POLITIE & Wetenschap

Online Blauw

Een onderzoek naar de rol van basisteams in de aanpak van digitale criminaliteit en ervaringen van slachtoffers met de politie

Dr. Ronald van Steden
Drs. Sandra ter Woerds
André Merk
Drs. Kristiaan Schuppers
Drs. Melissa Willekers
Daphne Valk-van Waarde MSc
Roselle Jansen MSc
Prof. dr. Stijn Ruiter

nscr Netherlands Institute for the Study of Crime and Law Enforcement
VU VRIJE UNIVERSITEIT AMSTERDAM Faculteit der Rechtsgeleerdheid
POLITIE

Online blauw

Online Blauw

Een onderzoek naar de rol van basisteams in de aanpak van digitale criminaliteit en ervaringen van slachtoffers met de politie

Dr. Ronald van Steden (VU, NSCR)
Drs. Sandra ter Woerds, André Merk (politie, eenheid Amsterdam)
Drs. Kristiaan Schuppers, drs. Melissa Willekers (politie, eenheid Den Haag)
Daphne Valk-van Waarde Msc (VU)
Roselle Jansen MSc en prof. dr. Stijn Ruiter (NSCR)

Sdu Lefebvre, juni 2025

POLITIE & Wetenschap

nscr Netherlands Institute for the Study of Crime and Law Enforcement

VU VRIJE UNIVERSITEIT AMSTERDAM

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:
Lefebvre Sdu Klantenservice
telefoon: 070 - 378 98 80
website: www.sdu.nl/service

Omslagontwerp: Imago Mediabuilders, Amersfoort
Afbeelding omslag: ANP foto

ISBN: 9789012410991
NUR: 600

Inhoudsopgave

1. Inleiding

1.1 Een 'digitale transformatie'

1.1.1 *Toenemend slachtofferschap van digitale criminaliteit*

Terwijl de registratie van traditionele ('offline') criminaliteit al jaren daalt, worden burgers en bedrijven in toenemende mate het slachtoffer van digitale ('online') criminaliteit. Deze ontwikkeling heeft te maken heeft met een lage pakkans afgezet tegen een verwachte hoge opbrengst (De Cuyper & Weijters, 2016). In 2023 was 16% van de bevolking van 15 jaar of ouder in de afgelopen twaalf maanden slachtoffer van een of meerdere vormen van digitale criminaliteit. Online aankoopfraude en oplichting zijn het grootste probleem, naast hacken en persoonsgerichte delicten, zoals online bedreiging en intimidatie. Gemiddeld doen slechts twee op de tien slachtoffers aangifte of melding bij de politie. Hierbij geldt dat hoe groter de ernst van de zaak, hoe groter de kans dat er een aangifte volgt (Akkermans et al., 2024). Uit een fenomeenbeeld van de politie blijkt dat in 2023 online fraude alleen al voor minimaal 109 miljoen euro aan schade zorgde (Politie, 2024a).

Minstens 21% van de slachtoffers van digitale criminaliteit ondervindt hiervan serieuze gevolgen (Akkermans et al., 2024). Dan gaat het bijvoorbeeld om financiële problemen, maar ook om emotionele impact, zoals schaamte en angst (Borwell et al., 2021, 2022). Daarom hebben deze slachtoffers behoefte aan erkenning, serieus worden genomen, praktisch advies, enzovoort (Borwell et al., 2024). Hun perspectief is voor basisteams belangrijk, omdat daar een substantieel deel van de aangiften en meldingen van slachtoffers van digitale criminaliteit binnenkomt. Naast dat dit onderzoek zich richt op de praktijken van basisteams met betrekking tot digitale criminaliteit, brengt het de gevolgen van digitale delicten voor slachtoffers, hun behoeften hierbij en de mate van tevredenheid die zij over de politie ervaren in beeld.

1.1.2 *Worsteling bij de politie*

De relevantie van dit onderzoek is dat de politie worstelt met de digitalisering van de samenleving en met de aanpak van digitale criminaliteit. Zoals Van Hoorn en Van Dijk schrijven:

> *'De politie moet zich vanzelfsprekend voortdurend aanpassen aan nieuwe ontwikkelingen en vragen vanuit de samenleving, waarvan de verdergaande verwevenheid van fysiek en digitaal de belangrijkste is. Daarbij is het zelden zo dat met het nieuwe het oude verdwijnt. De politie moet met nieuwe technologie aan de slag – zonder het menselijke te verliezen; ze moet digitaal actief zijn – zonder uit de fysieke wereld te verdwijnen; ze moet nationaal en internationaal aan de slag – zonder het lokale te laten verwateren; ze moet samenwerken met allerhande externe partijen en partners – zonder het eigene op te geven.'* (2024: 3)

Onder de noemer 'digitale transformatie' zet de politie nadrukkelijk in op de bestrijding van online vormen van criminaliteit door innovatieve vormen van werken te ontwikkelen (Landman, 2023; Stol et al., 2024). Landelijk lopen er meerdere initiatieven, projecten en acties die zich specifiek richten op het beter toerusten van de basispolitiezorg bij het bestrijden van digitale criminaliteit. Zo bestaan er CyberCentres die als hulploket voorlichting geven aan intake- en servicemedewerkers (I&S) (Boekhoorn, 2019). Ook zijn digitaal wijkagenten actief en investeert de politie in online gegevensvergaring (Boelens & Landman, 2021; Landman & Groothuis, 2022). Verder heeft de politie digitale districten, digitale flexteams, digi-kamers en cybersupportteams opgericht. En met taakaccenthouders cyber, IT-coaches en cybervrijwilligers zijn er binnen de politie specialistische functionarissen met digitale expertise werkzaam (Broekhuizen et al., 2022; Schiks et al., 2022).

Sinds 2022 richt Operatie Centurion zich op het bestrijden van veelvoorkomende digitale criminaliteit (aan- en verkoopfraude, bankhelpdeskfraude, hulpvraagfraude en bankphishing), op het voldoen aan de behoeften van slachtoffers, en op het verbeteren van de afhandeling van strafzaken (Van der Plas & Hagenaars, 2021). Hierbij zet de politie in op publiek-private samenwerking met het Openbaar Ministerie (OM), gemeenten, banken en de telecomsector om digitale criminaliteit tegen te gaan. Toch is de stap naar 'online blauw' – een lokale politie die is toegerust voor de aanpak van digitale criminaliteit, waaronder fraude, bedreiging en chantage – niet zomaar gezet. Het gebruikelijke politierepertoire schiet vaak tekort in een snel digitaliserende samenleving. Ook is de organisatie zelf nog niet afdoende ingericht op hoe effectief met digitale delicten om te gaan (Leukfeldt et al., 2013). Eerder wees de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) erop dat

> *'[d]e klassieke politiefunctie en het klassieke politiewerk zijn […] vormgegeven vanuit een fysieke, soevereine staat waarin het gedrag van mensen binnen die fysieke ruimte gereguleerd moet worden, en de orde in diezelfde fysieke ruimte moet worden gehandhaafd.'* (Bijleveld et al., 2021: 31)

Hierdoor krijgt het handhaven van de orde op straat meestal meer aandacht dan het reguleren van de online wereld.

1.2 Basisteams en digitale criminaliteit

Van basisteams in het bijzonder wordt verwacht dat ze actief zijn in zowel de fysieke als de digitale wereld. Het lokale 'blauwe vak', dicht bij burgers en in wijken, is immers van groot belang als eerste aanspreekpunt voor criminaliteit en onveiligheid (Van Steden et al., 2021). De in- en doorstroom van aangiften en meldingen op basisteams gaat echter niet vanzelf, omdat de dynamiek van delicten en problemen waarop teams zich moeten richten flink is veranderd (Terpstra et al., 2021). Hetzelfde geldt voor de behoeften en verwachtingen van burgers over wat de politie doet en kan (Dekker et al., 2024). Daarbij komt dat de deskundigheid en vaardigheden van politiemedewerkers op peil dient te worden gehouden. Uit eerder onderzoek blijkt dat I&S-medewerkers op basisteams en bij RSC's aangiften of meldingen van digitale criminaliteit niet altijd adequaat opnemen en registreren (Bureau Beke, 2024; Ruiter et al., 2024; Van Steden et al., 2023). Soms schatten zij de strafbaarheid van een delict of de ernst voor het slachtoffer (te) laag in. Ook hebben I&S-medewerkers regelmatig te weinig specialistische kennis van alle technische aspecten van digitale criminaliteit. Daardoor lukt het niet altijd om succesvol een aangifte op te nemen en een proces-verbaal op te maken (Boekhoorn, 2019). Het gevolg kan zijn dat een solide basis voor verder opsporingsonderzoek ontbreekt. Dit gebrek aan specialistische kennis en kunde geldt deels ook voor casescreeners bij de afdeling veelvoorkomende criminaliteit (VVC) (Ruiter et al., 2024).

Het hierboven geschetste beeld van gebrekkige kennis en kunde bij I&S-medewerkers, maar ook bij politiemensen in uniformdienst en bij rechercheonderdelen, wordt in andere publicaties bevestigd. Hoewel er inmiddels stappen voorwaarts zijn gezet, komt onder andere naar voren dat het herkennen van online strafbare gedragingen, het optreden op een plaats delict en het gebruik van digitale hulpmiddelen in de opsporing voor verbetering vatbaar zijn (Jansen et al., 2020; Politieonderwijsraad, 2020). Complicerende factoren zijn dat veel fysieke criminaliteit tegenwoordig in meer of mindere mate ook een digitale component heeft (Boekhoorn, 2019; Roks et al., 2021; Schiks et al., 2022) en dat online vormen van criminaliteit regelmatig het werkgebied van een basisteam overstijgen. Daders en dadergroepen kunnen in korte tijd door het hele land seriematig en op grote schaal slachtoffers maken. Soms opereren plegers van strafbare feiten vanuit het buitenland (Domenie et al., 2013; Jansen et al., 2019; Van den Eeden et al., 2021). Vanwege het (inter)nationale karakter en de fluïditeit van digitale criminaliteit blijkt het niet gemakkelijk daders te pakken en te sanctioneren.

