt in de variaties op een bepaald punt in de tijd tussen de waarnemers en steekproeven van items. In dit onderzoek kregen alle burgers en politiemedewerkers als groep dezelfde vragenlijst voorgelegd. Er is geprobeerd om de inhoud van de vragenlijst zo gelijk mogelijk te maken (idem). Dit houdt in: dezelfde casus (vignet), dezelfde vragen en dezelfde volgorde van vignetten en vragen. De burgers krijgen daarbij vragen uit deel 2 en politiemedewerkers vragen uit deel 3 (zie tabel 6).

In kwantitatief onderzoek heeft de validiteit betrekking op de mate waarin een concept nauwkeurig wordt gemeten. Er zijn twee prominente factoren die bepalen of een concept nauwkeurig gemeten wordt; (1) interne validiteit en (2) externe validiteit (Bryman et al., 2012; Heale & Twycross, 2015; Van Thiel, 2020). De interne validiteit gaat in op de geldigheid van het onderzoek; de mate waarin de conclusies van het onderzoek geldig zijn voor de onderzoeksgroep (Van Thiel, 2020, p. 61). Op basis van de steekproefcalculator met een foutmarge van 5 procent en een betrouwbaarheidsniveau van 95 procent, voldoet het burgerpanel (N = 461) aan de minimale respons eis (N = 332). Het aantal politiemedewerkers (N = 132) komt daarentegen niet aan de minimale eis (N = 331) van de steekproefcalculator (CheckMarket, z.d.). Dit betekent dat de resultaten uit het burgerpanel een hoge interne validiteit heeft en de politiemedewerkers een lage interne validiteit. Verder is de vragenlijst zoals toegelicht in sub-paragraaf 3.3.2 getest in twee pilotstudies. Ook dit verhoogt de interne validiteit van het onderzoek (Presser et al., 2004).

De externe validiteit gaat over de generaliseerbaarheid; de mate waarin de conclusies ook van toepassing zijn op de (gehele) populatie (Van Thiel, 2020, p. 62). In dit onderzoek is ervoor gekozen om iets kunnen zeggen over de populatie in Noord-Nederland. Op basis van de uitspraak over de interne validiteit kan er al geconcludeerd worden dat de generalisbaarheid laag is voor politiemedewerkers en gemiddeld tot hoog voor burgers. Dit betekent dat niet alleen de externe validiteit hoog is voor burgers, maar ook dat de resultaten een gemiddelde tot een hoge nauwkeurigheid hebben (Bryman et al., 2012; Heale & Twycross, 2015; Van Thiel, 2020).

Tot slot, moet er rekening mee worden gehouden dat dit onderzoek is geschreven in tijden van de corona(crisis). In de aanleiding van dit onderzoek werd al beschreven dat cybercriminaliteit door de coronapandemie is toegenomen (Politie, 2021). Deze pandemie kan mogelijk invloed hebben op de onderzoeksresultaten, bijvoorbeeld dat burgers en politiemedewerkers meer affiniteit hebben gekregen met cybercriminaliteit door deze toename.

3.6 Ethische uitdagingen

Het ethische principe in dit onderzoek vertrekt vanuit het idee: "*How should we treat the people on whom we conduct research?" (*Bryman et al., 2012, p. 130). De ethische uitdagingen van (bestuurskundig) onderzoek kennen daarbij vijf ethische regels: (1) goede bedoelingen, (2) waarachtigheid, (3) privacy, (4) vertrouwelijkheid en (5) instemming (Thiel, 2015, pp. 181-183). Deze ethische regels staan beschreven in de uitnodigingsbrief naar de respondenten (zie bijlage 1). In deze brief staat alle informatie met betrekking tot de ethische verantwoording van dit onderzoek. Dit betekent dat de respondenten worden geïnformeerd over het meedoen aan een vrijwillig onderzoek, het doel van het onderzoek en de vertrouwelijkheid van de persoonlijke gegevens. Daarnaast hebben de respondenten ook de mogelijkheid om voorafgaand aan het onderzoek vragen te stellen via het email adres beschreven onderaan de brief.

3.7 Conclusie

Dit hoofdstuk heeft toegelicht welke onderzoeksmethodologie is gebruikt in deze studie. In het kort, zijn de belangrijkste punten dat het gaat om een kwantitatieve onderzoeksmethode met een vragenlijst in de vorm van een vignettenstudie. In eerste instantie was de bedoeling om acht vignetten mee te nemen in het onderzoek, maar uit de pilots kwam naar voren dat vier vignetten volstonden. De resultaten uit de vier vignetten zullen in het volgende hoofdstuk worden beschreven.

Hoofdstuk 4. Resultaten

In dit hoofdstuk worden de resultaten uit de vragenlijsten gepresenteerd. In paragraaf 4.1 wordt eerst het resultaat uit het burgerpanel weergegeven en in paragraaf 4.2 de resultaten uit de basisteams van de politie. In paragraaf 4.3 worden de resultaten uit 4.1 en 4.2 met elkaar vergeleken. Elke paragraaf bestaat uit twee sub-paragrafen die de resultaten onderscheiden van de impactsvragen en behoefte(voorziening)vragen. Het hoofdstuk sluit af met een antwoord op de hypothesen in paragraaf 4.4.

4.1 Burgerpanel

4.1.1 Impactvormen van slachtofferschap

In deze sub-paragraaf staat de empirische deelvraag: “Wat is volgens de burgers de slachtofferimpact van cybercriminaliteit en traditionele criminaliteit?” centraal. Het antwoord op deze vraag wordt gegeven door de impactvormen (psychologisch/emotioneel, fysiek, gedragsmatig/sociaal, financieel/materieel) van cybercriminaliteit te vergelijken met die van traditionele criminaliteit. Ook wordt in deze sub-paragraaf gedeeltelijk de verantwoording toegelicht op hypothese 1, omdat deze sub-paragraaf alleen gaat over de gepercipieerde impact volgens burgers.

Hypothese 1: *De slachtofferimpact van cybercriminaliteit wordt hoger gepercipieerd dan de slachtofferimpact van traditionele criminaliteit.*

De gemiddelde scores kunnen lopen van (1) zeer onwaarschijnlijk tot (5) zeer waarschijnlijk. Dit betekent hoe hoger de score, hoe groter de waarschijnlijke impact zal zijn. De gemiddelde scores zijn berekend door vragen samen te voegen die vallen onder een bepaalde impactvorm. Bij de psychologisch/emotionele impact in tabel 7 zijn bijvoorbeeld de vragen 1 tot en met 5 samengevoegd tot één gemiddelde (zie ook tabel 5, paragraaf 3.3).

In tabel 7 zijn de gemiddelde resultaten gebaseerd op basis van 461 burgers die alle vignetten hebben ingevuld. De onderstreepte getallen zijn de hoogste cijfers onder de noemer van inbraak en schending van lichamelijke integriteit per impactvorm.

Tabel 7. *De gemiddelde resultaten van de impactvormen volgens burgers*

	Inbraak		**Schending lichamelijke integriteit**		
Impactvormen	Hacken van een online bankaccount	Woninginbraak	Beeld gerelateerd seksueel misbruik	Aanranding	Gem. totaal
Psychologisch/emotioneel	<u>4,16</u>	3,73	<u>4,45</u>	4,08	4,11 (α = .74)
Fysiek	3,46	<u>3,55</u>	<u>3,88</u>	3,70	3,65 (α = .82)

Gedragsmatig/sociaal	3,49	3,20	4,20	3,93	3,71 (α = .76)
Financieel/materiaal	3,14	3,30	3,12	2,82	3,10 (α = .77)
Gem. Totaal	3,56 (α = .83)	3,45 (α = .86)	3,91 (α = .87)	3,63 (α = .91)	

Noot. α= Cronbach's Alpha

Tabel 7 toont dat geen één cijfer een (5) zeer waarschijnlijk scoort of lager (afgerond) dan een (3) misschien scoort. Onder de noemer van inbraak scoort hacken van een online bankaccount aanzienlijk hoger op de psychologisch/emotionele impact (M = 4,16) en in mindere mate hoger op de gedragsmatig/sociale impact (M = 3,49) dan bij woninginbraak. Woninginbraak scoort daarentegen iets hoger op de fysieke impact (M = 3,55) en nog iets hoger op de financieel/materiele impact (M = 3,30) dan bij het hacken van een online bankaccount. Onder de noemer van schending lichamelijke integriteit scoort beeld gerelateerd seksueel misbruik op alle impactvormen hoger (M = 4,45, 3,88, 4,20, 3,12) dan bij aanranding. Dit betekent dat de cybercriminaliteitsdelicten een hoger gemiddelde scoren op de psychologisch/emotionele impact en de gedragsmatig/sociale impact dan de traditionele criminaliteitsdelicten. Deze uitkomsten bevestigen dat een aantal studies (Price et al., 2013; Bonanno & Hymel, 2013: Perren et al., 2010) verklaren dat de psychologisch/emotionele impact groter is bij cybercriminaliteit dan bij traditionele criminaliteit. Deze uitkomsten bevestigen daarentegen niet dat een aantal studies (Button et al., 2020; Morrall et al., 2010) verklaren dat de fysieke impact groter is bij cybercriminaliteit dan bij traditionele criminaliteit.

Ook zijn alle impactvormen per individueel delict berekend. De totale gemiddelde impact van hacken van een bankaccount (M = 3,56) is hoger dan de totale gemiddelde impact van woninginbraak (M = 3,45). Ook beeld gerelateerd seksueel misbruik (M = 3,91) scoort hoger op de totale gemiddelde impact dan aanranding (M = 3,63). Dit geeft weer dat de individuele cybercriminaliteitsdelicten in vergelijking met de individuele traditionele criminaliteitsdelicten een grotere slachtofferimpact hebben. Daarnaast is de Cronbach's Alpha bij elk delict boven de .83. Dit betekent dat de scores (afgerond) vallen in de betrouwbaarheidscategorie 'goed' (Pallant, 2016).

Verder zijn ook de individuele impactvormen berekend bij alle delicten. Hieruit blijkt dat de totale gemiddelde impact van psychologisch/emotionele impact (M = 4,11) het hoogst scoort en daaropvolgend de gedragsmatig/sociale impact (M = 3,71), de fysiek impact (M = 3,65) en de financieel/materiele impact (M = 3,10). De Cronbach's Alpha scoort bij elke impactvorm boven de .74. Dit betekent dat de scores (afgerond) vallen in de betrouwbaarheidscategorie 'acceptabel' (Pallant, 2016).

Als laatst zijn ook de totale gemiddelden van de cybercriminaliteit- en de traditionele criminaliteit delicten samengevoegd tot één gemiddelde. De gemiddelde impact van cybercriminaliteit (M = 3,74; SD = 0,50) en traditionele criminaliteit (M = 3,54; SD = 0,57) bleken uit de Paired Samples Test significant te zijn (t (460) = 11,08; p<0.01). Dit geeft weer dat

cybercriminaliteit significant hoger scoort dan traditionele criminaliteit. In het algemeen, vinden burgers dat de slachtofferimpact dus groter is bij cybercriminaliteit dan bij traditionele criminaliteit.