Een mogelijk gevolg is dat slachtoffers zich ontmoedigd voelen om aangifte of melding te doen bij de politie, omdat 'er toch niets mee gedaan wordt'. Als burgers zich niet begrepen en geholpen voelen, kan dit een negatieve invloed hebben op hun vertrouwen in de politie. Samenhangend met het laatste punt wijzen onderzoekers op een relatief lage meldings- en aangiftebereidheid bij digitale criminaliteit (Leukfeldt et al., 2018; Ruiter et al., 2024; Sipma & Van Leijsen, 2019) – al wisselt de aangiftebereidheid per type digitaal delict. Vanwege de geconstateerde lage meldings- en aangiftebereid-

heid is de omvang van digitale criminaliteit veel groter dan officiële politieregistraties en CBS-cijfers doen vermoeden.

Tegen deze achtergrond is het van belang dat basisteams meebewegen met veranderende vormen van criminaliteit. Spithoven en collega's wijzen op de noodzaak van meer bewustwording rond digitale criminaliteit en zij stellen dat er meer prioriteit zou moeten worden gegeven aan de aanpak hiervan. Dat vergt aanpassingen van de organisatie en personele de capaciteit, onder meer om de technische, praktische en juridische kennis onder politiemensen te verbeteren. Ook geven zij aan dat lokale aanspreekpunten (denk aan taakaccenthouders en digitaal wijkagenten) versterking zouden moeten krijgen om de informatiepositie van de politie te vergroten, de samenwerking met veiligheidspartners te intensiveren en slachtoffers beter te helpen (Kort & Spithoven, 2022; Spithoven et al., 2022). Voorwaar geen eenvoudige opgave! Het onderhavige onderzoek draagt bij aan handelingsperspectieven voor basisteams, met daarbij bijzondere aandacht voor het perspectief van slachtoffers van digitale criminaliteit. Hoewel er inmiddels studies bestaan naar *best practices* in de aanpak van digitale criminaliteit (Broekhuizen et al., 2022; Schiks et al., 2022), is de manier waarop basisteams verspreid over het land met dit soort criminaliteit omgaan onderbelicht gebleven.

1.3 Doel

Het doel van dit onderzoek is om inzichtelijk te maken in hoeverre en op welke wijze basisteams digitale criminaliteit afhandelen – en wat hieromtrent ervaringen van slachtoffers van digitale criminaliteit zijn. Naast zicht op hoe basisteams digitale criminaliteit verwerken, is het ook belangrijk om beter te begrijpen welke impact delicten op slachtoffers hebben, wat hun behoeften zijn en hoe tevreden zij over de politie zijn. Door de perspectieven van basisteams en van aangevers samen te brengen, krijgt de politie meer inzicht in haar eigen werkwijzen, in wat er goed gaat en in wat er beter kan.

1.4 Probleemstelling en onderzoeksvragen

De probleemstelling van het onderzoek luidt als volgt:
Hoe gaan basisteams binnen de politie om met digitale criminaliteit en wat is hierop het perspectief van slachtoffers?

Bijbehorende onderzoeksvragen zijn:
1. Wat is er in de wetenschappelijke literatuur bekend over definities, slachtofferschap en politiële aanpak van digitale criminaliteit op basisteams?
2. Hoe ziet het werkaanbod, de afhandeling en de opvolging van digitale criminaliteit er op basisteams in kwantitatieve zin uit?
3. Hoe is de aanpak van digitale criminaliteit binnen basisteams ingebed?

4. Hoe vindt de afhandeling van digitale criminaliteit op zaakniveau binnen basisteams plaats?
5. Wat is de impact van digitale criminaliteit op slachtoffers, welke behoeften hebben zij bij aangifte en hoe tevreden zijn zij met de politie na aangifte, in vergelijking met slachtoffers van traditionele vormen van criminaliteit?

1.5 Methodologie en zes deelstudies

Dit onderzoek is uitgevoerd tussen eind 2022 en medio 2024. Gelet op het dynamische karakter van digitale criminaliteit en de digitale transformatie binnen de politie kunnen zich sindsdien op punten enige veranderingen hebben voorgedaan. Die veranderingen komen waar nodig aan bod. Aan het onderzoek ligt een zogeheten *mixed-methods* benadering ten grondslag. Naast een inventarisatie van de wetenschappelijke literatuur is er gekozen voor zowel kwantitatieve als kwalitatieve deelstudies. Hieronder worden de zes deelstudies kort toegelicht.[1]

De eerste deelstudie, het genoemde literatuuronderzoek, heeft een korte weergave van wetenschappelijke publicaties en enkele beleidsstukken over digitale criminaliteit, (lokaal) politiewerk en slachtofferschap opgeleverd.
De tweede deelstudie, een quickscan, zoomt aan de hand van een steekproef van 600 zaken in op de aard, omvang en afhandeling van het landelijke werkaanbod van digitale criminaliteit binnen de politie, in het bijzonder de basisteams. Het gaat hier om de periode oktober 2022 tot en met september 2023.
Op basis van 54 geanonimiseerde interviews schetst de derde deelstudie de context en werkwijze van zes geanonimiseerde basisteams (Team Noord, Team Oost, Team Midden, Team Stad, Team Strand en Team Zee) ten aanzien van hun dagelijkse omgang met digitale criminaliteit.
Aan de hand van de gereconstrueerde 77 zaken focust de vierde deelstudie op hoe deze zes basisteams digitale criminaliteit in de praktijk afhandelen en opvolgen. De uitkomsten van de zaakreconstructies zijn met medewerkers van de basisteams besproken.
De vijfde deelstudie betreft een grootschalige survey onder 25.760 respondenten die aangiften van criminaliteit hebben gedaan en bevat een kwantitatieve analyse van de impact van specifiek digitale criminaliteit op slachtoffers, de behoeften van deze slachtoffers bij aangifte en hun tevredenheid over de politie. Ervaringen van slachtoffers van fysieke criminaliteit zijn vergeleken met slachtoffers van digitale criminaliteit.
De zesde en aanpalende deelstudie bevat zestien geanonimiseerde interviews met slachtoffers van digitale criminaliteit over dezelfde thema's: impact, behoeften en tevredenheid over de politie. Hun verhalen geven een kwalitatieve inkleuring van de kwantitatieve resultaten, zoals die uit genoemde survey naar voren komen.

1 Aan de verschillende deelstudies en hoofdstukken van dit rapport hebben verschillende auteurs bijgedragen. Hun bijdragen staan vermeld in Bijlage 1. De hierop volgende bijlagen bevatten gedetailleerde methodologie van de afzonderlijke deelstudies.

Tot slot zijn de uitkomsten van deze deelstudies gedeeld met vertegenwoordigers van de zes basisteams en met beleidsmakers binnen de politie. Dat gebeurde tijdens een reflectiesessie op 2 oktober 2024 te Utrecht. Daarnaast heeft het onderzoeksteam workshops gegeven op het wetenschapscongres van de Politieacademie (10 oktober 2024 te Apeldoorn) en op de landelijke vakdag Centurion (23 oktober 2024 te Soesterberg). Feedback die uit deze sessies voortkwam, is in de onderzoeksresultaten verwerkt.

1.6 Leeswijzer

Het onderzoeksrapport is als volgt opgezet. Hoofdstuk 2 bevat een literatuurstudie naar definities en categoriseringen van digitale criminaliteit, het slachtofferschap en de aanpak van dit type criminaliteit door de politie. Op basis van een landelijke kwantitatieve quickscan schetst hoofdstuk 3 de aard en omvang van het werkaanbod van digitale criminaliteit, de wijze van afhandeling en opvolging hiervan binnen de politie, specifiek op het niveau van basisteams. Hoofdstuk 4 zet de praktijk en de werkwijzen van zes basisteams rond de afhandeling van meldingen en aangiften van digitale criminaliteit centraal. Hoofdstuk 5 laat aan de hand de zaakreconstructies zien hoe die afhandeling er op zaakniveau uitziet. Hoofdstuk 6 combineert inzichten uit een kwantitatieve en kwalitatieve studie naar de ervaringen en perspectieven van slachtoffers van digitale criminaliteit. Afsluitend brengt hoofdstuk 7 alle resultaten samen door antwoord te geven op de gestelde onderzoeksvragen. De onderzoeksbevindingen bieden aanknopingspunten voor beleid en praktijk van de politie. Deze handreikingen komen ook in het laatste hoofdstuk aan bod.

2. Definities, slachtofferschap en politiële aanpak

2.1 Inleiding

Dit hoofdstuk bevat de uitkomsten van een literatuurstudie[2] naar definities en categorieën van digitale criminaliteit en slachtofferschap van dit type criminaliteit. Er bestaat in zowel de wetenschap als in de politiepraktijk onduidelijkheid over wat er precies onder digitale criminaliteit moet worden verstaan. Daarom is het eerste doel van dit hoofdstuk om meer inzicht te verschaffen in de verschillende begrippen (2.2) Het tweede doel is om de literatuur over slachtofferschap van digitale criminaliteit in beeld te brengen. Onderwerpen zijn de bereidheid van slachtoffers om al dan niet een aangifte of melding te doen, de persoonskenmerken van slachtoffers en de impact van een delict (2.3). Het derde en laatste doel is om de aanpak van digitale criminaliteit te beschrijven op nationaal, regionaal en lokaal niveau, met extra aandacht voor het laatste niveau waarop de basisteams opereren (2.4). Het hoofdstuk sluit af met een korte terugblik op bevindingen (2.5).

2.2 Definities

2.2.1 *Digitale criminaliteit nader omschreven*

Digitale criminaliteit is een dynamisch containerbegrip. Binnen de wetenschappelijke literatuur ontbreekt het aan een gemeenschappelijk conceptueel kader (Borwell en collega's, 2020; Spithoven, 2020; Stol, 2020). Auteurs gebruiken een heel arsenaal aan voorvoegsels door elkaar, zoals 'gedigitaliseerde', 'online', 'ICT-', 'internet-', 'computer-', 'cyber-' en 'hightech' criminaliteit – en ook 'e-crime' komt voor (Black en collega's, 2019; Donalds & Osei-Bryson, 2019; Holt & Bossler, 2020). Dit schept begripsverwarring en komt de aanpak en monitoring van digitale criminaliteit vanzelfsprekend niet ten goede. Hetzelfde geldt voor de noodzaak tot samenwerking en kennisuitwisseling tussen de politie en andere relevante partijen.

Akdemir en collega's (2020) hebben een poging gedaan om het debat rondom de conceptualisering van digitale criminaliteit in de wetenschappelijke literatuur te systema-

2 De methodologie en aanpak van deze literatuurstudie staat vermeld in Bijlage 2.

tiseren. Uit hun analyse blijkt dat de definities van Thomas en Loader (2000) en die van Gordon en Ford (2006) het meest in de wetenschappelijke literatuur worden geciteerd. Thomas en Loader definiëren digitale criminaliteit als *'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks'* (2000: 3). Gordon en Ford verstaan onder digitale criminaliteit simpelweg: *'any crime that is facilitated or committed using a computer, network, or hardware device'* (2006: 14). Beide definities benadrukken dat illegale activiteiten en criminele delicten met behulp van computers, computernetwerken en andere digitale technologie worden gepleegd. Dat is de kern van digitale criminaliteit.

Een veelgemaakt onderscheid is dat tussen '*cybercrime*' en 'gedigitaliseerde criminaliteit' (Leukfeldt & Van 't Hoff-de Goede, 2023). Dit onderscheid kan als volgt worden uitgelegd: bij *cybercrime* gaat het om digitale criminaliteit die zowel gepleegd wordt met ICT als gericht is op ICT. Denk aan DDoss-aanvallen en criminelen die computers en netwerken illegaal hacken en overnemen, maar ook aan vormen van fraude met hacking en ransomware als digitale componenten (Odinot en collega's, 2018; Oerlemans & Van der Wagen, 2020; Stol & Jansen, 2013; Spithoven, 2020). Bij *gedigitaliseerde criminaliteit* spelen informatie- en communicatietechnologie (ICT), zoals computers, laptops, iPads en smartphones, in meer of mindere mate een rol. Dit gebeurt zonder dat er in computersystemen wordt ingebroken (Borwell en collega's, 2020). Digitale gegevensdragers zijn hierbij alleen een hulpmiddel voor het plegen van delicten. Tegelijk is het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit in de praktijk niet zo helder. Vormen lopen door elkaar heen. Daarom wordt het onderscheid losgelaten en gaat het in dit rapport om digitale criminaliteit.

2.2.2 *Hybride karakter*

Het hybride karakter van digitale criminaliteit toont zich in een vermenging van fysieke en digitale delicten (Boekhoorn, 2019; Roks en collega's, 2021; Schiks en collega's, 2022). Stalking in persoon kan bijvoorbeeld gepaard gaan met stalking via digitale middelen, zoals appjes en sociale media. Hetzelfde geldt voor een verregaande vermenging tussen digitale criminaliteit en straatcriminaliteit bij het ronselen van 'geldezels' of 'katvangers' (vaak jonge mensen die hun bankrekening 'uitlenen' voor het doorsluizen van crimineel geld) op een schoolplein of in een wijk (Bekkers en collega's, 2023; Leukfeldt & Roks, 2021; Weulen Kranenbarg & Van 't Hoff-de Goede, 2023). Een laatste voorbeeld is dat er door de politie met regelmaat bij jonge cybercriminelen wapens, munitie en explosieven worden aangetroffen (OM & Politie, 2024). Online en offline criminaliteit lopen dus in elkaar over.

2.2.3 *Categorisering*

Om tot meer duidelijkheid en kadering te komen kan ook gebruikt worden gemaakt van een classificatieinstrument, waarbij het motief van de verdachte of dader van digi-

tale criminaliteit centraal staat. Er kunnen meerdere hoofdcategorieën van motieven worden onderscheiden bij het in beeld brengen van delicten waar basisteams mee te maken hebben (Leukfeldt en collega's, 2015):

1. *Digitale criminaliteit met geldelijk of financieel gewin,* een van de meest voorkomende motieven van daders. Bij fraude/oplichting worden geld of waardevolle spullen door misleiding afhandig gemaakt (Borwell en collega's, 2020; Spithoven, 2020). Denk bijvoorbeeld aan bankhelpdeskfraude, BEC-fraude, hulpvraagfraude, betaalverzoekfraude, tech support scam, misbruik van accounts voor bestellingen, aan- en verkoopfraude en beleggingsfraude.
2. *Persoonsgerichte digitale criminaliteit*, ook wel interpersoonlijke delicten genoemd, richt zich zonder direct financieel oogmerk op de aantasting van iemands persoonlijke levenssfeer of op de beschadiging van een persoon. Vormen zijn bedreiging, pesten, smaad en laster – en nauw verwant: stalking en sexting (Barrense-Dias, en collega's, 2017; Borwell, 2020; Spithoven, 2020; Spithoven & Van Tuijl, 2024).
3. *Bij chantage/afpersing* worden geld of waardevolle goederen afhandig gemaakt via digitale modus operandi in combinatie met dreiging met geweld of andere vormen van dreiging, zoals (be)dreiging met smaad of het openbaren van een geheim. Sextortion is een subcategorie van chantage/afpersing (Ray & Henry, 2024).

Bovenstaande driedeling vormt het kader van de quickscan (hoofdstuk 3) waarin de aard en omvang van digitale criminaliteit uiteen worden uiteengezet.

2.3 Slachtofferschap van digitale criminaliteit

2.3.1 *Meldings- en aangiftebereidheid*

Hoewel mensen misschien wel de intentie hebben om melding of aangifte van een digitaal delict te doen, is het aantal dat daadwerkelijk naar de politie stapt gering. Zoals al eerder naar voren kwam, doet slechts 16% aangifte. Deels hangt aangiftebereidheid samen met de demografische kenmerken van slachtoffers (Van de Weijer en collega's, 2019). In de praktijk wisselt de meldings- en aangiftebereidheid ook per delict. Als de (ervaren) ernst van een delict toeneemt, stijgt over het algemeen ook de meldings- en aangiftebereidheid van slachtoffers (Akkermans en collega's, 2024; Boekhoorn & Tolsma, 2016; Tarling & Morris, 2010; Van de Weijer en collega's, 2019). Slachtoffers van phishing doen het vaakst aangifte, die van hacken het minst (Akkermans en collega's, 2024). Daarnaast kunnen slachtoffers bij andere instanties, waaronder banken, creditcardmaatschappijen, verzekeraars, online marktplaatsen en fraudehelpdesks, een melding doen. Slachtoffers van digitale criminaliteit stappen eerder naar deze instanties dan naar de politie (Van de Weijer en collega's, 2019). Een verklaring is dat zij bij banken en dergelijke in aanmerking komen voor financiële compensatie.

De motieven en behoeften achter meldings- en aangiftebereidheid verschillen per digitaal delict. Veelvoorkomende motieven die in de literatuur naar voren komen zijn dat

het slachtofferschap stopt, de dader wordt gepakt, er straf en vergelding volgt en dat wordt voorkomen dat een dader opnieuw kan toeslaan. Ook de behoefte aan compensatie en schadevergoeding, erkenning, herstel, een veiliger online omgeving en meer inzicht in het digitale delict en de (strafrechtelijke) aanpak daarvan worden regelmatig genoemd (Bluhm en collega's, 2023; Leukfeldt en collega's, 2018; Van de Weijer en collega's, 2020). In hoofdstuk 6 komt naar voren dat slachtoffers van digitale en fysieke criminaliteit verschillende behoeften hebben.

Vaak genoemde motieven om geen aangifte te doen zijn dat slachtoffers het probleem zelf kunnen oplossen of het idee hebben dat de politie er toch niets aan doet. Verder is het mogelijk dat mensen zich niet bewust zijn van hun slachtofferschap, zich vooral zelf verantwoordelijk voelen, zich schamen of beperkte financiële schade hebben ondervonden. Wanneer het slachtoffer de dader persoonlijk kent, wordt er minder snel aangifte gedaan (Van de Weijer en collega's, 2020). Mensen zijn wellicht bang voor vergelding of willen geen strafrechtelijk traject tegen een kennis, vriend of familielid beginnen.

2.3.2 *Persoonskenmerken*

De generieke hypothese dat naarmate mensen (zeker jongeren) online actiever zijn dit automatisch risicoverhogend werkt, is omstreden. Dat mensen meer tijd op internet en op sociale media doorbrengen, wil niet altijd zeggen dat de kans om slachtoffer van een digitaal delict te worden ook meteen stijgt. Er spelen ook andere factoren mee, waaronder gebrek aan kennis over online gevaren bij potentiële slachtoffers, gelegenheid (bijvoorbeeld makkelijk kraakbare wachtwoorden) die aan daders wordt geboden, en hoe mensen zich op internet gedragen (Leukfeldt & Van 't Hoff-de Goede, 2023; Van der Kleij et al, 2020).

Uit eerdere studies naar slachtofferschap (en naar melders of aangevers) van digitale criminaliteit blijkt dat extraverte mensen een groter risico lopen om slachtoffer van digitale – en wellicht ook traditionele – criminaliteit te worden. Dit type mensen is gericht op voordelen in het leven en staat open voor nieuwe kansen, waardoor ze sneller risico's nemen en daardoor eerder slachtoffer worden. Impulsiviteit speelt hierbij een rol van betekenis (Borwell en collega's, 2018; Halevi en collega's, 2013; Modic & Lea, 2011; Van Wilsem, 2013). Hetzelfde geldt voor personen met verminderde emotionele stabiliteit (Sipma en Van Leijsen, 2019; Van de Weijer en Leukfeldt, 2017). Hoe hoger mensen scoren op dit soort persoonskenmerken, hoe groter hun kwetsbaarheid voor slachtofferschap.

Ook altruïstische personen zijn gevoeliger voor slachtofferschap. Zij zijn eerder geneigd om anderen te vertrouwen. Dit zorgt ervoor dat altruïstische personen kwetsbaarder zijn voor bijvoorbeeld oplichting of phishingaanvallen. Daarnaast wordt het risico op slachtofferschap verhoogd als mensen niet erg ervaren zijn met online activi-

teiten, minder snel frauduleuze handelingen herkennen, maar snel doen wat er van hen wordt gevraagd (Borwell en collega's, 2018; Bullée, 2017; Parrish en collega's, 2009). Wederom geldt dat een hoge score op dit soort persoonskenmerken mensen kwetsbaarder maakt voor slachtofferschap. Personen die risicomijdend zijn, hebben juist minder kans om in de val van digitale criminaliteit te trappen.

Tot slot hangen eerdere slachtofferervaringen van digitale criminaliteit samen met hernieuwd slachtofferschap. Iemand die eerder slachtoffer is geweest van een delict, heeft een grotere kans dit nog een keer (of zelfs vaker) te worden. Zoals hierboven opgemerkt zijn de impulsiviteit, emotionele (in)stabiliteit en openheid van personen robuuste indicatoren voor herhaling. Impulsieve personen worden beduidend vaker gehackt, emotioneel instabiele personen trappen sneller in phishing-mails en open personen zijn minder geneigd om gevoelige informatie online goed af te schermen (Sipma & Van Leijsen, 2019).