4.1.2 Behoefte na slachtofferschap

In deze sub-paragraaf staat de empirische deelvraag: “Wat zijn volgens de burgers de behoeften na slachtofferschap van cybercriminaliteit en traditionele criminaliteit?” centraal. Het antwoord op deze vraag wordt gegeven door de behoefteclusters (financieel, emotioneel, informatie, strafproces, primair en praktisch) van cybercriminaliteit te vergelijken met die van traditionele criminaliteit. Ook wordt in deze sub-paragraaf de verantwoording toegelicht op hypothese 2.

Hypothese 2: *Volgens burgers zijn de behoeften na slachtofferschap groter bij cybercriminaliteit dan bij traditionele criminaliteit.*

Ook hier lopen de gemiddelde scores van (1) zeer onwaarschijnlijk tot (5) zeer waarschijnlijk. Dit betekent hoe hoger de score, hoe groter de waarschijnlijke impact zal zijn. De gemiddelde scores zijn berekend door vragen samen te voegen die vallen onder een bepaalde behoefte cluster. Bij de behoefte ‘strafproces’ in tabel 8 zijn bijvoorbeeld de vragen 4, 5 en 9 samengevoegd tot één gemiddelde (zie ook tabel 6, paragraaf 3.3).

In tabel 8 zijn de gemiddelde resultaten gebaseerd op basis van 461 burgers die alle vignetten hebben ingevuld. De onderstreepte getallen zijn de hoogste cijfers onder de noemer van inbraak en schending van lichamelijke integriteit per behoeften cluster.

Tabel 8. *De gemiddelde resultaten van de behoeften clusters volgens burgers*

	Inbraak		**Schending lichamelijke integriteit**		
Behoeften clusters	Hacken van een online bankaccount	Woninginbraak	Beeld gerelateerd seksueel misbruik	Aanranding	Gem. totaal
Financieel	4.46	<u>4,60</u>	<u>2,95</u>	2,67	3,67 (α = .55)
Emotioneel	4,02	<u>4,03</u>	<u>4,67</u>	4,59	4,33 (α = .64)
Informatie	<u>4,43</u>	4,40	3,82	<u>3,83</u>	4,12 (α = .70)
Strafproces	4,61	<u>4,75</u>	<u>4,40</u>	4,32	4,52 (α = .71)
Primair	<u>4,10</u>	3,80	3,81	<u>3,83</u>	3,89 (α = .81)
Praktisch	<u>4,22</u>	4,21	<u>4,09</u>	3,85	4.09 (α = .72)
Gem. Totaal	4,31 (α = .81)	4,30 (α = .82)	3,96 (α = .78)	3,85 (α = .85)	

Noot. α= Cronbach’s Alpha

Tabel 8 toont dat geen één cijfer (afgerond) lager scoort dan een (3) misschien. Onder de noemer van inbraak scoort hacken van een online bankaccount aanzienlijk hoger op de behoefte ‘primair’ (M = 4,10) en in mindere mate op de behoeftes ‘informatie’ (M = 4,43) en ‘praktisch’ (M = 4,22) dan bij woninginbraak. Woninginbraak scoort daarentegen hoger op de behoeftes ‘financieel’ (M = 4,60), ‘emotioneel’ (M = 4,03) en ‘strafproces’ (M = 4,75) dan bij hacken van een online bankaccount. Onder de noemer van schending van lichamelijke integriteit scoort beeld gerelateerd seksueel misbruik hoger op de behoeftes ‘financieel’ (M = 2,95), ‘emotioneel’ (M = 4,67), ‘strafproces’ (M = 4,40) en ‘praktisch’ (M = 4,09) dan bij aanranding. Aanranding daarentegen scoort net iets hoger op de behoeftes ‘informatie’ (M = 3,83) en ‘primair’ (M = 3,83) dan beeld gerelateerd seksueel misbruik. Dit geeft weer dat alleen de cybercriminaliteitsdelicten een hoger gemiddelde scoren op de behoefte ‘praktisch’ dan de traditionele criminaliteitsdelicten. Op basis van deze resultaten is niet nauwkeurig te bepalen welke top drie slachtofferbehoeften gelden voor cybercriminaliteit en traditionele criminaliteit, omdat elk delict een ander combinatie van een top drie heeft (Leukfeldt et al., 2018).

Ook zijn alle behoeftes per individueel delict berekend. De totale gemiddelde van de behoeftes bij hacken van een bankaccount (M = 4,31) is net aan hoger dan het totale gemiddelde van de behoeftes bij woninginbraak (M = 4,30). Ook beeld gerelateerd seksueel misbruik (M = 3,96) scoort net iets hoger op de totale gemiddelde van de behoeftes dan bij aanranding (M = 3,85). Dit geeft weer dat de individuele cybercriminaliteitsdelicten in vergelijking met de individuele traditionele criminaliteitsdelicten een grotere behoefte na slachtofferschap hebben. Daarnaast is de Cronbach’s Alpha bij elk delict boven de .78. Dit betekent dat de scores (afgerond) vallen in de betrouwbaarheidscategorie ‘goed’ (Pallant, 2016).

Verder zijn ook de individuele behoefte clusters berekend bij de delicten. Hieruit blijkt dat de totale gemiddelde behoefte ‘financieel’ (M = 3,67) het laagst scoort en daaropvolgend de behoeftes ‘primair’ (M = 3,89), ‘praktisch’ (M = 4,09), ‘informatie’ (M = 4,12), ‘emotioneel’ (M = 4,33) en ‘strafproces’ (M = 4,52). Over het algemeen, vinden burgers dus de behoefte ‘strafproces’ het meest waarschijnlijk. Dit bevestigt de studies (Leukfeldt et al., 2018; Harrell en Langton, 2013; Cassidy et al.,, 2013; Slonje e.a. 2012; Worsley e.a., 2017, Cross et al., 2016) die deze behoefte na slachtofferschap bovenaan de lijst hebben staan.

Daarnaast is de Cronbach’s Alpha bij elke behoeften cluster boven de .55. Deze score wordt gescoord op de behoefte ‘financieel’ en valt daarmee in de categorie ‘slecht’ betrouwbaarheid (Pallant, 2016). Deze behoefte scoort waarschijnlijk laag, omdat de delicten onder de noemer van schending van lichamelijke integriteit niet direct een financiële behoefte hebben, waardoor de vragen laag scoren, maar ook laag intern consistent zijn. Ook de behoefte ‘emotioneel’ valt in de categorie ‘twijfelachtig’. De rest van de behoeftes scoren hoger dan .70 en vallen daarmee in de betrouwbaarheidsscore van ‘acceptabel’ (Pallant, 2016).

Als laatst zijn ook de totale gemiddelden van de cybercriminaliteit- en de traditionele criminaliteit delicten samengevoegd tot één gemiddelde. De gemiddelde behoefte van cybercriminaliteit (M = 4,13; SD = 0,42) en traditionele criminaliteit (M = 4,08; SD = 0,45) bleken uit de Paired Samples Test significant te zijn (t (460) = 3,78; p<0.01). Dit geeft weer dat cybercriminaliteit significant hoger scoort dan traditionele criminaliteit. Volgens burgers zijn de behoeften na slachtofferschap dus groter bij cybercriminaliteit dan bij traditionele criminaliteit. In de volgende paragraaf en specifiek in sub-paragraaf 4.2.2 wordt verder ingegaan op de behoeftevoorziening na slachtofferschap.

4.2 De basisteams van de politie

4.2.1 Impactvormen van slachtofferschap

In deze sub-paragraaf staat de empirische deelvraag: “Wat is volgens de basisteams van de politie de slachtofferimpact van cybercriminaliteit en traditionele criminaliteit?” centraal. Het antwoord op deze vraag wordt gegeven door de impactvormen (psychologisch/emotioneel, fysiek, gedragsmatig/sociaal, financieel/materieel) van cybercriminaliteit te vergelijken met die van traditionele criminaliteit. Daarnaast volgt de verdere verantwoording op hypothese 1, omdat hier de gepercipieerde impact volgens politiemedewerkers wordt toegelicht.

Hypothese 1: *De impact van cybercriminaliteit wordt hoger gepercipieerd dan de impact van traditionele criminaliteit.*

In deze sub-paragraaf gaat het over de gepercipieerde impact volgens politiemedewerkers. De gemiddelde scores kunnen lopen van (1) zeer onwaarschijnlijk tot (5) zeer waarschijnlijk. Dit betekent hoe hoger de score, hoe groter de waarschijnlijke impact zal zijn. De gemiddelde scores zijn berekend door vragen samen te voegen die vallen onder een bepaalde impactvorm. Bij de psychologisch/emotionele impact in tabel 7 zijn bijvoorbeeld de vragen 1 tot en met 5 samengevoegd tot één gemiddelde (zie ook tabel 5, paragraaf 3.3).

In tabel 9 zijn de gemiddelde resultaten gebaseerd op basis van 132 politiemedewerkers die alle vignetten hebben ingevuld. De onderstreepte getallen zijn de hoogste cijfers onder de noemer van inbraak en schending van lichamelijke integriteit per impactvorm.

Tabel 9. *De gemiddelde resultaten van alle impactvormen volgens politiemedewerkers*

	Inbraak		Schending lichamelijke integriteit		
Impactvormen	Hacken van een online bankaccount	Woninginbraak	Beeld gerelateerd seksueel misbruik	Aanranding	Gem. totaal
Psychologisch/emotioneel	4,24	3,73	4,48	4,16	4,15 (α = .67)
Fysiek	3,53	3,64	3,91	3,65	3,68 (α = .77)
Gedragsmatig/sociaal	3,64	3,16	4,14	3,85	3,70 (α = .71)
Financieel/materiaal	3,18	3,19	3,00	2,78	3,04 (α = .72)
Gem. Totaal	3,64 (α = 79.)	3,43 (α = .84)	3,89 (α = .86)	3,61 (α = .88)	

Noot. α= Cronbach's Alpha

Tabel 9 toont dat geen één cijfer een (5) zeer waarschijnlijk scoort of lager dan een (2) onwaarschijnlijk scoort. Onder de noemer van inbraak scoort hacken van een online bankaccount aanzienlijk hoger op de psychologisch/emotionele impact (M = 4,24) en gedragsmatig/sociale impact (M = 3,64) dan bij woninginbraak. Woninginbraak scoort daarentegen iets hoger op de fysieke impact (M = 3,64) en net iets hoger op de financieel/materiele impact (M = 3,19) dan bij hacken van een online bankaccount. Onder de noemer van schending lichamelijke integriteit scoort beeld gerelateerd seksueel misbruik op alle impactvormen hoger (M = 4,48, 3,91,4,41,3,00) dan bij aanranding. Dit geeft weer dat de cybercriminaliteitsdelicten een hoger gemiddelde scoren op de psychologisch/emotionele impact en de gedragsmatig/sociale impact dan de traditionele criminaliteitsdelicten. Deze uitkomsten bevestigen, net zoals in sub-paragraaf 4.1.1, dat studies (Price et al., 2013; Bonanno & Hymel, 2013: Perren et al., 2010) verklaren dat de psychologisch/emotionele impact groter is bij cybercriminaliteit dan bij traditionele criminaliteit. Deze uitkomsten bevestigen daarentegen niet dat studies (Button et al., 2020; Morrall et al., 2010) verklaren dat de fysieke impact groter is bij cybercriminaliteit dan bij traditionele criminaliteit.