2.3.3 *De impact van digitale delicten*

Een misdrijf kan verschillende gevolgen hebben voor verschillende slachtoffers, waardoor de impact op een individu lastig te voorspellen is. De impact van (terugkerend) slachtofferschap kan echter groot zijn. Volgens eerdere publicaties lijken deze impact en gevolgen van digitale criminaliteit niet of nauwelijks te verschillen in vergelijking met fysieke criminaliteit (Bluhm en collega's, 2023; Hamby en collega's, 2018; Jansen & Leukfeldt, 2018; Notté en collega's, 2021). Tegelijk kunnen er kritische kanttekeningen bij die bevindingen worden geplaatst. Zo lijkt de impact van delicten op slachtoffers van digitale criminaliteit wel degelijk te verschillen van slachtoffers van traditionele criminaliteit, zoals bijvoorbeeld inbraak, geweld of beroving (Borwell en collega's, 2024, 2025; Holt & Bossler, 2009). Bij delicten die de persoonlijke levenssfeer van mensen ernstig aantasten (zoals stalken, pesten, sexting en sextortion) en/of die grote financiële schade veroorzaken, kan de slachtofferimpact van digitale criminaliteit zelfs groter zijn dan bij traditionele criminaliteit. Mensen beschouwen hun digitale apparaten als verlengstuk van zichzelf, waardoor zij persoonlijk hard worden geraakt. Deze impact kan een langeretermijneffect hebben. Zo lijkt volgens Shapland en Hall (2007) de shock zelf voor slachtoffers vaak van korte duur, terwijl het verlies aan vertrouwen in mensen jaren kan aanhouden.

In de praktijk interacteren en overlappen soorten impact met elkaar (Modic & Anderson, 2015). Voor een helder beeld worden de vier verschillende impactsvormen hieronder opgesomd:

1. Veel slachtoffers van digitale criminaliteit ondervinden *financiële impact*. Slachtoffers van digitale criminaliteit melden zowel directe als indirecte financiële gevolgen, zoals tijdverlies en de noodzaak om (dure) apparatuur te vervangen (Kerr en collega's, 2013). De financiële gevolgen voor slachtoffers variëren van enkele (honderden) euro's tot bedragen van boven de paar ton of zelfs nog hoger. Digitale frau-

de en oplichting, maar ook afpersing en chantage, zijn vaak de oorzaak van deze schade.
2. Slachtoffers van digitale criminaliteit ervaren soms *emotionele en psychische impact*. Deze impact betreft angst, schaamte, shock, verdriet, stress, machteloosheid, frustratie, eenzaamheid en woede. In ernstige gevallen kan er sprake zijn van depressie, een posttraumatische stressstoornis of zelfmoordneigingen (Borwell en collega's, 2020; Kunst & Koster, 2017; Notté en collega's, 2021). Criminaliteit in de interpersoonlijke sfeer, zoals online bedreiging of intimidatie, heeft de meest emotionele en psychologische impact, maar ook digitale oplichting, fraude, hacken en andere online delicten zorgen voor dit type impact. De ernst van het delict en herhaald slachtofferschap wegen hierbij mee (Notté en collega's, 2021; Sipma & Van Leijsen, 2019).
3. Een andere vorm van impact is *sociaal* van aard. Net als bij traditionele criminaliteit kunnen slachtoffers van digitale criminaliteit door hun directe sociale omgeving, door vreemden en door de politie verantwoordelijk worden gehouden voor hun eigen slachtofferschap (Cross en collega's, 2016; Kerr en collega's, 2013; Leukfeldt en collega's, 2018; Walker en collega's, 2013). Dit wordt ook wel *victim blaming* genoemd (Borwell en collega's 2021). Slachtoffers krijgen bijvoorbeeld het verwijt dat ze naïef zijn geweest door persoonlijke inloggegevens of pincodes af te geven, of dat ze uit zichzelf risicovolle activiteiten op het internet hebben ondernomen.
4. De emotionele en sociale impact van digitale criminaliteit kunnen ook met *fysieke impact* verweven zijn (Shapland & Hall, 2007). Slachtoffers kunnen indirecte fysieke gevolgen van een delict ervaren, waaronder hoofdpijn, slapeloosheid en gewichtsverlies (Cross en collega's, 2016; Dinisman & Moroz, 2017; Kerr en collega's, 2013). Dit komt voort uit spanning, stress en andere reacties op een nare of zelfs traumatische gebeurtenis. Dergelijke reacties doen niet onder voor de gevolgen van traditionele vormen van criminaliteit.

In hoofdstuk 6 komt de impact van digitale delicten op slachtoffers uitgebreid aan de orde.

2.4 De aanpak van digitale criminaliteit door de politie

2.4.1 *Nationaal niveau*

Op nationaal niveau opereert het Team High-Tech Crime (THTC) dat zich richt op complexe en omvangrijke cybercrime die de landsgrenzen overstijgt. Daarnaast is er het Landelijk Meldpunt Internet Oplichting (LMIO) dat online aangiften van digitale aan- en verkoopfraude clustert en doorstuurt naar de basisteams. Bij de Operationele Informatieverwerking van de Landelijke Eenheid (OIV-LE) komen deze aangiften binnen. Het is de opdracht van de landelijke Operatie Centurion om de aanpak van gedi-

gitaliseerde criminaliteit binnen zowel de politie als het OM te versnellen en te verbeteren, en het LMIO heeft daar een rol in. Hieronder volgt een toelichting.

Team High-Tech Crime
In 2007 werd het landelijke THTC opgericht. Dit team voert zelfstandig opsporingsonderzoeken uit naar high-tech crime, waaronder de meest geavanceerde vormen van cybercrime (Domenie en collega's, 2013; Struiksma en collega's, 2012). Gespecialiseerde rechercheurs houden zich bezig met hackers, DDoS-aanvallen, ransomware, malware, botnets en criminele fora op het darkweb. Het THTC werkt binnen het Landelijk Operationeel Cybercrime Overleg (LOCO) samen met lokale cybercrimeteams om hen te ondersteunen in de opsporing (Broekhuizen en collega's, 2022). Ook werkt het THTC preventief om delicten te voorkomen en cybercriminelen te verstoren. Het team zoekt wereldwijd naar belangrijke botnets of criminele actoren, zonder dat hier een aangifte aan ten grondslag ligt. Het Cyber Offender Prevention Squad (COPS) richt zich binnen deze preventieve aanpak op daderpreventie. Het COPS werkt samen met publieke en private partijen, zoals gemeenten en cybersecuritybedrijven. Het doel van deze integrale samenwerking is om (potentiële) daders van cybercrime te op te sporen, te vervolgen en te ontmoedigen.

Landelijk Meldpunt Internetoplichting
Het LMIO is een landelijk politieteam dat is opgericht om samen met zijn partners – het OM, Marktplaats, de fraudehelpdesk, de bankensector, Payment Service Providers en de Autoriteit Consument en Markt – aan- en verkoopfraude via online handelingsplaatsen aan te pakken en te voorkomen (Terpstra en collega's, 2021). Het LMIO ontvangt en analyseert aangiften van aan- en verkoopfraude en bereidt strafrechtelijke onderzoeken voor die worden verzonden naar de basisteams in wiens/wier werkgebied de verdachte(n) woont/wonen voor verdere afhandeling. Dit proces is inmiddels deels geautomatiseerd. Het LMIO start op basis van drie criteria een voorbereidend onderzoek: het aantal verwante aangiften dat tot een verdachte is te traceren, de hoogte van het schadebedrag en de eventuele minderjarigheid van een verdachte. Zaken met het hoogste aantal aangiften of met grotere schadebedragen worden geprioriteerd en opgepakt. Ook neemt het LMIO maatregelen om online oplichting te verstoren en zoekt het team naar mogelijkheden voor slachtoffers om geld terug te krijgen. De laatste jaren heeft het team geïnvesteerd in een alternatieve afdoening van zaken, zoals een waarschuwingsbrief, het stopgesprek en directe aansprakelijkheid, om de opsporings- en vervolgingsketen te ontlasten (Doornbusch en collega's, 2023).

Operatie Centurion
Operatie Centurion is uitgerold met als doel de aanpak van gedigitaliseerde criminaliteit te versnellen en te verbeteren en de pakkans van verdachten/daders te vergroten (Van der Plas & Hagenaars, 2021). Bij veel vormen van digitale criminaliteit geldt dat de fysieke afstand tussen dader en slachtoffer groter is dan bij traditionele criminaliteit, waarbij verdachte en slachtoffer minder vaak in elkaars buurt leven. Hierdoor is lande-

lijke en internationale coördinatie nodig. Operatie Centurion richt zich op het bestrijden van veelvoorkomende digitale criminaliteit, in het bijzonder aan- en verkoopfraude, bankhelpdeskfraude, hulpvraagfraude en phishing. De opdracht is om criminele verbanden bloot leggen door een bundeling van intelligence en expertise. Het coördineren en opsporen van criminele verbanden vindt vervolgens plaats op eenheidsniveau. Inmiddels zijn binnen meerdere eenheden gespecialiseerde teams en hubs opgericht die focussen op de aanpak van bovengenoemde Centurion-feiten.

2.4.2 *Regionaal niveau*

Samen met het landelijke THTC opereren er op regionaal niveau ook cybercrimeteams die zaken oppakken, verstoren en voorkomen. Voorts zetten Regionale Service Centra (RSC) meldingen en aangiften, waaronder die van digitale criminaliteit, aan basisteams door. In een aantal politie-eenheden lopen er regionale pilots met de zogeheten 'Digitale Meldkamer' of 'DigiPrio1'. De volgende paragrafen bevatten een korte toelichting.

Cybercrimeteams
Grootschalige en complexe cybercrimezaken vallen onder de Dienst Regionale Recherche (DRR). Denk hierbij aan het hacken van overheidsinstellingen of ziekenhuizen (Boekhoorn, 2019). Cybercrimeteams bestaan uit zowel ervaren tactisch rechercheurs als uit digitaal experts. Hun doelen zijn het opsporen en aanhouden van verdachten, het opbouwen van kennis en ervaring en het samenwerken met verschillende partners. Daarnaast hebben de regionale cyberteams de taak om basisteams en districtsrecherches (DR's) te ondersteunen bij het oppakken van ingewikkelde zaken, zodat zij hun specialistische kennis kunnen uitlenen aan lokale collega's.