Ook zijn alle impactvorm per individueel delict berekend. De totale gemiddelde impact van hacken van een bankaccount (M = 3,64) is hoger dan de totale gemiddelde impact van woninginbraak (M = 3,43). Ook beeld gerelateerd seksueel misbruik (M = 3,89) scoort hoger op de totale gemiddelde impact dan aanranding (M = 3,61). Dit geeft weer dat de individuele cybercriminaliteitsdelicten in vergelijking met de individuele traditionele criminaliteitsdelicten een grotere slachtofferimpact hebben. Daarnaast is de Cronbach's Alpha bij elk delict boven de .79. Dit betekent dat de scores (afgerond) vallen in de betrouwbaarheidscategorie 'goed' (Pallant, 2016).

Verder zijn ook de individuele impactvormen berekend bij deze delicten. Hieruit blijkt dat de totale gemiddelde impact van psychologisch/emotionele impact (M = 4,15) het hoogst

scoort en daaropvolgend de gedragsmatig/sociale impact (M = 3,70), de fysieke impact (M= 3,68) en de financieel/materiele impact (M = 3,04). De Cronbach's Alpha scoort bij elke impactvorm boven de .67. Dit betekent dat de scores (afgerond) vallen in de betrouwbaarheidscategorie 'acceptabel' (Pallant, 2016).

Als laatst zijn ook de totale gemiddelden van de cybercriminaliteit- en de traditionele criminaliteit delicten samengevoegd tot één gemiddelde. De gemiddelde impact van cybercriminaliteit (M = 3,77; SD = 0,44) en traditionele criminaliteit (M = 3,52; SD = 0,46) bleken uit de Paired Samples Test significant te zijn (t (131) = 7,32; p<0.01). Dit geeft weer dat cybercriminaliteit significant hoger scoort dan traditionele criminaliteit. In het algemeen geven politiemedewerkers aan dat de slachtofferimpact groter is bij cybercriminaliteit dan bij traditionele criminaliteit.

4.2.2 Behoeftevoorziening na slachtofferschap

In deze sub-paragraaf staat de empirische deelvraag: "In hoeverre kan de politie volgens de politiemedewerkers in de behoeften van slachtoffers voorzien?" centraal. Het antwoord op deze vraag wordt gegeven door de behoefteclusters (financieel, emotioneel, informatie, strafproces, primair en praktisch) van cybercriminaliteit te vergelijken met die van traditionele criminaliteit. Ook wordt in deze sub-paragraaf de verantwoording toegelicht op hypothese 3.

Hypothese 3*: Volgens politiemedewerkers zijn de behoeftevoorzieningen na slachtofferschap groter bij traditionele criminaliteit dan bij cybercriminaliteit*

Ook hier lopen de gemiddelde scores van (1) zeer onwaarschijnlijk tot (5) zeer waarschijnlijk. Dit betekent hoe hoger de score, hoe groter de waarschijnlijke impact zal zijn. De gemiddelde scores zijn berekend door vragen samen te voegen die vallen onder een bepaald behoefte cluster. Bij de behoefte 'strafproces' in tabel 8 zijn bijvoorbeeld de vragen 4, 5 en 9 samengevoegd tot één gemiddelde (zie ook tabel 6, paragraaf 3.3).

In tabel 10 zijn de gemiddelde resultaten gebaseerd op basis van 132 politiemedewerkers die alle vignetten hebben ingevuld. De onderstreepte getallen zijn de hoogste cijfers onder de noemer van inbraak en schending van lichamelijke integriteit per behoeftevoorziening cluster.

Tabel 10. *De gemiddelde resultaten van alle behoeftevoorziening clusters volgens politiemedewerkers*

	Inbraak		**Schending lichamelijke integriteit**		
Behoeftevoorziening clusters	Hacken van een online bankaccount	Woninginbraak	Beeld gerelateerd seksueel misbruik	Aanranding	Gem. totaal
Financieel	2,28	2,43	2,31	2,18	2,30 (α = .85)
Emotioneel	3,39	3,64	3,63	3,77	3,61 (α = .91)
Informatie	4,04	4,22	4,22	4,02	4,13 (α = .85)
Strafproces	3,98	4,15	4,46	4,41	4,25 (α = .86)
Primair	3,88	3,87	3,94	3,64	3,83 (α = .83)
Praktisch	2,88	3,17	3,19	3,13	3,09 (α = .85)
Gem. Totaal	3,41 (α = .75)	3,58 (α = .78)	3,63 (α = .79)	3,52 (α = .81)	

Noot. α= Cronbach's Alpha

Tabel 10 toont dat er geen één keer (5) zeer waarschijnlijk wordt gescoord, maar wel voor het eerst (2) zeer onwaarschijnlijk (zie financieel, tabel 10). Dit betekent, volgens politiemedewerkers dat het zeer onwaarschijnlijk is dat de politie na slachtofferschap in de behoefte 'financieel' voorziet. Onder de noemer van inbraak scoort woninginbraak gemiddeld hoger op de behoeftevoorzieningen 'financieel' (M = 2,43), 'emotioneel' (M = 3,64), 'informatie' (M = 4,22), 'strafproces' (M = 4,15) en 'praktisch' (M = 3,17) dan bij hacken van een online bankaccount. Hacken van een online bankaccount scoort daarentegen net aan iets hoger op de behoeftevoorziening 'primair' (M = 3,87) dan bij woninginbraak. Onder de noemer van schending van lichamelijke integriteit scoort beeld gerelateerd seksueel misbruik hoger op de behoeftevoorzieningen 'financieel' (M = 2,31), 'informatie' (M = 4,22), 'strafproces' (M = 4,46), 'primair' (M = 3,94) en 'praktisch' (M = 3,19) dan bij aanranding. Aanranding daarentegen scoort hoger op de behoeftevoorziening 'emotioneel' (M = 3,77) dan beeld gerelateerd seksueel misbruik. Over het algemeen, is volgens politiemedewerkers de behoeftevoorziening onder de noemer van inbraak groter bij traditionele criminaliteit en onder de noemer van bij schending lichamelijke integriteit groter bij cybercriminaliteit.

Het valt op dat er een top drie slachtofferbehoeftevoorziening is aan te wijzen (Leukfeldt et al., 2018). De top drie kan per delict van plaats verschillen, maar de behoeftevoorziening 'strafproces', 'informatie', en 'primair' staan bij alle delicten in de top drie. Dit betekent dus dat politiemedewerkers vinden dat de politie slachtoffers het meest waarschijnlijk in deze drie behoeften moeten worden voorzien, voor zowel cyber- als traditionele criminaliteit. Aan de andere kant vinden ze ook dat de politie slachtoffers het minst waarschijnlijk kunnen voorzien in de behoefte 'financieel'.

Ook zijn alle behoeftes per individueel delict berekend. Het totale gemiddelde bij de behoeftevoorziening van woninginbraak (M = 3,58) is hoger dan het totale gemiddelde bij hacken van een online bankaccount (M = 3,41). Beeld gerelateerd seksueel misbruik (M = 3,63) scoort daarentegen hoger op de totale gemiddelde behoeftevoorziening dan aanranding (M = 3,52). Dit betekent dat politiemedewerkers het waarschijnlijker vinden dat de politie slachtoffers onder de noemer van inbraak kan voorzien bij traditionele criminaliteit dan bij cybercriminaliteit. Onder de noemer van schending lichamelijke integriteit is de voorziening waarschijnlijker bij cybercriminaliteit dan bij traditionele criminaliteit. De Cronbach's Alpha scoort bij elke behoeftevoorziening cluster boven de .75. Dit betekent dat de scores (afgerond) vallen in de betrouwbaarheidscategorie 'goed' (Pallant, 2016).

Verder zijn ook de individuele behoeftevoorziening berekend bij de delicten. Hieruit blijkt dat de totale gemiddelde behoefte 'financieel' (M = 2,30) het laagst scoort en daaropvolgend de behoeftes 'praktisch' (M = 3,09), 'emotioneel' (M = 3,61), 'primair' (M = 3,83), 'informatie' (M = 4,13) en 'strafproces' (M = 4,25). Dit geeft weer dat politiemedewerkers vinden dat de politie slachtoffers het minst waarschijnlijk kan voorzien in de behoefte 'financieel', en het meest waarschijnlijk in de behoefte 'strafproces'. De Cronbach's Alpha scoort bij elk delict boven de .83. Dit betekent dat de scores (afgerond) vallen in de betrouwbaarheidscategorie 'goed' (Pallant, 2016).

Als laatst zijn ook de totale gemiddelden van de cybercriminaliteit- en de traditionele criminaliteit delicten samengevoegd tot één gemiddelde. De gemiddelde behoeftevoorziening van cybercriminaliteit (M = 3,52; SD = 0,46) en traditionele criminaliteit (M = 3,55; SD = 0,49) bleken uit de Paired Samples Test niet significant te zijn (t (131) = 1,27; p<0.205). Dit geeft weer dat traditionele criminaliteit niet significant hoger scoort dan cybercriminaliteit. Volgens politiemedewerkers zijn de behoeftevoorzieningen na slachtofferschap dus niet groter bij traditionele criminaliteit dan bij cybercriminaliteit. In sub-paragraaf 4.1.2 bleek de behoefte volgens burgers daarentegen groter te zijn bij cybercriminaliteit dan bij traditionele criminaliteit. Deze en andere verschillen zullen verder aanbod komen in de volgende paragraaf.

4.3 Verschillen tussen de basisteams van de politie en burgers

In deze paragraaf staat de empirische deelvraag: "Bestaan er verschillen in percepties tussen de basisteams van de politie en de burgers?" centraal. Hiervoor zijn de gemiddelde scores overgenomen uit paragraaf 4.1 en 4.2.

4.3.1 Impactvormen van slachtofferschap

In deze sub-paragraaf worden de gemiddelde scores uit de impactvormen volgens burgers (zie sub-paragraaf 4.1.1) en politiemedewerkers (zie sub-paragraaf 4.2.1) toegelicht. Deze

scores worden per criminaliteitsvorm en bijhorende delictsvormen weergegeven. Dit betekent dat in tabel 11 de gemiddelde scores van cybercriminaliteit en in tabel 12 de gemiddelde scores van traditionele criminaliteit worden weergegeven. In deze sub-paragraaf zijn niet de gemiddelde totale scores per impactvorm berekend, zoals bij tabel 7 tot en met 10 wel het geval was. Deze scores zijn niet meegenomen, omdat de gegevens van burgers en politiemedewerkers in twee aparte SPSS-bestanden zijn opgenomen. Hierdoor was het niet mogelijk om de Cronbach's Alpha te berekenen. De onderstreepte getallen zijn de hoogste cijfers van het delict per impactvorm.

Tabel 11. *De gemiddelde impactvormen bij cybercriminaliteitsdelicten volgens burgers en politiemedewerkers*

	Cybercriminaliteit			
	Hacken van een online bankaccount		**Beeld gerelateerd seksueel misbruik**	
Impactvormen	*Burgers*	*Politiemedewerkers*	*Burgers*	*Politiemedewerkers*
Psychologisch/emotioneel	4,16	<u>4,24</u>	4,45	<u>4,48</u>
Fysiek	3,46	<u>3,53</u>	3,88	<u>3,91</u>
Gedragsmatig/sociaal	3,49	<u>3,64</u>	<u>4,20</u>	4,14
Financieel/materiaal	3,14	<u>3,18</u>	<u>3,12</u>	3,00
Gem. Totaal	3,56 (α = .83)	3,64 (α = 79.)	3,91 (α = .87)	3,89 (α = .86)

Noot. α= Cronbach's Alpha

Tabel 11 toont dat gemiddelde impactvormen tussen burgers en politiemedewerkers per cybercriminaliteit delict dicht bij elkaar liggen. Hacken van een online bankaccount scoort net iets hoger bij politiemedewerkers (M = 3,64) dan bij burgers (M = 3,56). Beeld gerelateerd seksueel misbruik scoort daarentegen net iets hoger bij burgers (M = 3,91) dan bij politiemedewerkers (M = 3,89). Verder valt het op dat beeld gerelateerd seksueel misbruik gemiddeld hoger scoort dan hacken van een online bankaccount. Dit geeft weer dat burgers en politiemedewerkers het waarschijnlijker vinden dat de slachtofferimpact bij beeld gerelateerd seksueel misbruik groter is dan bij het hacken van een online bankaccount.

Tabel 12. *De gemiddelde impactvormen bij traditionele criminaliteitsdelicten volgens burgers en politiemedewerkers*

	Traditionele criminaliteit			
	Woninginbraak		**Aanranding**	
Impactvormen	*Burgers*	*Politiemedewerkers*	*Burgers*	*Politiemedewerkers*
Psychologisch/emotioneel	<u>3,73</u>	<u>3,73</u>	4,08	<u>4,16</u>

Fysiek	3,55	3,64	3,70	3,65
Gedragsmatige/sociale	3,20	3,16	3,93	3,85
Financieel/materiaal	3,30	3,19	2,82	2,78
Gem. Totaal	3,45 (α = .86)	3,43 (α = .84)	3,63 (α = .91)	3,61 (α = .88)

Noot. α= Cronbach's Alpha

Tabel 12 toont dat ook hier de gemiddelde impactvormen tussen burgers en politiemedewerkers per traditioneel criminaliteit delict dicht bij elkaar liggen. Woninginbraak scoort net iets hoger bij burgers (M = 3,45) dan bij politiemedewerkers (M = 3,43). Ook aanranding scoort daarentegen net iets hoger bij burgers (M = 3,63) dan bij politiemedewerkers (M = 3,61). Verder valt het op dat aanranding gemiddeld hoger scoort dan een woninginbraak. Dit geeft weer dat burgers en politiemedewerkers het waarschijnlijker vinden dat de slachtoffersimpact groter is bij aanranding dan bij woninginbraak.

4.3.2 Behoefte(voorziening) na slachtofferschap

In deze sub-paragraaf worden de gemiddelde scores uit de behoefte volgens burgers (zie sub-paragraaf 4.1.2) en behoeftevoorziening politiemedewerkers (zie sub-paragraaf 4.2.2) toegelicht. Ook deze scores worden per criminaliteitsvorm en bijhorende delictsvormen weergegeven. Dit betekent dat in tabel 13 de gemiddelde scores van cybercriminaliteit en in tabel 14 de gemiddelde scores van traditionele criminaliteit worden weergegeven. In deze sub-paragraaf zijn om dezelfde reden als in sub-paragraaf 4.3.1 niet de gemiddelde totale scores per behoeftecluster berekend. De onderstreepte getallen zijn de hoogste cijfers van het delict per behoefte(voorziening) cluster.

Tabel 13. *De gemiddelde behoefte(voorziening) bij cybercriminaliteitsdelicten volgens burgers en politiemedewerkers*

	Cybercriminaliteit			
	Hacken van een online bankaccount		**Beeld gerelateerd seksueel misbruik**	
Behoefte(voorziening) clusters	*Burgers*	*Politiemedewerkers*	*Burgers*	*Politiemedewerkers*
Financieel	4.46	2,28	2,95	2,31
Emotioneel	4,02	3,39	4,67	3,63
Informatie	4,43	4,04	3,82	4,22
Strafproces	4,61	3,98	4,40	4,46
Primair	4,10	3,88	3,81	3,94
Praktisch	4,22	2,88	4,09	3,19
Gem. Totaal	4,31 (α = .81)	3,41 (α = .75)	3,96 (α = .78)	3,63 (α = .79)

Noot. α= Cronbach's Alpha

Tabel 13 toont dat gemiddelde scores op behoefte en behoeftevoorziening uiteenlopen. De behoefte scores vanuit burgers zijn aanzienlijk hoger dan de scores op de behoeftevoorziening vanuit politiemedewerkers. Deze scores zijn echter niet goed vergelijkbaar, omdat politiemedewerkers vragen kregen voorgelegd in hoeverre de politie in de behoeftes kan voorzien en burgers vragen over behoeftes in het algemeen. Verder is te zien dat hacken van een online bankaccount (M = 4,31) een hogere behoefte score heeft dan beeld gerelateerd seksueel misbruik (M = 3, 96). Dit geeft weer dat burgers het waarschijnlijker vinden dat slachtoffers een grotere behoefte hebben bij hacken van een online bankaccount dan bij beeld gerelateerd seksueel misbruik. Daarentegen toont de score bij politiemedewerkers dat beeld gerelateerd seksueel misbruik (M = 3,63) een hogere behoeftevoorziening heeft dan hacken van een online bankaccount (M = 3,41). Dit geeft weer dat politiemedewerkers het waarschijnlijker vinden dat de politie in de behoefte kan voorzien bij beeld gerelateerd seksueel misbruik dan bij het hacken van een online bankaccount.

Tabel 14. *De gemiddelde behoefte(voorziening) bij traditionele criminaliteitsdelicten volgens burgers en politiemedewerkers*

	Traditionele criminaliteit			
	Woninginbraak		**Aanranding**	
Behoefte(voorziening) clusters	*Burgers*	*Politiemedewerkers*	*Burgers*	*Politiemedewerkers*
Financieel	4,60	2,43	2,67	2,18
Emotioneel	4,03	3,64	4,59	3,77
Informatie	4,40	4,22	3,83	4,02
Strafproces	4,75	4,15	4,32	4,41
Primair	3,80	3,87	3,83	3,64
Praktisch	4,21	3,17	3,85	3,13
Gem. Totaal	4,30 (α = .82)	3,58 (α = .78)	3,85 (α = .85)	3,52 (α = .81)

Noot. α= Cronbach's Alpha

Tabel 14 toont eveneens dat de gemiddeldes van burgers hoger scoren dan de gemiddeldes van politiemedewerkers (zie tabel 13). Bij de toelichting van tabel 13 werd beschreven dat deze gemiddeldes niet met elkaar te vergelijken zijn, dezelfde redenering geldt ook bij tabel 14. Verder is te zien dat woninginbraak (M = 4,30) een hogere behoefte score heeft dan aanranding (M = 3,85). Dit houdt in dat burgers het waarschijnlijker vinden dat slachtoffers een grotere behoeften hebben bij woninginbraak dan bij aanranding. Hetzelfde resultaat doet zich voor bij de gemiddeldes van de politiemedewerkers. Ook zij scoren hoger op de behoeftevoorziening bij woninginbraak (M = 3,58) dan bij aanranding (M = 3,52). Dit geeft weer

dat politiemedewerkers het waarschijnlijker vinden dat de politie in de behoefte kan voorzien bij woninginbraak dan bij aanranding, maar de verschillen zijn niet aanzienlijk groot.

4.4 Conclusie resultaten

In deze paragraaf wordt nagegaan of de opgestelde hypothesen, die zijn getoetst in dit hoofdstuk worden verworpen of worden aangehouden. Hieronder zullen de resultaten op deze hypothesen nogmaals kort worden toegelicht.

Hypothese 1: *De impact van cybercriminaliteit wordt hoger gepercipieerd dan de impact van traditionele criminaliteit.*

De gepercipieerde impact volgens burgers blijkt uit paragraaf 4.1.1 hoger te zijn voor cybercriminaliteit (M = 3,74) dan voor traditionele criminaliteit (M = 3,54). De gepercipieerde impact volgens politiemedewerkers blijkt uit paragraaf 4.2.1 eveneens hoger te zijn voor cybercriminaliteit (M = 3,77) dan voor traditionele criminaliteit (M = 3,52). Verder valt op dat de scores van burgers en politiemedewerkers nauwelijks verschillen. Op basis van deze resultaten kan hypothese 1 worden aangehouden. De testen zijn, zowel bij burgers als bij politiemedewerkers significant. Hierbij moet wel rekening worden gehouden dat er geen statistische toetsen, zoals de Cronbach's Alpha, zijn uitgevoerd tussen de groepen burgers en politiemedewerkers. Deze groepen zijn afzonderlijk geanalyseerd en getest.

Hypothese 2: *Volgens burgers zijn de behoeften na slachtofferschap groter bij cybercriminaliteit dan bij traditionele criminaliteit.*

Volgens burgers zijn de behoeften na slachtofferschap groter bij cybercriminaliteit (M = 4,13) dan bij traditionele criminaliteit (M = 4,08). De uitgevoerde Paired Samples Test liet zien dat ook deze test significant was. Dit betekent dat hypothese 2, net zoals hypothese 1, kan worden aangehouden.

Hypothese 3*: Volgens politiemedewerkers zijn de behoeftevoorzieningen na slachtofferschap groter bij traditionele criminaliteit dan bij cybercriminaliteit*

Volgens politiemedewerkers lijkt de behoeftevoorziening na slachtofferschap uit de gemiddelde scores hoger uit te vallen bij traditionele criminaliteit (M = 3,55) dan bij cybercriminaliteit (M = 3,52). Uit de Paired Samples Test blijkt de test tussen de cyber- en traditionele delicten niet significant te zijn ($p<0.205$). Dit betekent dat deze hypothese verworpen wordt.

Hoofdstuk 5. Conclusie en discussie

In dit hoofdstuk wordt in paragraaf 5.1 de conclusie van dit onderzoek beschreven. Vervolgens wordt in paragraaf 5.2 de discussie uiteengezet. De discussie bestaat uit twee sub-paragrafen waar wordt ingegaan op de interpretatie van de resultaten en de onderzoeks- en beleidsaanbevelingen.