Regionale Service Centra en meldkamers
Op regionaal niveau vervullen RSC een cruciale functie aan de voorkant van het primaire politieproces. Burgers kunnen via het algemene politienummer (0900-8844) contact leggen met een RSC over allerlei meldingen, waaronder over digitale criminaliteit (Bureau Beke, 2024; Van Steden en collega's, 2023). RSC-medewerkers nemen de binnenkomende meldingen op, doen een eerste check, informeren burgers en verwijzen hen desgewenst door voor een aangifte op een basisteam. Daarnaast controleren deze medewerkers ook internetaangiften. Naast de RSC kunnen burgers in noodgevallen via 112 contact leggen met regionale meldkamers.

2.4.3 *Lokaal niveau*

Zoals beschreven zijn de basisteams primair verantwoordelijk voor de aanpak van veelvoorkomende criminaliteit (VVC) die steeds vaker een digitale component heeft of digitaal van karakter is. Het gaat hier om zaken met een relatief lage technologische complexiteit, meestal diverse soorten fraude en oplichting en persoonsgerichte delic-

ten. De volgende paragrafen gaan over de instroom en screening van zaken en de mogelijke opsporing daarvan. Tot slot worden de contouren geschetst van de lokale preventie, monitoring en verstoring van digitale criminaliteit (of fysieke criminaliteit met een digitale component).

Instroom
Net als bij traditionele vormen van digitale criminaliteit kan de politie op eigen initiatief een onderzoek naar een digitale zaak starten, maar vaker doen slachtoffers een aangifte of melding die op lokaal niveau bij de basisteams binnenstroomt. Hiervoor bestaan er verschillende aanvoerroutes. Allereerst kunnen slachtoffers persoonlijk langsgaan bij I&S-medewerkers van een basisteam (Bureau Beke, 2024: Van Steden en collega's, 2024). Meestal hebben zij eerst contact met een RSC die een aangifte of melding telefonisch afhandelt of een afspraak inplant op een basisteam in de wijk waar het delict heeft plaatsgevonden. Naast dat burgers persoonlijk bij de balie langskomen, kunnen zaken ook bij een basisteam instromen doordat burgers een (112-)melding doen.

Bij sommige basisteams is het mogelijk om via e-mail, Facebook, WhatsApp of een videogesprek contact met de politie te leggen (Jansen en collega's, 2020). Ook komen aangiften of meldingen van gedigitaliseerde criminaliteit en cybercrime binnen vanuit andere eenheden, vanuit het buitenland of vanuit externe (private) instanties, zoals fraudehelpdesks, online handelsplatforms, banken en verzekeraars (Domenie en collega's, 2013; Van den Eeden en collega's, 2021). Internetaangiften van Centurion-feiten (bankhelpdeskfraude, bankphishing en hulpvraagfraude) stromen in bij de RSC. Het RSC beoordeelt de aangiften op dezelfde manier als het OIV-LE. Na controle vindt een automatische routering richting de basisteams alleen plaats indien er sprake is van een Nederlands IBAN-nummer. Bij bankphishing, bankhelpdeskfraude en hulpvraagfraude is zo'n nummer vaak niet aanwezig. Bij online aan- en verkoopfraude werkt automatische routering beter. Vervolgens verschijnen de zaken via Betere Opsporing door Sturing op Zaken (BOSZ) in de werkvoorraad van een basisteam.

Screening
Ieder basisteam (of in sommige gevallen het district) heeft meerdere casescreeners in dienst – een functiebenaming die door het land heen verschillend is. Deze casescreeners zijn verantwoordelijk voor het dagelijks beoordelen van alle nieuw binnengekomen (potentiële) opsporingsverzoeken (Van Steden en collega's, 2023). Zowel de politie als het OM wordt geconfronteerd met een veelheid aan strafbare digitale en/of fysieke zaken. De beschikbare opsporingscapaciteit is beperkt en dwingt tot stellen van prioriteiten en het maken van keuzes. Dit betekent dat er afgewogen moet worden of in een zaak tot opsporing moet worden overgegaan; en zo ja, met welke inzet. Doorgaans krijgen alleen 'prio-1-zaken' (met letsel) voorrang.

Wanneer een aangifte binnenkomt, toetst de casescreener of er sprake is van een strafbaar feit en van een 'high-impact' misdrijf. Dit doet een casescreener aan de hand van screenings- en selectiviteitskaders. Er moeten voor de politie ook indicaties en aanknopingspunten zijn om een opsporingsonderzoek in te stellen en om de identiteit van een verdachte te kunnen achterhalen. Een casescreener weegt af of de inspanningen die hiermee gemoeid zijn in redelijke verhouding staan tot het belang van het onderzoeksdossier (Landelijk Platform VVC, 2021). Het OM geeft daarnaast vanuit zijn gezagsrol richting de politie aan welke criteria moeten gelden bij het beoordelen of een zaak al dan niet wordt opgepakt en met welke prioriteit. Aan de hand hiervan kan een casescreener zelfstandig bepalen of er een onderzoeksdossier van een misdrijf aangemaakt wordt, of dat een aangifte of melding wordt afgewezen. Vroegtijdig beëindigen wordt wel in samenspraak met het OM gedaan (dan gaat het bijvoorbeeld over beschikbare capaciteit).

Opsporing
Als aangiften door de screening zijn gekomen, kunnen zaken worden verrijkt met informatie over de verdachte en het incident. Dit kan worden gedaan door de casescreener zelf, maar ook door andere afdelingen van het basisteam en binnen de politie. Zo kunnen videobeelden, bankrekeningnummers en IP-adressen worden gecontroleerd en kunnen telefoons worden uitgelezen. Het doel van deze verrijking is om een verdachte op te sporen en te horen. Mocht er geen aanwijsbare verdachte in beeld komen, dan kan een zaak alsnog worden afgerond (Leukfeldt en collega's, 2012).

Als er wordt besloten tot een opsporingsonderzoek kan dat worden toebedeeld aan de basisteamrecherche (het VVC-team), de districtsrecherche (DR), de Dienst Regionale Recherche (DRR) of een team van een andere eenheid. Ook dan is het nog mogelijk dat een zaak vroegtijdig wordt beëindigd, bijvoorbeeld als het misdrijf niet kan worden bewezen of als een zaak buitenproportioneel veel politie-inzet vergt in vergelijking met de ernst ervan (Ruiter en collega's, 2024). Beslissingen hierover vinden in samenspraak met het OM plaats.

Eenmaal bezig met opsporing zoeken rechercheurs naar sporen, horen ze getuigen en slachtoffers, leggen ze gegevens vast in een proces-verbaal, observeren ze verdachten en houden hen eventueel aan. Zij kunnen hierbij een beroep doen op digitaal experts die de recherche ondersteunen bij het opsporingsproces (Leukfeldt en collega's, 2012; Zuurveen & Stol, 2020). Opnieuw blijkt uit eerder onderzoek dat een te grote complexiteit van digitale zaken en gebrekkige kennis bij rechercheurs een effectieve opsporing in de weg kunnen staan. Voorts kan versnipperd eigenaarschap de opsporing frustreren (Ruiter en collega's, 2024). Digitale criminaliteit is niet aan geografische grenzen gebonden, waardoor er meerdere opsporingsteams over een onderzoek kunnen gaan.

Preventie, monitoring en verstoring
De lokale aanpak van digitale criminaliteit stopt niet bij de opsporing en (mogelijke) vervolging van verdachten. Ook richten basisteams zich op preventie, monitoring en verstoring. In studies wordt betoogd dat de politie meer zou moeten investeren in communicatie met het grotere publiek over de risico's van digitale criminaliteit, de modi operandi van daders en het belang van aangifte doen. Daarnaast is ruimte voor meer samenwerking tussen de politie en lokale veiligheidspartners om de informatiepositie van basisteams over daders en dadergroepen te versterken, hun gedrag te monitoren en hen vervolgens te dwarsbomen (Spithoven en collega's, 2022; Spithoven & Leukfeldt, 2023).

Het monitoren van gedragingen op het internet vindt plaats door politiemedewerkers die zijn getraind in OSINT (Open Source Intelligence) en OIS (Opsporing Internet sociale media). Zij spitten en graven naar opsporingsinformatie en bewijslast in de vorm van teksten, beelden en audio voor het bestrijden van criminele activiteiten zoals (online) fraude en persoonsgerichte delicten (Broekhuizen en collega's, 2022; Landman & Groothuis, 2022). Het speuren op sociale mediaplatforms, waaronder Facebook, Snapchat en Instagram, neemt hierbij een voorname plaats in. OSINT is op basisteams verbonden met het opzetten van digikamers en digihubs als ontmoetingsplekken voor collega's om gezamenlijk aan de slag te gaan met online vraagstukken.

Specifiek heeft de politie in digitaal wijkagenten geïnvesteerd die op internet surveilleren, openbare bronnen monitoren en zowel repressieve als preventieve taken uitvoeren in het kader van digitale criminaliteit. Zij moeten de wijk, het web en de wereld met elkaar verbinden. Digitaal wijkagenten hebben in de praktijk veel vrijheid om hun eigen taken en werkzaamheden in te vullen. Soms dragen zij bij aan het voorbereiden dan wel uitvoeren van opsporingsonderzoeken. Het is bijvoorbeeld mogelijk dat een digitaal wijkagent verdachten in beeld brengt, zodat er een proces-verbaal kan worden opgesteld (Boelens & Landman, 2021). Momenteel zoekt de politie nog naar de meest optimale invulling van hun takenpakket en functie op de basisteams.

2.5 Tot besluit

Uit de literatuur blijkt dat de precieze invulling van wat onder de noemer 'digitale criminaliteit' valt fluïde is. Het onderscheid tussen 'fysiek' en 'digitaal' is niet bij alle delicten even scherp en hetzelfde geldt voor het onderscheid tussen 'cybercrime' en 'gedigitaliseerde criminaliteit'. In dit rapport gaat de aandacht uit naar de vormen van digitale criminaliteit waarmee basisteams veelvuldig in aanraking komen: online fraude, persoonsgerichte delicten en chantage/afpersing. De basisteams spelen een niet te onderschatten rol in contacten met slachtoffers die allerlei behoeften hebben en die regelmatig een flinke financiële, emotionele, sociale en zelfs fysieke impact van digitale delicten ervaren.