5.1 Conclusie

In dit onderzoek is, aan de hand van voornamelijk een vignettenstudie, antwoord geformuleerd op de onderzoeksvraag: *Wat is volgens de basisteams van de politie en burgers uit Noord-Nederland de slachtofferimpact en de behoefte(voorziening) na slachtofferschap van cybercriminaliteit in vergelijking met traditionele criminaliteit?*

Het antwoord op deze vraag is een opsomming van de theoretische en empirische deelvragen (zie ook paragraaf 1.2). De antwoorden op de theoretische deelvragen (hoofdstuk 2) hebben bepaald welke definities, theorieën en informatie bekend zijn in de literatuur over de slachtofferimpact en behoefte(voorziening) na slachtofferschap van cybercriminaliteit en traditionele criminaliteit. Deze literatuur is vervolgens gebruikt om een antwoord te krijgen op de empirische deelvragen. Deze empirische deelvragen zijn beantwoord in de resultaten (hoofdstuk 4).

Over het algemeen, hebben de resultaten laten zien dat de perspectieven van burgers en politiemedewerkers ten aanzien van de slachtofferimpact niet veel van elkaar verschillen. Beide groepen laten zien dat de impact van cybercriminaliteit hoger wordt gepercipieerd dan de impact van traditionele criminaliteit (conclusie hypothese 1). Verder valt op dat beide groepen ten aanzien van de slachtofferimpact aangeven dat de psychologisch/emotionele impact het grootst in vergelijking met de andere impactvormen. Tot slot, geven beide groepen aan dat de delicten onder de noemer schending van lichamelijke integriteit een hogere slachtofferimpact hebben dan de delicten onder de noemer inbraak.

De behoefte na slachtofferschap is alleen vanuit het perspectief van burgers beoordeeld. Volgens burgers zijn de behoeften na slachtofferschap groter bij cybercriminaliteit dan bij traditionele criminaliteit (conclusie hypothese 2). Verder blijkt dat de behoefte na slachtofferschap afhankelijk is van het delict. De behoefte ‘emotioneel’ scoort het hoogst bij de delicten onder de noemer schending lichamelijke integriteit, terwijl de behoefte ‘stafproces’ hoog scoort bij delicten onder de noemer inbraak. Gemiddeld genomen, is de behoefte na slachtofferschap groter onder de noemer inbraak dan onder de noemer schending lichamelijke integriteit.

De behoeftevoorziening na slachtofferschap is alleen vanuit het perspectief van politiemedewerkers beoordeeld. Het is niet significant of de behoeftevoorziening na

slachtofferschap volgens politiemedewerkers groter is bij traditionele criminaliteit dan bij cybercriminaliteit (conclusie hypothese 3). Dit heeft te maken met het feit dat politiemedewerkers vinden dat de politie het meest waarschijnlijk in de behoefte kan voorzien van het cybercriminaliteitsdelict, namelijk beeld gerelateerd seksueel misbruik. Verder valt op dat politiemedewerkers vinden dat de politie, een slachtoffer bij alle vier delicten het meest waarschijnlijk kan voorzien in de behoeften van strafproces, informatie en primair. Daarentegen vinden politiemedewerkers dat de politie een slachtoffer het minst waarschijnlijk kan voorzien in de behoefte 'financieel'.

In de voorgaande hoofdstukken en deze conclusie staat beschreven dat de slachtofferimpact is beoordeeld vanuit beide perspectieven en dat de behoefte en behoeftevoorziening na slachtofferschap beoordeeld is vanuit één perspectief. In de discussie wordt hier verder op ingegaan (zie paragraaf 5.2.1).

5.2 Discussie

In deze paragraaf worden de resultaten uit het onderzoek geïnterpreteerd. Dit betekent dat in sub-paragraaf 5.2.1 de resultaten wordt geïnterpreteerd aan de hand van de literatuur in dit onderzoek. In sub-paragraaf 5.2.2 worden onderzoeks- en beleidsaanbevelingen beschreven.

5.2.1 Interpretatie resultaten

In de aanleiding van dit onderzoek is beschreven dat de cybercriminaliteit steeds dichter bij de slachtoffercijfers van de traditionele criminaliteit komt (CBS, 2020a). In het rapport 'Veilig Online 2020' verkondigden burgers dat zij zich over het algemeen veilig online voelen (Ministerie van Economische Zaken, 2020). Er zijn in de literatuur geen rapporten over het jaar 2021 beschikbaar om de vergelijking tussen cybercriminaliteit en traditionele criminaliteit inzichtelijk(er) te maken. Dit onderzoek biedt resultaten over deze vergelijking in 2021, in tijden van de corona(crisis). Op basis van de resultaten in dit onderzoek zou een vervolgrapport over 'Veilig Online versus Veilig Offline 2021' moeten worden opgesteld, namens de Rijksoverheid. De resultaten in dit onderzoek laten zien dat de slachtofferimpact van cybercriminaliteit volgens burgers en politiemedewerkers inmiddels voorbij de traditionele criminaliteit is (vandaar de titel van dit onderzoek).

De resultaten over de slachtofferimpact komen gedeeltelijk overeen met eerdere studies, die beweren dat de slachtofferimpact van cybercriminaliteit voorbij de traditionele criminaliteit is (Price et al., 2013; Bonanno & Hymel, 2013: Perren et al., 2010; Leukfeldt et al., 2018). Aan de andere kant is er ook nog veel onbekend over de slachtofferimpact van deze criminaliteitsvergelijking. Dit onderzoek heeft aangetoond dat de gedragsmatig/sociale impact

groter is bij cybercriminaliteit dan bij traditionele criminaliteit en dat de financiële impact de laagste scorende impact is van de vier impactvormen (zie tabel 7 & 9).

De resultaten over de behoefte na slachtofferschap komen grotendeels overeen met eerdere studies, die beweren dat slachtoffers vooral behoefte hebben aan het straf- en vergeldingsproces (Leukfeldt et al., 2018; Cross et al., 2016; Cassidy, et al., 2013; Slonje e.a. 2012; Worsley e.a., 2017). Over het algemeen, verschillen de behoefte na slachtofferschap van cybercriminaliteit en traditionele criminaliteit niet veel van elkaar. Cybercriminaliteit lijkt net iets hoger te scoren dan traditionele criminaliteit.

De resultaten over de behoeftevoorziening na slachtofferschap van cybercriminaliteit en traditionele criminaliteit verschillen ook niet veel van elkaar. In dit onderzoek is ervoor gekozen om de behoefte clusters van ten Boom en Kuijpers (2008) te gebruiken voor zowel de behoefte als de behoeftevoorziening, omdat er nog veel onbekend is in de literatuur over de behoeftevoorziening na slachtofferschap.

Achteraf gezien, hadden de vragen over de behoeftevoorziening meer gespecifieerd moeten worden naar de rol en verantwoordelijkheid van de politie. Hierdoor zijn de resultaten uit de behoefte vanuit burgers en behoeftevoorziening vanuit politiemedewerkers niet met elkaar te vergelijken. Een aanbeveling is om in vervolgonderzoek is de behoefte dan wel de behoeftevoorziening na slachtofferschap te specifiëren naar de rol en verantwoordelijkheid van de politie, zodat de perspectieven van burgers kunnen worden vergeleken met de perspectieven van politiemedewerkers.

Verder is een methodologische discussie maakbaar, wanneer de vraag wordt gesteld of de twee cybercriminaliteitsdelicten en twee traditionele criminaliteitsdelicten in dit onderzoek een betrouwbare en valide bron zijn voor het soort criminaliteit dat ze vertegenwoordigen. In vervolgonderzoek, met andere criminaliteitsdelicten hoeven deze resultaten en conclusies niet overeen te komen. Dit zou kunnen betekenen dat in vervolgonderzoek met andere criminaliteitsdelicten de slachtofferimpact bij traditionele criminaliteit hoger kan zijn dan cybercriminaliteit.

In de volgende sub-paragraaf wordt verder ingegaan op de onderzoeks- en beleidsaanbevelingen van dit onderzoek.

5.2.2 Onderzoeks- en beleidsaanbevelingen

Op basis van de resultaten uit dit onderzoek en de mogelijke methodologische discussie (zie sub-paragraaf 5.2.1) is mijn aanbeveling om meer onderzoek te verrichten naar de vergelijking van cyber- en traditionele criminaliteit. In dit onderzoek zijn vier criminaliteitsvormen meegenomen, terwijl er in werkelijkheid talloze delictsvormen bestaan.

In het theoretisch kader van dit onderzoek werd beschreven dat de slachtoffers van cybercriminaliteit zijn weggestuurd en daardoor geen aangifte kunnen doen. Ook werd

beschreven dat slachtoffers het gevoel hebben dat ze niet serieus worden genomen (Leukfeldt et al., 2018). Volgens Stol (2018) is dit te wijten aan gebrek aan kennis over cybercriminaliteit bij politiemedewerkers (Stol, 2018). Deze kennis is niet onderzocht in dit onderzoek, maar wel het perspectief van politiemedewerkers op de slachtofferimpact en behoeftevoorziening na slachtofferschap. Hieruit is gebleken dat politiemedewerkers vinden dat de slachtofferimpact hoger is bij cybercriminaliteit dan bij traditionele criminaliteit (zie hypothese 1). Dit betekent dat het niet ligt aan het perspectief van politiemedewerkers ten aanzien van slachtofferschap van cybercriminaliteit. Maar mogelijk, zoals Stol (2018), beweert een gebrek aan kennis bij politiemedewerkers over cybercriminaliteit (Stol, 2018). Een andere mogelijke verklaring is dat er onvoldoende capaciteit is door prioritering van andere zaken binnen de politie (Huisman et al., 2016).

Mijn beleidsaanbeveling zou zijn om de prioriteiten binnen de politie meer te gaan verleggen naar cybercriminaliteit, mede gezien de toename van het aantal cybercriminaliteitsdelicten (mede door de coronacrisis) en de opkomende technologieën, zoals AI en IoT (Taveres et al., 2020). Deze verlegging moet gebaseerd zijn op onderzoeken die bijvoorbeeld de impact van cybercriminaliteitsdelicten en traditionele delicten naast elkaar leggen, zoals in dit onderzoek is gedaan. Op basis van deze onderzoeken kunnen de juiste prioriteiten worden gesteld binnen de politie. Dit zou kunnen betekenen dat politiemedewerkers in de basisteams zich steeds meer bezig houden met cybercriminaliteit en kennis ontwikkelen over cybercriminaliteit, omdat de impact en/of behoefte hiervan relevanter is dan de kennis over traditionele criminaliteit.

De opzet en inrichting van de basisteams bij de Nationale Politie zijn gebaseerd op het uitgangspunt dat leden van het team ‘breed inzetbaar’ moeten zijn en dat er is geprobeerd de teams flexibeler te maken, zodat zij adequater kunnen reageren op vragen en problemen (Terpstra et al.,2016, p.55). Deze ‘breed inzetbaarheid’ van de basisteams zal volgens Stol (2018) waarschijnlijk tekort schieten op het gebied van cybercriminaliteit. Vanuit een bestuurskundig perspectief is daarom aan te bevelen om onderzoek te doen naar de opzet en inrichting binnen de basisteams ten aanzien van cybercriminaliteit.

Verder is het aanbevelingswaard om onderzoek te doen naar de manier van ‘sturing’ in de basisteams ten aanzien van cybercriminaliteit. Donald Schön (1983) heeft in zijn studie een moeras-metafoor geïntroduceerd rond het belang van reflectie voor professioneel handelen. Hierbij maakt hij de vergelijking tussen de ‘hoge gronden’ en de ‘moerassige laaglanden’ (Kunneman, 2012, pp 31-32).

“*In the varied topography of professional practise, there is a high, hard ground where practitioners can make effective use of research-based theory and technique, and there is a swampy lowland where situations are confusing ‘messes’ incapable of technical solution. The*

difficulty is that the problems of the high ground, however great their interest, are often relatively unimportant to clients or the larger society, while the swamp are the problems greatest human concern" (Schön, 1983, p. 42).

De metafoor van Schön (1983) zou een probleem kunnen zijn tussen het professioneel handelen van de politiemedewerkers in de basisteams ten aanzien van cybercriminaliteit en de wensen en sturing vanuit de 'hoge gronden' bij de Nationale Politie.

Literatuur

Bonanno, R. A., & Hymel, S. (2013). Cyber Bullying and Internalizing Difficulties: Above and Beyond the Impact of Traditional Forms of Bullying. *Journal of Youth and Adolescence*, *42*(5), 685–697. https://doi.org/10.1007/s10964-013-9937-1

Borwell, J., Jansen, J., & Stol, W. (2021). The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory. *Social Science Computer Review*, 1–22. https://doi.org/10.1177/0894439320983828

Bryman, D. S. S. A., Bryman, O. O. A. S. R. A., Bell, P. P. P. E. A., Bell, E. P. P. O. A., & Teevan, J. J. (2012). *Social Research Methods*. Oxford University Press.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47–S59. https://doi.org/10.1080/14616696.2020.1804973

Button, M., Lewis, C., & Tapley, J. (2012). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54. https://doi.org/10.1057/sj.2012.11

Button, M., Sugiura, L., Blackbourn, D., Kapend, R., Shepherd, D., & Wang, V. (2020, april). *Victims of Computer Misuse Main Findings*. University of Portsmouth. https://www.researchgate.net/publication/341179558_Victims_of_Computer_Misuse_Main_Findings

Campbell, R. (2008). The psychological impact of rape victims. *American Psychologist*, *63*(8), 702–717. https://doi.org/10.1037/0003-066x.63.8.702

Centraal Bureau voor de Statistiek. (2020a, maart). *Veiligheidsmonitor 2019*. https://www.cbs.nl/nl-nl/publicatie/2020/10/veiligheidsmonitor-2019

Centraal Bureau voor de Statistiek. (2020b, maart 2). *Minder traditionele criminaliteit, meer cybercrime*. https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime

Centraal Bureau voor de Statistiek. (2020c, oktober 2). *Innovatief onderzoek naar slachtoffers van high impact crimes*. https://www.cbs.nl/nl-nl/over-ons/innovatie/project/innovatief-onderzoek-naar-slachtoffers-van-high-impact-crimes

CheckMarket. (z.d.). *Steekproefcalculator*. Geraadpleegd op 7 augustus 2021, van https://nl.checkmarket.com/steekproefcalculator/

Cohen, M. A. (1988). Pain, Suffering, and Jury Awards: A Study of the Cost of Crime to Victims. *Law & Society Review*, *22*(3), 537. https://doi.org/10.2307/3053629

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, 1–14. https://eprints.qut.edu.au/98343/

CyberScienceCenter. (z.d.). *Safety, Security and Law Enforcement in a Digital Society | Cyber Science Center*. Geraadpleegd op 6 april 2021, van https://cybersciencecenter.nl/over-csc/

Dillman, D. A., & D. (1999). *Mail and Internet Surveys* (2de ed.). Wiley.

Dillman, D. A., Tortora, R. D., & Conradt, J. (1998). Influence of plain vs. fance Design on response rates for web surveys. *Influence of plain vs. fance Design on response rates for web surveys*, 1–6. https://subsites.sesrc.wsu.edu/dillman/papers/1998/influenceofplain.pdf

Dinisman, T., & Moroz, A. (2017). Understanding victims of crime: The impact of the crime and support needs. *Victim Support*, 1–41. https://doi.org/10.13140/RG.2.2.17335.73124

Enalyzer. (z.d.). *Homepage | Enalyzer*. Geraadpleegd op 7 augustus 2021, van https://www.enalyzer.com/nl/

Erdogan, B., & Baker, M. J. (2002). Increasing Mail Survey Response Rates from an Industrial Population. *Industrial Marketing Management*, *31*(1), 65–73. https://doi.org/10.1016/s0019-8501(00)00117-6

Federale Politie. (2018, 19 oktober). *Phishing, smishing en vishing*. https://www.politie.be/5998/nl/nieuws/phishing-smishing-en-vishing

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online Social Networks: Threats and Solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), 2019–2036. https://doi.org/10.1109/comst.2014.2321628

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud & Security*, *2015*(10), 5–12. https://doi.org/10.1016/s1361-3723(15)30093-2

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

Hassan, Z. A., Schattner, P., & Mazza, D. (2006). Doing a Pilot Study: Why is it Essential. *Doing a Pilot Study: Why is it Essential*. Published. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4453116/

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence Based Nursing*, *18*(3), 66–67. https://doi.org/10.1136/eb-2015-102129

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative Research Methods*. SAGE Publications.

Heo, M., Kim, N., & Faith, M. S. (2015). Statistical power as a function of Cronbach alpha of instrument questionnaire items. *BMC Medical Research Methodology*, *15*(1). https://doi.org/10.1186/s12874-015-0070-6

Huisman, S., Princen, M., Klerks, P., & Kop, N. (2016). *Handelen naar waarheid*. Politieacademie. https://www.politieacademie.nl/Documents/160608%2016-048%20Handelen%20naar%20waarheid.pdf

IBM. (z.d.). *SPSS Statistics*. IBM SPSS Statistics. Geraadpleegd op 7 augustus 2021, van https://www.ibm.com/products/spss-statistics

In, J. (2017). Introduction of a pilot study. *Korean Journal of Anesthesiology*, *70*(6), 601. https://doi.org/10.4097/kjae.2017.70.6.601

Jansen, J., & Leukfeldt, R. (2017). Coping with Cybercrime Victimization: An Exploratory Study into the Impact and Change. *2018 | Volume 6, Issue 2*. Published. https://doi.org/10.21428/88de04a1.976bcaf6

Kanayama, T. (2017). Impact of Cybercrime in Japan - Findings of Cybercrime Victimization Survey. *Sociology Study*, *7*(6). https://doi.org/10.17265/2159-5526/2017.06.004

KBO-PCOB. (2019, 20 december). *Babbeltrucplegers hebben senioren in het vizier*. https://www.kbo-pcob.nl/nieuws/babbeltrucplegers-hebben-senioren-in-het-vizier/

Kerr, J., Button, M., McNaugthon Nicholls, C., & Owen, R. (2013, januari). *Research on Sentencing Online Fraud Offences*. https://www.sentencingcouncil.org.uk/wp-content/uploads/Research_on_sentencing_online_fraud_offences.pdf

Knijf, E. (2011, oktober). *Slachtoffers van woninginbraak*. CVV. https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Woninginbraak/Documenten/Slachtoffers_van_woninginbraak/onderzoek_tevredenheid_slachtoffers_woninginbraak.pdf

Kunneman, H. (2012). *Het belang van moreel kapitaal in zorg en welzijn*. Stichting Paul Cremerslezing.

Kwok, A. O. J., & Koh, S. G. M. (2020). Deepfake: a social construction of technology perspective. *Current Issues in Tourism*, *24*(13), 1798–1802. https://doi.org/10.1080/13683500.2020.1738357

Lamet, W., & Wittebrood, K. (2009). *Nooit meer dezelfde: gevolgen van misdrijven voor slachtoffers*. Sociaal en Cultureel Planbureau. https://pure.uva.nl/ws/files/750078/81861_317355.pdf

Lee, S. (2018). The Moderating Effect between Cyber Victimization and Cyber Offending. *Korean Association of Victimology*, *26*(1), 99–120. https://doi.org/10.36220/kjv.2018.26.1.99

Leukfeldt, R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. NSCR.

https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y

Leukfeldt, R., & Weulen Kranenbarg, M. (2017). De menselijke factor in cybercrime. *Tijdschrift voor Criminologie*, *59*(3), 282–290. https://doi.org/10.5553/tvc/0165182x2017059003004

Maguire, M. (1991). The Needs and Rights of Victims of Crime. *Crime and Justice*, *14*, 363–433. https://doi.org/10.1086/449190

Mara, C. A., & Cribbie, R. A. (2012). Paired-Samples Tests of Equivalence. *Communications in Statistics - Simulation and Computation*, *41*(10), 1928–1943. https://doi.org/10.1080/03610918.2011.626545

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

Miller, T. R., Cohen, M. A., Wiersema, B., & National Institute of Justice (U.S.). (1996). *Victim Costs and Consequences*. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Ministerie van Algemene Zaken. (2021, 19 februari). *Januari 2020: Eerste signalen corona*. Coronavirus tijdlijn | Rijksoverheid.nl. https://www.rijksoverheid.nl/onderwerpen/coronavirus-tijdlijn/januari-2020-eerste-signalen-corona

Ministerie van Economische Zaken, Schippers, N., & Hengstz, K. (2020, oktober). *Veilig Online 2020*. Ministerie van Economische Zaken en Klimaat. https://www.rijksoverheid.nl/documenten/rapporten/2020/09/30/veilig-online-2020

Ministerie van Justitie en Veiligheid. (2020, 29 juni). *Grapperhaus: Ontwikkeling digitale dreiging Nederland is zorgwekkend*. Nieuwsbericht | Rijksoverheid.nl. https://www.rijksoverheid.nl/actueel/nieuws/2020/06/29/grapperhaus-ontwikkeling-digitale-dreiging-nederland-is-zorgwekkend

Ministerie van Justitie en Veiligheid. (2021, 13 april). *Samenwerken bij aanpak helpdeskfraude werkt*. Nieuwsbericht | Openbaar Ministerie.

https://www.om.nl/actueel/nieuws/2021/03/08/samenwerken-bij-aanpak-helpdeskfraude-werkt

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

Morrall, P., Marschall, P., Pattison, S., & Macdonald, G. (2010). Crime and health: a preliminary study into the effects of crime on the mental health of UK university students. *Journal of Psychiatric and Mental Health Nursing*, *17*(9), 821–828. https://doi.org/10.1111/j.1365-2850.2010.01594.x

Naezer, M. (2019). Jongeren, sexting en seksueel grensoverschrijdend gedrag. *Bijblijven*, *35*(6–7), 93–99. https://doi.org/10.1007/s12414-019-0057-z

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2019). *Cybersecuritybeeld Nederland*. Ministerie van Justitie en Veiligheid. https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019

NOS. (2017, 15 september). *"Kwart verkrachters niet gedreven door lust"*. https://nos.nl/artikel/2193128-kwart-verkrachters-niet-gedreven-door-lust

NU.nl. (2020, 17 februari). *Banken melden 5,3 miljoen euro schade in twee jaar door helpdeskfraude*. NU - Het laatste nieuws het eerst op NU.nl. https://www.nu.nl/tech/6030194/banken-melden-53-miljoen-euro-schade-in-twee-jaar-door-helpdeskfraude.html

NWO. (2020). *Cybersecurity-onderzoek aan universiteiten, wetenschappelijke kennisinstituten en hogescholen*. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/04/09/cybersecurity-onderzoek-aan-universiteiten-wetenschappelijke-kennisinstituten-en-hogescholen/bijlage-cybersecurity-onderzoek-aan-universiteiten-wetenschappelijke-kennisinstituten-en-hogescholen.pdf

Opstelten, I. W. (2013, april). *Aanpak High Impact Crimes*. Ministerie van Veiligheid en Justitie. https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Woninginbraak/Documenten/Aanpak_high_impact_crimes/aanpak-high-impact-crimes.pdf

Pallant, J. (2016). *SPSS Survival Manual*. McGraw-Hill Education.