Opvallend genoeg ontbreekt in de literatuur over slachtoffers van digitale criminaliteit het thema 'hoe tevreden' zij over de politie zijn. Hoewel er genoeg studie is verricht naar burgertevredenheid over lokaal politiewerk (Boateng, 2018; Bolger en collega's, 2021; Tyler & Huo, 2002; Yuksel & Tepe, 2013), lijkt op dit vlak nog geen onderscheid gemaakt te worden tussen slachtoffers van traditionele en slachtoffers van digitale criminaliteit. In hoofdstuk 6 wordt deze omissie in de literatuur opgevuld. Tot slot: naast het opnemen van aangiften en de screening hiervan, zijn basisteams ook belast met de opsporing van verdachten. Toch is er nauwelijks iets bekend over 'hoe groot' de instroom van digitale criminaliteit op basisteams is en hoe vervolgens de afhandeling en opvolging van geregistreerde delicten plaatsvindt. Daar gaan de volgende hoofdstukken over.

3. Quickscan naar de aard en omvang van digitale criminaliteit

3.1 Inleiding

Tot op heden is het lastig gebleken om de aard en omvang van digitale criminaliteit in de breedte vanuit de politiesystemen inzichtelijk te maken. De Landelijke Cyberintelligence binnen de politie – een netwerk van informatieanalisten/onderzoekers binnen de verschillende eenheden die zich bezighouden met het thema cybercrime – heeft de laatste jaren geïnvesteerd om cybercrimefenomenen goed uit deze systemen te halen. Echter, door de focus op cybercrime is gedigitaliseerde criminaliteit onderbelicht gebleven. Basisteams hebben juist ook met dit type digitale criminaliteit te maken.

Er bestaan inmiddels verschillende interne onderzoeken waarin omvangschattingen zijn gedaan, maar die zijn vooral gericht op online fraude (Hesseling, 2021; Schuppers en collega's, 2022). Hoewel het vermoeden bestaat dat online fraude in de praktijk een fors deel van de geregistreerde digitale criminaliteit betreft, is er minder goed zicht op de omvang van digitale persoonsgerichte criminaliteit: delicten die in de persoonsgerichte sfeer worden gepleegd, zoals stalking, bedreiging en smaad/laster/belediging. Ook is het beeld van hoe werkstromen – dat wil zeggen: de registratie en afhandeling van digitale criminaliteit – binnen de politie lopen incompleet.

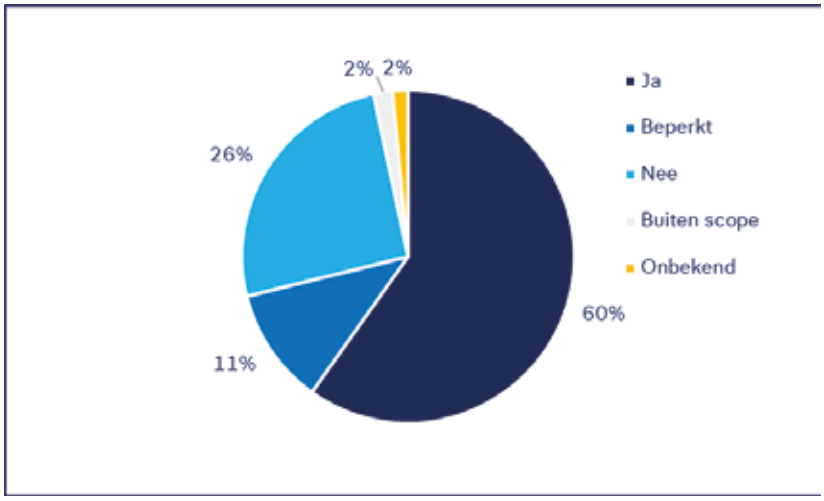
Om beter zicht te krijgen op het werkaanbod van digitale criminaliteit binnen de Nederlandse politie, in het bijzonder binnen districten en basisteams, ligt de focus in dit hoofdstuk op de omvang en aard van geregistreerde digitale criminaliteit in de periode oktober 2022 tot en met september 2023 (3.2).[3] Dat gebeurt aan de hand van een steekproef (N=600) en query's (zoektermen) op de volgende deelthema's: 'online fraude/oplichting', 'cybercrime', 'online bedreiging/stalking', 'online smaad/laster/belediging' en 'sexting/sextortion'. De paragraaf daarna gaat over de politieonderdelen die betrokken zijn bij de afhandeling van digitale criminaliteit, met extra aandacht voor de basisteams en voor bekende verdachten (3.3). Vervolgens wordt de opvolging van meldingen/delicten van digitale criminaliteit die op basisteams zijn binnengekomen besproken (3.4). Tot slot worden de inzichten uit dit hoofdstuk vergeleken met eerder uitgevoerd onderzoek naar de instroom van digitale criminaliteit op basisteams (3.5).

3 Zie Bijlage 3 voor de methodologie en aanpak van deze quickscan.

3.2 Het werkaanbod

3.2.1 *Omvang*

Steekproef
Uit de quickscan – een steekproef (N=600) van zaken – is naar voren gekomen dat 71% van de registraties (aangiften en meldingen) een digitale component heeft. Bij 60% gaat het om een substantiële component ('Ja' in Figuur 1) in de uitvoering van het delict. Bij 11% is de digitale component weliswaar aanwezig in de uitvoering van het delict, maar is dit – ten opzichte van de fysieke bestandsdelen – beperkt ('beperkt' in Figuur 1). Binnen de categorie 'beperkt' gaat het relatief vaak om persoonsgerichte delicten. Denk bijvoorbeeld aan stalkingszaken waarin de incidenten en dreiging vooral fysiek van aard zijn geweest, maar de verdachte ook één of een enkele keer via sociale media contact met het slachtoffer heeft gezocht. Bij een ruim een kwart is het incident niet digitaal van aard en 2% van de registraties valt buiten de scope van ons onderzoek (die laatste categorie bevat onder meer kinderporno en grooming: digitaal kinderlokken; zie Bijlage 3 voor extra toelichting op deze scope). In het vervolg van dit hoofdstuk komen alleen de gevallen aan bod waarbij de digitale component van criminaliteit substantieel is.



Figuur 1 Aandeel digitale criminaliteit binnen steekproef (N=600)

Schatting
In de onderzoeksperiode oktober 2022 tot en met september 2023 zijn er in totaal 198.476 unieke registraties (aangiften en meldingen) van potentiële digitale criminaliteit naar voren gekomen. Op basis van bovengenoemde steekproefuitkomsten is de

schatting/extrapolatie – met een betrouwbaarheidsmarge van 95% – dat (afgerond op duizendtallen) in de onderzoeksperiode tussen 111.000 en 127.000 registraties een substantiële digitale component hebben, ofwel digitale criminaliteit betreffen.[4] Dit moet als een ondergrens worden beschouwd omdat met de query's/zoekslagen vermoedelijk niet alle registraties van digitale criminaliteit naar boven zijn gekomen. Er is getracht het aandeel 'false positives' beperkt te houden, hetgeen ook onvermijdelijk leidt tot 'false negatives'.

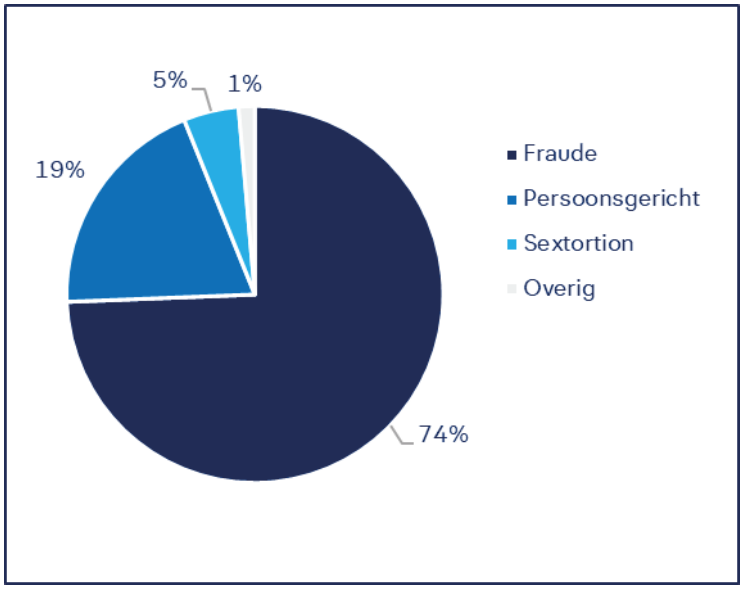
Er kan een uitsplitsing worden gemaakt naar de query's gericht op online fraude/cybercrime (in deze registraties zit veel overlap; het overgrote deel betrof online fraude) enerzijds, en de query's gericht op persoonsgerichte delicten (optelling van online bedreiging/stalking, online smaad/laster/belediging en sexting/sextortion) anderzijds. In het eerste geval kan 81% van de uitkomsten als digitale criminaliteit worden gekwalificeerd, terwijl dit bij persoonsgerichte delicten 37% is. In de schatting – met een betrouwbaarheidsmarge van 95% – zou dat neerkomen op tussen de 99.000 en 108.000 van de 122.000 registraties die gaan over online fraude/cybercrime. Bij persoonsgerichte delicten ligt dit aantal tussen de 26.200 en 34.200 van de bijna 82.300 registraties. Het aantal registraties van deze twee categorieën query's kan niet direct bij elkaar worden opgeteld, omdat er een kleine overlap zit tussen de query's. Wel geven de cijfers een eerste inzicht in de verhouding tussen online fraude en persoonsgerichte delicten.