Perren, S., Dooley, J., Shaw, T., & Cross, D. (2010). Bullying in school and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents. *Child and Adolescent Psychiatry and Mental Health*, *4*(1). https://doi.org/10.1186/1753-2000-4-28

Politie. (z.d.-a). *Babbeltruc*. politie.nl. Geraadpleegd op 19 april 2021, van https://www.politie.nl/themas/babbeltruc.html#alinea-title-hoe-herken-ik-een-babbeltruc-bij-een-pinautomaat

Politie. (z.d.-b). *Oplichting door nepbankmedewerkers*. Politie.nl. Geraadpleegd op 25 mei 2021, van https://www.politie.nl/binaries/content/assets/politie/onderwerpen/fraude/folder-bankhelpdeskfraude-2.pdf

Politie. (2021, 15 januari). *Criminaliteit 2020: minder inbraak, meer cybercrime*. politie.nl. https://www.politie.nl/nieuws/2021/januari/15/00-criminaliteit-2020-minder-inbraak-meer-cybercrime.html

Politieacademie. (2014, januari). *Babbeltrucs bij diefstal uit woning*. https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/89256.pdf

Price, M., Chin, M. A., Higa-McMillan, C., Kim, S., & Christopher Frueh, B. (2013). Prevalence and Internalizing Problems of Ethnoracially Diverse Victims of Traditional and Cyber Bullying. *School Mental Health*, *5*(4), 183–191. https://doi.org/10.1007/s12310-013-9104-6

Rijksoverheid. (2020). *VI Justitie en Veiligheid Rijksbegroting 2021*. https://www.rijksoverheid.nl/onderwerpen/prinsjesdag/documenten/begrotingen/2020/09/15/vi-justitie-en-veiligheid-rijksbegroting-2021

Sauermann, H., & Roach, M. (2012). Increasing Web Survey Response Rates in Innovation Research: An Experimental Study of Static and Dynamic Contact Design Features. *SSRN Electronic Journal*. Published. https://doi.org/10.2139/ssrn.1618295

Schon, D. A. & Basic Books. (1983). *Reflective Practitioner*. Adfo Books.

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

Spitzberg, B., & Gawron, J. (2016). Toward Online Linguistic Surveillance of Threatening Messages. *Journal of Digital Forensics, Security and Law*, 43–78. https://doi.org/10.15394/jdfsl.2016.1418

Stol, W. (2018). Politiewerk is . . . werken in een digitale samenleving. *Tijdschrift voor de Politie*, *80(5)*, 22–25. https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/94702.pdf

Tavares, J. M. R. S., Mishra, B. K., Khari, M., Kumar, R., & Zaman, N. (2020). *Handbook of E-Business Security*. Taylor & Francis.

Ten Boom, A., & Kuijpers, K. F. (2008). *Behoeften van slachtoffers van delicten*. WODC. https://repository.wodc.nl/bitstream/handle/20.500.12832/1211/ob262_volledige_tekst_tcm28-69141.pdf?sequence=2&isAllowed=y

Ten Voorde, J. (2017). Digitale seksuele delicten in het straf- en strafprocesrecht. *PROCES*, *96*(6), 407–421. https://doi.org/10.5553/proces/016500762017096006003

Terpstra, J. B., Van Duijneveldt, I., Eikenaar, T., Havinga, T., Stokkom, B. A. M., Van Duijneveldt, I., Programma Politie en Wetenschap (Apeldoorn), & Radboud Universiteit Nijmegen. (2016). *Basisteams in de Nationale Politie*. Politie & Wetenschap.

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Van der Bruggen, M. (2015). Een beschouwing van de ontwikkeling van het internet en cybercriminaliteit en de gevolgen hiervan voor de internationale bestrijding van digitale kinderporno. *Tijdschrift voor Criminologie*, *57*(2), 242–259. https://doi.org/10.5553/tvc/0165182x2015057002005

Van Erp, J., Stol, W., & Van Wilsem, J. (2013). Criminaliteit en criminologie in een gedigitaliseerde wereld. *Tijdschrift voor Criminologie*, *55*(4), 327–341. https://doi.org/10.5553/tvc/0165182x2013055004001

Van Thiel, S. (2020). *Bestuurskundig onderzoek* (Vol. 3). Coutinho.

Veenma, K., Batenburg, R., & Breedveld, E. (2004). *De Vignetmethode. Een praktische handreiking bij beleidsonderzoek.* Tilburg: IVA. https://docplayer.nl/55996268-Veenma-k-batenburg-r-breedveld-e-2004-de-vignetmethode-een-praktische-handreiking-bij-beleidsonderzoek-tilburg-iva.html

Veiligbankieren. (2021, 8 juni). *Phishing: alles wat u moet weten | Veilig bankieren*. https://www.veiligbankieren.nl/fraude/phishing-smishing/

Verhoeven, N. (2014). *Wat is onderzoek?* (5de ed.). Boom Lemma.

Wemmers, J. A. (2006). Reparation and the International Criminal Court: Meeting the Needs of Victims. *SSRN Electronic Journal*. Published. https://doi.org/10.2139/ssrn.3636291

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2017). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behavior*, *40*(1), 40–55. https://doi.org/10.1080/01639625.2017.1411030

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society*. SAGE Publications.

Bijlagen

Bijlage 1 – Uitnodigingsbrieven

1.1 Brief voor politiemedewerkers

[Datum]

Beste collega,

Wij nodigen je uit om mee te doen aan een onderzoek over de gevolgen van online en offline criminaliteit voor slachtoffers. Meedoen aan dit onderzoek is vrijwillig. Voordat je beslist of je wilt meedoen aan dit onderzoek, krijg je uitleg over wat het onderzoek inhoudt. Lees deze informatie rustig door en benader de onderzoeker (onderaan de brief) bij vragen.

Achtergrond en doel van het onderzoek
De Nationale Politie (Programma Digitalisering & Cybercrime) wil meer inzicht krijgen in de gevolgen van online en offline criminaliteit voor slachtoffers, en wat dit betekent voor de rol van de politie. Belangrijk onderdeel hiervan is zicht te krijgen op de perspectieven van Nederlandse burgers en politiemensen op dit thema. Het onderzoek kan bijdragen aan het vormgeven van de toekomstige rol van de politie in criminaliteitsbestrijding en slachtofferzorg voor online en offline criminaliteit. Jouw deelname is daarom zeer waardevol.

Dit deel van het onderzoek vindt plaats vanuit een samenwerking tussen de politie, gemeente Leeuwarden, NHL Stenden Hogeschool en Vrije Universiteit Amsterdam. De vragenlijsten worden voorgelegd aan leden van het burgerpanel van de gemeente Leeuwarden en medewerkers van de basisteams in de politie-eenheid Noord-Nederland, District Fryslân, Groningen en Drenthe.

Instructie
Om deel te nemen aan dit onderzoek, klik hier. De vragenlijst is het meest geschikt om in te vullen op de computer, maar kan ook op een smartphone worden ingevuld.

Inhoud van de vragenlijst
In de vragenlijst krijg je vier voorbeeldsituaties van slachtofferschap voorgelegd. Over deze situaties krijg je een aantal vragen. Daarnaast wordt aan het eind van de vragenlijst een aantal algemene vragen gesteld.

Tijd

Het beantwoorden van de vragenlijst zal ongeveer 10 minuten van je tijd in beslag nemen.

Vertrouwelijkheid van je gegevens

Je gegevens worden alleen gebruikt voor dit onderzoek en worden geanonimiseerd opgeslagen.

Heb je vragen?

Wanneer je vragen hebt over het onderzoek, de vragenlijst of ergens tegenaan loopt bij het invullen, dan kun je contact opnemen met het onderzoeksteam. Dit kan via [email] of [telefoonnummer]

Alvast hartelijk dank voor je deelname.

Met vriendelijke groet,

[redacted]

Cybercrimeteam Eenheid Noord-Nederland/ Cyber Science Center

1.2 Brief voor burgerpanel Leeuwarden

[Datum]

Geachte heer/mevrouw,

Wij nodigen u uit om mee te doen aan een onderzoek over de gevolgen van online en offline criminaliteit voor slachtoffers. Meedoen aan dit onderzoek is vrijwillig. Voordat u beslist of u wilt meedoen aan dit onderzoek, krijgt u uitleg over wat het onderzoek inhoudt. Lees deze informatie rustig door. U kunt het onderzoeksteam of de gemeente Leeuwarden (onderaan de brief) benaderen bij vragen.

Achtergrond en doel van het onderzoek
De Nationale Politie (Programma Digitalisering & Cybercrime) wil meer inzicht krijgen in de gevolgen van online en offline criminaliteit voor slachtoffers, en wat dit betekent voor de rol van de politie. Belangrijk onderdeel hiervan is zicht te krijgen op de perspectieven van Nederlandse burgers en politiemensen op dit thema. Het onderzoek kan bijdragen aan het vormgeven van de toekomstige rol van de politie in criminaliteitsbestrijding en slachtofferzorg voor online en offline criminaliteit. Uw deelname is daarom zeer waardevol.

Dit deel van het onderzoek vindt plaats vanuit een samenwerking tussen de politie, gemeente Leeuwarden, NHL Stenden Hogeschool en Vrije Universiteit Amsterdam. De vragenlijsten worden voorgelegd aan leden van het burgerpanel van de gemeente Leeuwarden en medewerkers van de basisteams in de politie-eenheid Noord-Nederland, District Fryslân, Groningen en Drenthe.

Instructie
Om deel te nemen aan dit onderzoek, klik hier. De vragenlijst is het meest geschikt om in te vullen op de computer, maar kan ook op een smartphone worden ingevuld.

Inhoud van de vragenlijst
In de vragenlijst krijgt u vier voorbeeldsituaties van slachtofferschap voorgelegd. Over deze situaties krijgt u een aantal vragen. Daarnaast wordt aan het eind van de vragenlijst een aantal algemene vragen gesteld.

Tijd
Het beantwoorden van de vragenlijst zal ongeveer 10 minuten van uw tijd in beslag nemen.

Vertrouwelijkheid van uw gegevens

Uw gegevens worden alleen gebruikt voor dit onderzoek en worden geanonimiseerd opgeslagen.

Heeft u vragen?