3.2.2 *Aard*

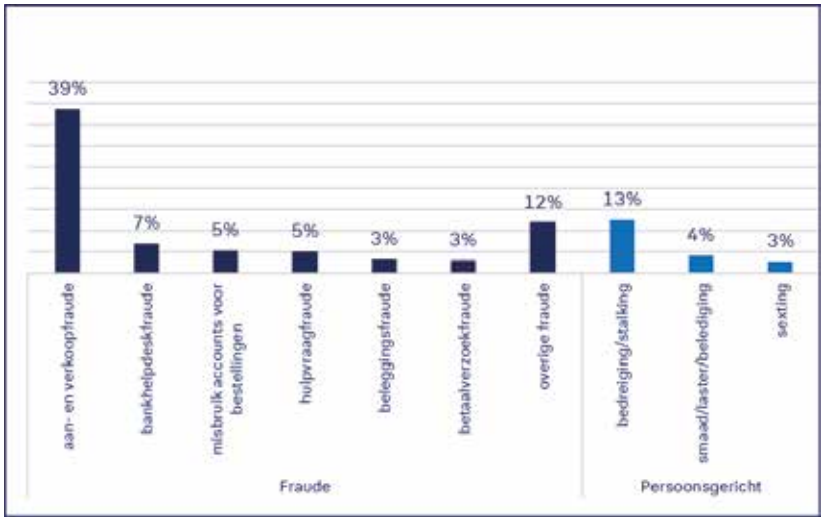
Binnen Figuur 2 inzoomend op de registraties die als digitale criminaliteit worden beschouwd (N=359; 60% van de 600 registraties in de steekproef), komt naar voren dat het grootste deel van deze registraties online fraude betreft (74%). Het aandeel persoonsgerichte criminaliteit is nagenoeg een vijfde (19%) en het aandeel van chantage/afpersing, dat geheel uit sextortion bestaat, is 5%.

In Figuur 3 zijn de categorieën 'fraude' en 'persoonsgericht' verder uitgesplitst. Daarbij blijkt aan-en verkoopfraude de grootste subcategorie (39%). Deze categorie betreft zelfs ruim de helft van alle online frauderegistraties. Binnen de categorie fraude volgen op afstand de subcategorieën bankhelpdeskfraude (7%), misbruik accounts voor bestellingen (5%) en hulpvraagfraude (5%). Binnen de categorie persoonsgerichte delicten is bedreiging/stalking het meest voorkomende delict. Op het totaal aantal registraties van digitale criminaliteit is dit aandeel 13%. Binnen de subcategorie persoonsgerichte delicten gaat het om bijna tweederde van de registraties.

4 Op basis van formule: $CI = p +- Z^* \sqrt{(p((1-p)/n)}$.



Figuur 2 Categorieën digitale criminaliteit (N=359)



Figuur 3 Aandeel subcategorieën fraude en persoonsgerichte delicten op totaal (N=359)

Hybride persoonsgerichte delicten
Zoals in hoofdstuk 2 aan de hand van de literatuurstudie al aan de orde kwam, is het onderscheid tussen fysieke en digitale criminaliteit niet altijd even helder. Er ontstaan in toenemende mate mengvormen. Vooral bij persoonsgerichte delicten met een substantiële digitale component is vaak zichtbaar dat er sprake is van een hybride karakter. Bedreigingen, smaad/laster en andere delicten worden niet alleen via de digitale weg gepleegd, maar ook fysiek (Box 1). Op basis van de steekproef is naar voren gekomen dat van de digitale persoonsgerichte delicten 40% als hybride kan worden getypeerd.

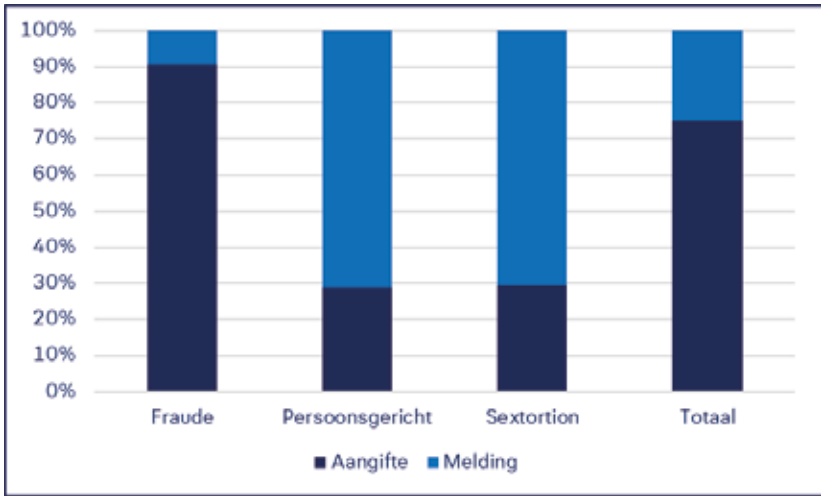
Box 1: Voorbeeld van hybride (fysieke en digitale) criminaliteit
Bedreiging/stalking: '*… Op zondag [geanonimiseerd] werd ik weer mishandeld door X… Sinds die zondag belde X mij duizenden keren op mijn mobiele telefoon… Via Snapchat maakte X meerdere accounts aan met nepnamen. Ik weet zeker dat X mij toevoegde via de zoekfunctie. De persoon die je toevoegt via de zoekfunctie moet mijn gebruikersnaam kennen…*'

Aangiften/meldingen
In totaal gaat het bij registraties van digitale criminaliteit in driekwart van de gevallen om aangiften en bij een kwart om meldingen (Figuur 4). Daarbij bestaan er grote verschillen tussen de categorie online fraude en de overige categorieën delicten. Zo komt naar voren dat het bij fraudedelicten in negen van de tien gevallen gaat om aangiften.[5] Dit hoge aandeel komt mede doordat slachtoffers aangifte moeten doen om in aanmerking te komen voor compensatie door instanties, zoals banken. Bij persoonsgerichte delicten gaat het vooral om meldingen (ruim 70%). Daarbij is een zekere differentiatie zichtbaar wat betreft de aard van de meldingen. Bij een deel gaat het om summiere meldingen en/of zijn er geen of weinig aanwijzingen voor strafbare feiten. Maar het gaat ook om meldingen waarin meer aanwijzingen zijn voor strafbare feiten. Toch is het niet tot een aangifte gekomen.

Vergelijking met het totale werkaanbod
De resultaten met betrekking tot de omvang van het werkaanbod van digitale criminaliteit zijn lastig af te zetten tegen het totale werkaanbod van aangiften en meldingen bij de politie. Dit komt doordat een groot scala van aangiften en meldingen incidenten betreft die over (ernstige) overlast – onder meer in het kader van wonen en kwetsbare

5 Een kanttekening hierbij is dat de frauderegistraties inzichtelijk zijn gemaakt aan de hand van maatschappelijke klassen met betrekking tot fraude en de resultaten aan de hand van de landelijke cybercrimequery. *Meldingen* van fraude (niet resulterend in aangiften) kunnen in andere maatschappelijke klassen naar voren komen. Deze zijn niet meegenomen in ons onderzoek als zij niet in de landelijke cybercrimequery zijn meegekomen (gericht op cybercrime en niet op digitale criminaliteit in algemeen). Dit lijkt echter slechts in beperkte mate te gebeuren. Op basis van BlueIntel (waarin de registraties uit de landelijke cybercrime query zijn gescoord) blijkt dat 95% van de frauderegistraties terechtkomt in de maatschappelijke klassen voor fraude. Ongeveer 4% komt terecht in maatschappelijke klassen voor meldingen, waarin de maatschappelijke klassen E40 AFHANDELING OVERIGE MELDINGEN, J12 VERDACHTE SITUATIE en J30 ALGEMENE MUTATIE de meest voorkomende zijn.

personen – en niet over criminaliteit gaat. Daarom is het zinvoller om alleen te kijken naar het aandeel aangiften van digitale criminaliteit op het totaal aantal aangiften dat bij de politie binnenstroomt. Met een betrouwbaarheidsmarge van 95% zijn er in de onderzoeksperiode naar schatting tussen de 83.300 en 95.100 aangiften gedaan van digitale criminaliteit.[6] Het totaal aantal aangiften betrof in deze periode ruim 672.700.[7] Het aandeel digitale criminaliteit op het totaal aantal aangiften bedraagt daarmee tussen de 12% en 14%.[8]



Figuur 4 Aandeel aangiften/meldingen (N=359)

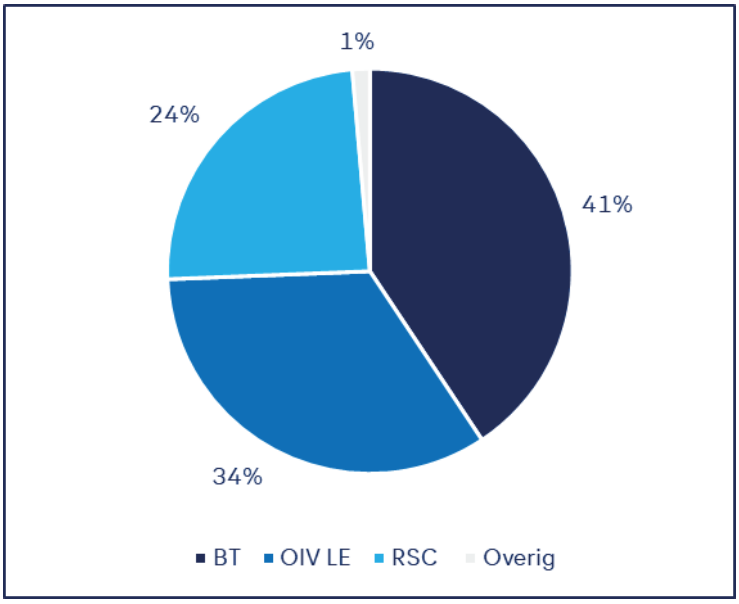
3.3 Organisatieonderdelen

3.3.1 *Instroom*

De aangiften/meldingen van digitale criminaliteit zijn het vaakst binnengekomen via een basisteam. Figuur 5 laat zien dat het om 41% van de aangiften/meldingen gaat. Veelal zijn dit mensen die naar het bureau komen, maar deels gaat het ook om telefonisch contact of contact via andere kanalen, bijvoorbeeld per mail. Verder komt een derde van de aangiften/meldingen bij de Operationele Informatieverwerking van de

6 Zie voetnoot 4 voor de gebruikte formule.
7 BHV-Kubus Basisproces Stuur, inclusief aangiften van verkeersdelicten, voornamelijk 'verlaten plaats ongeval' (parkeerschade).
8 Voor het totaal aangiften is als bron de Kubus-Basisproces Stuur in BVI-Cognos gebruikt. Hierbij zijn dezelfde keuzes gemaakt wat betreft de meetwaarde (aangiften) en datumvariabele (datum kennisname), wat de uitkomsten vergelijkbaar maakt met de uitkomsten op basis van het Cognosrapport in BVI-Cognos waarbinnen de query's/zoekslagen zijn gemaakt.