Wanneer u vragen heeft over de inhoud van het onderzoek kunt contact opnemen met het onderzoeksteam. Dit kan via [email]. Voor overige vragen kunt u contact opnemen met de gemeente Leeuwarden. Dit kan via onderzoek@leeuwarden.nl.

Alvast hartelijk dank voor uw deelname.

Met vriendelijke groet,

[Handtekening]
[Naam]
[Functie]

Bijlage 2 – Vragenlijst

2.1 Introductie

Hartelijk dank voor uw deelname aan dit onderzoek.

U krijgt enkele voorbeeldsituaties te zien. Daarna krijgt u vragen hierover.
Het is belangrijk dat u de situatie **eerst goed doorleest** voordat u de vragen beantwoordt.

Veel succes!

N.B. Per situatie worden dezelfde vragen gesteld. Dit kan wat vreemd overkomen, maar is nodig om betrouwbare resultaten te verkrijgen.

2.2 Vignetten

Situatie 1: Hacken van online bankaccount

Meneer Hulst (45 jaar), ambtenaar bij de provincie, werd op 20 maart 2021 benaderd door zijn bank. Althans dat dacht hij. Meneer Hulst ontving een sms, waarin stond:

“je ING-app is uit veiligheidsoverwegingen geblokkeerd. Klik op de link om weer toegang te krijgen: ing-bankieren.com/?31622463403”

Meneer Hulst klikte op de link. Hiermee kwam hij op een scherm dat precies leek op het vertrouwde scherm van zijn bank. Er werd gevraagd naar zijn inloggegevens. Nietsvermoedend vulde meneer Hulst deze in.

Het ‘bekende’ scherm bleek echter een nagemaakte website van zijn bank. De daders onderschepten de gegevens van meneer Hulst en logden in op zijn echte bankaccount. Uiteindelijk is er €25.000,- van zijn spaarrekening gestolen.

Meneer Hulst kreeg de schade niet vergoed via zijn verzekering of bank.

Situatie 2: Wraakporno

Isabel (19 jaar) zit in haar laatste middelbare schooljaar van het VWO. Daarnaast heeft ze een bijbaan in de horeca.

In haar wiskundeklas zit haar ex-vriend (ook 19 jaar). Tijdens hun relatie heeft Isabel een keer naaktfoto's van haar billen en borsten naar hem gestuurd.

Haar ex-vriend heeft deze foto’s zonder haar toestemming online gezet op een sociale media-account. De klasgenoten van wiskunde konden hierdoor de naaktfoto's zien.

Situatie 3: Woninginbraak

Meneer Hulst (45 jaar), ambtenaar bij de provincie, is slachtoffer geworden van woninginbraak. Meneer Hulst was tijdens de inbraak niet thuis

De daders hadden aan de achterzijde van de woning een raam ingeslagen. Via dit raam hebben de daders de woning betreden. Uiteindelijk zijn er goederen en geld weggenomen ter waarde van €25.000,-.

Meneer Hulst kreeg de schade niet vergoed via zijn verzekering of bank.

Situatie 4: Aanranding

Isabel (19 jaar) zit in haar laatste middelbare schooljaar van het VWO. Daarnaast heeft ze een bijbaan in de horeca.

In haar wiskundeklas zit een jongen (ook 19 jaar) die haar herhaaldelijk aanraakt zonder dat zij dat wil. Dit begon met tikken op haar schouder en rug. Later waren deze tikken niet meer op haar schouder of rug, maar raakte de jongen steeds meer haar billen en borsten aan.

Ook buiten de wiskundeklas heeft hij haar een keer op deze manier aangeraakt en vervolgens daarover verhalen verteld aan de rest van de wiskundeklas.

2.3 Vragen over vignetten

Deel 1:
Onderstaande vragen gaan over hoe waarschijnlijk u het vindt dat [persoon X] (leeftijd, delict) door het delict bepaalde gevolgen ervaart.

Hoe waarschijnlijk is het volgens u dat [persoon X] door dit delict…

		Zeer onwaarschijnlijk	Onwaarschijnlijk	Misschien	Waarschijnlijk	Zeer waarschijnlijk
		1	*2*	*3*	*4*	*5*
1	Depressieve klachten ervaart? (Zoals somberheid en lusteloosheid)	O	O	O	O	O
2	Boosheid ervaart?	O	O	O	O	O
3	Afname van zijn zelfvertrouwen ervaart?	O	O	O	O	O
4	Angst ervaart om nog eens slachtoffer te worden van hetzelfde delict?	O	O	O	O	O
5	Gevoelens van schuld en schaamte ervaart?	O	O	O	O	O
6	Slaapproblemen ervaart?	O	O	O	O	O
7	Paniek- of angst gerelateerde lichamelijke klachten ervaart? (Zoals hartkloppingen, trillen, zweten, benauwdheid)	O	O	O	O	O
8	Een afname van vertrouwen in andere mensen ervaart?	O	O	O	O	O
9	Vermijdingsgedrag vertoont? (Zoals het vermijden van fysieke plaatsen en/of online platformen)	O	O	O	O	O
10	Minder of niet meer werkt?	O	O	O	O	O
11	Financiële schade had om de gevolgen van het delict op te lossen (bijvoorbeeld om een bedrijf in te schakelen)?	O	O	O	O	O

Deel 2:
Onderstaande vragen gaan over hoe waarschijnlijk u het vindt dat [persoon X] (leeftijd, delict) door het delict bepaalde behoeften heeft.

Hoe waarschijnlijk is het volgens u dat [persoon X] door dit delict behoefte heeft aan …

		Zeer onwaarschijnlijk	Onwaarschijnlijk	Misschien	Waarschijnlijk	Zeer waarschijnlijk
		1	*2*	*3*	*4*	*5*
1	Financiële compensatie voor de geleden schade?	O	O	O	O	O
2	Emotionele steun? (Zoals iemand om mee te praten)	O	O	O	O	O
3	Duidelijkheid over hoe het delict heeft kunnen plaatsvinden?	O	O	O	O	O
4	Aanhouding van de dader?	O	O	O	O	O
5	Contact met de politie?	O	O	O	O	O
6	Informatie over het eventuele politieonderzoek?	O	O	O	O	O
7	Tips om toekomstig slachtofferschap te voorkomen?	O	O	O	O	O
8	Meehelpen te voorkomen dat andere mensen slachtoffer worden van hetzelfde delict?	O	O	O	O	O
9	Serieus genomen worden als slachtoffer door instanties zoals de politie?	O	O	O	O	O
10	Hulp bij het oplossen van door het delict ontstane praktische problemen?	O	O	O	O	O

Deel 3:

Burgers kunnen bepaalde behoeftes hebben, nadat zij slachtoffer zijn geworden van dit delict. Onderstaande vragen gaan over hoe waarschijnlijk het volgens u is dat de politie in deze behoeftes kan voorzien voor [persoon X] (leeftijd, delict)

Hoe waarschijnlijk is het volgens u dat de politie in deze behoefte kan voorzien voor [persoon X]?

		Zeer onwaarschijnlijk	Onwaarschijnlijk	Misschien	Waarschijnlijk	Zeer waarschijnlijk
		1	*2*	*3*	*4*	*5*
1	Financiële compensatie voor de geleden schade	O	O	O	O	O
2	Emotionele steun (Zoals iemand om mee te praten)	O	O	O	O	O
3	Duidelijkheid over hoe het delict heeft kunnen plaatsvinden	O	O	O	O	O
4	Aanhouding van de dader	O	O	O	O	O

5	Contact met de politie	O	O	O	O	O
6	Informatie over het eventuele politieonderzoek	O	O	O	O	O
7	Tips om toekomstig slachtofferschap te voorkomen	O	O	O	O	O
8	Meehelpen te voorkomen dat andere mensen slachtoffer worden van hetzelfde delict	O	O	O	O	O
9	Serieus genomen worden als slachtoffer	O	O	O	O	O
10	Hulp bij het oplossen van door het delict ontstane praktische problemen?	O	O	O	O	O

2.4 Algemene vragen

1. Met welk geslacht identificeert u zichzelf?

- Man
- Vrouw
- Beide
- Geen van beide

2. Wat is uw geboortejaar?

[*jjjj*]

3. Wat is de hoogste opleiding die u heeft afgerond met een diploma, akte of getuigschrift?

- Geen opleiding
- Lagere school (incl. speciaal onderwijs, bijv. LOM, BLO, etc.)
- 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, semiwetenschappelijk onderwijs
- Doctoraat
- Geen antwoord

4. Welke omschrijving past het beste bij u?
(Kies de situatie die het best bij u past)

- Werkende met betaald werk/ zelfstandige
- Werkloos/ werkzoekende
- Vrijwilliger
- Arbeidsongeschikt
- Scholier of studerende
- Huisman/ huisvrouw
- Gepensioneerd of met de VUT
- Geen van deze
- Geen antwoord

5. Bent u *ooit* slachtoffer geworden van criminaliteit?
[Meerdere antwoorden mogelijk]

- Ja, van offline criminaliteit [ga door naar vraag 5]
- Ja, van online criminaliteit [ga door naar vraag 6]
- Nee [ga door naar vraag 10]

6. Van welk(e) offline delict(en) bent u ooit slachtoffer geworden?
[Meerdere antwoorden mogelijk]

- Woninginbraak
- Aanranding
- Anders, namelijk …
- Zeg ik liever niet

7. Van welk(e) online delict(en) bent u ooit slachtoffer geworden?
[Meerdere antwoorden mogelijk]

- Hacken van online bankaccount
- Wraakporno
- Anders, namelijk …
- Zeg ik liever niet

8. Bent u *in de afgelopen 12 maanden* slachtoffer geworden van criminaliteit?

- Ja, van offline criminaliteit [ga door naar vraag 8]
- Ja, van online criminaliteit [ga door naar vraag 9]
- Nee [ga door naar vraag 10]

9. **Van welk(e) offline delict(en) bent u in de afgelopen 12 maanden slachtoffer geworden?**
   [Meerdere antwoorden mogelijk]

- o Woninginbraak
- o Aanranding
- o Anders, namelijk …
- o Zeg ik liever niet

10. **Van welk(e) online delict(en) bent u in de afgelopen 12 maanden slachtoffer geworden?**
    [Meerdere antwoorden mogelijk]

- o Hacken van online bankaccount
- o Wraakporno
- o Anders, namelijk …
- o Zeg ik liever niet

[Extra vragen voor respondenten van politie]

11. **Waar bent u werkzaam?**

- o Basisteam in district Fryslân (team A1 t/m A6)
- O Basisteam in district Groningen (team B1 t/m B7)
- O Basisteam in district Drenthe (team C1 t/m C3)
- o Anders, namelijk …

12. **Waaruit bestaan uw voornaamste werkzaamheden?**

- o GGP/noodhulp
- o Intake & Service
- o Crimeteam/opsporing
- o Leiding
- o Anders, namelijk …

13. **Wat is uw functie?**

- o Generalist GGP
- o Senior GGP – Wijkagent
- o Senior GGP – Overig
- o Medewerker Intake & Service
- o Senior Tactische Opsporing
- o Operationeel Specialist
- o Operationeel Expert
- o Teamchef
- o Aspirant/stagiair
- o Anders, namelijk ….