Landelijke Eenheid (OIV-LE) binnen. Daarbij gaat het om internetaangiften van online aan-en verkoopfraude. In nog een kwart van de gevallen is een RSC binnen een van de eenheden het startpunt van een aangifte of melding. Bij de RSC's gaat het in ruim 60% van de instroom om aangiften. Dan gaat het vrijwel altijd om internetaangiften van verschillende vormen van online fraude, exclusief aan-en verkoopfraude. Een kleine 40% van de instroom op een RSC betreft (telefonische) meldingen van hoofdzakelijk persoonsgerichte delicten.



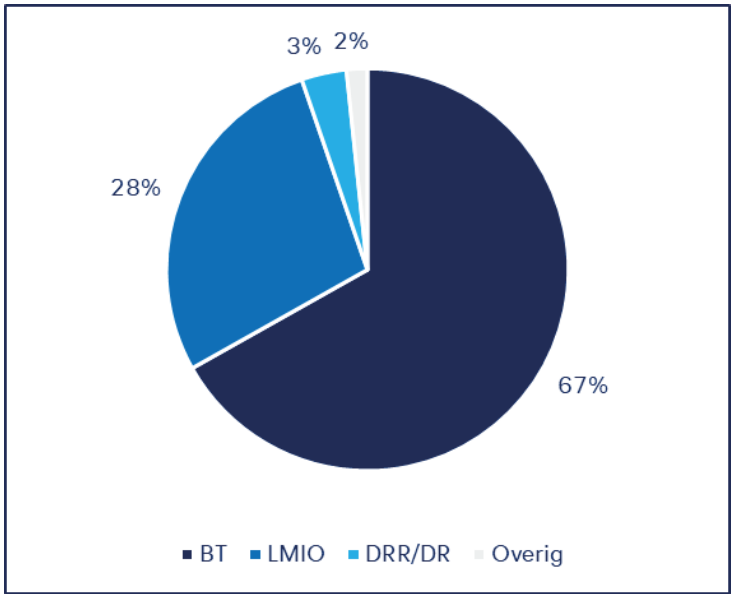
Figuur 5 Organisatieonderdeel instroom (N=359)

De registraties van digitale criminaliteit op de basisteams bestaan voor ruim de helft (60%) uit online fraude, 28% uit persoonsgerichte delicten, 10% uit sextortion en 3% uit overige delicten. Per categorie bestaan er verschillen met betrekking tot waar de aangiften/meldingen zijn binnengekomen. Gekeken naar de instroom loopt online fraude voor eenderde van de aangiften/meldingen via de basisteams, bijna de helft (45%) via de OIV-LE (internetaangiften aan-en verkoopfraude) en 22% via en RSC (veelal internetaangiften van andere vormen van online fraude). Wat betreft persoonsgerichte delicten is een groot aandeel (59%) binnengekomen via de basisteams. Het overige deel verliep veelal via een RSC (zoals hierboven vermeld vooral in de vorm van meldingen). Meldingen/aangiften van sextortion stromen in ruim acht op de tien gevallen in via de basisteams.

3.3.2 *Afhandeling*

In de afhandeling van digitale delicten komen de basisteams nog vaker naar voren (Figuur 6). Ruim tweederde van de registraties wordt afgehandeld door de basisteams. De internetaangiften over aan- en verkoopfraude worden in eerste aanleg door het LMIO behandeld. Het gaat om ruim een kwart (28%) van de aangiften. Het LMIO maakt op basis van die aangiften een nadere veredelingsslag, onder meer uitmondend in de zogeheten 'oplichterslijst'. Deze lijst werd tot en met juni 2023 rondgestuurd naar de eenheden – en daarbinnen naar districten en basisteams.

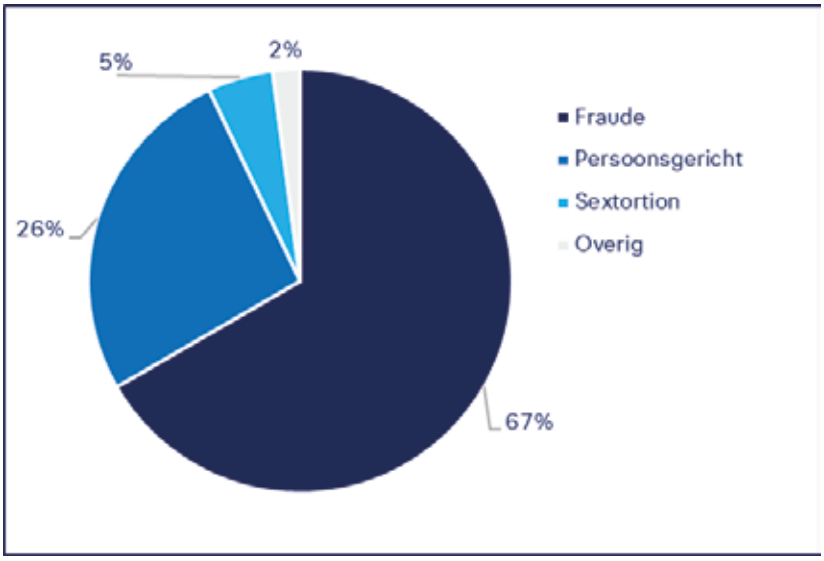
Vanaf 1 juli 2023 worden internetaangiften van aan- en verkoopfraude automatisch gerouteerd naar de basisteams indien sprake is van een herleidbare verdachte. In september 2023 is dit werkproces ook ingegaan voor phishing (betaalverzoekfraude en bankphishing) en voor hulpvraagfraude. Deze laatste uitbreiding heeft nog weinig effect op de routering van zaken die zijn onderzocht binnen onze analyse, omdat de onderzoeksperiode tot en met september 2023 loopt. Het beeld ten aanzien van routeringen in de eerste maanden na veranderingen van het werkproces zijn in ieder geval niet ingrijpend. Een klein deel van de aangiften van digitale criminaliteit (3%) is afgehandeld door de recherche op districtelijk of regionaal niveau. Tot slot zijn er enkele registraties die zijn afgedaan door het RSC (in categorie 'Overig'). Daarbij zijn de melders bijvoorbeeld doorverwezen naar een andere instantie, zoals een school, voor verdere afhandeling.



Figuur 6 Organisatieonderdeel afhandeling (N=359)

De basisteams

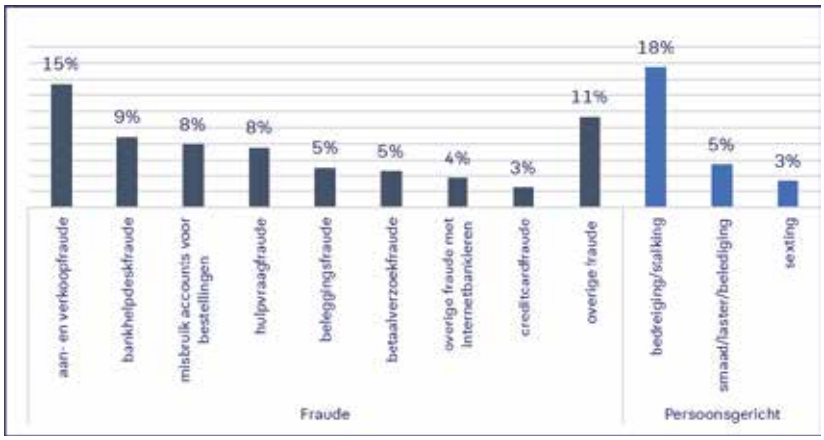
In Figuur 7, verder inzoomend op de afgehandelde meldingen/aangiften van digitale criminaliteit op de basisteams, komt naar voren dat online fraude de grootste categorie (67%) is. Vervolgens laat Figuur 8 zien dat de meest voorkomend variant aan- en verkoopfraude (15%) is, gevolgd door bankhelpdeskfraude (9%),[9] misbruik van accounts voor bestellingen (8%) en hulpvraagfraude (8%). Verder toont Figuur 7 aan dat 26% van de afgehandelde meldingen/aangiften bestaat uit persoonsgerichte delicten. Sextortion (chantage/afpersing) beslaat 5% en 2% valt in de categorie 'overig'. Meer in detail blijkt uit Figuur 8 dat het grootste aandeel van persoonsgerichte digitale delicten bedreiging/stalking (18%) omvat.



Figuur 7 Afgehandeld door basisteams (N=240)

Net als in het totaalbeeld geldt dat het bij de registraties van online fraude met name gaat om aangiften (84%) en bij persoonsgerichte delicten en sextortion om meldingen (bijna 70%). Vergeleken met het totaalbeeld zijn er binnen de frauderegistraties die door basisteams worden afgedaan relatief meer meldingen. Andersom geredeneerd zijn de door de basisteams afgehandelde aangiften van digitale criminaliteit in 80% van de gevallen online fraude, bij 16% gaat het om persoonsgerichte delicten en bij 3% om sextortion. Bij de afgehandelde meldingen gaat het in 62% van de gevallen om persoonsgerichte delicten, betreft het een kwart fraude en 10% sextortion.

9 Hier is alleen gekeken naar bankhelpdeskfraude waarvan de digitale component substantieel is. De variant waarbij slachtoffers alleen gebeld zijn en hun bankpas (plus pincode) is opgehaald is op 'digitaal beperkt' gezet, omdat het delict vooral telefonisch/in fysieke domein plaatsvindt. Met alle door de basisteams afgehandelde delicten die een substantiële en beperkte digitaal component hebben, komt bankhelpdeskfraude op 15% van het totaal afgehandelde meldingen/aangiften uit.



Figuur 8 Subcategorieën fraude en persoonsgerichte delicten (N=240)

Bekende daders
Bij de afhandeling van digitale criminaliteit op de basisteams is ook gekeken naar de mate waarin er voor slachtoffers bekende daders in beeld zijn op het moment zat zij een aangifte/melding doen. Bij persoonsgerichte delicten is in ruim acht van de tien gevallen de dader een bekende. Daarbij komen (ex)partners het vaakst voor, maar het gaat ook om vrienden, kennissen, buren, (oud)collega's, enzovoort. Bij online fraude-delicten komt het slechts sporadisch voor dat er een bekende verdachte in beeld is. Ook bij sextortion is in het overgrote deel van de zaken de dader onbekend.

3.4 Opvolging op de basisteams

3.4.1 *Doorstroom van digitale criminaliteit*

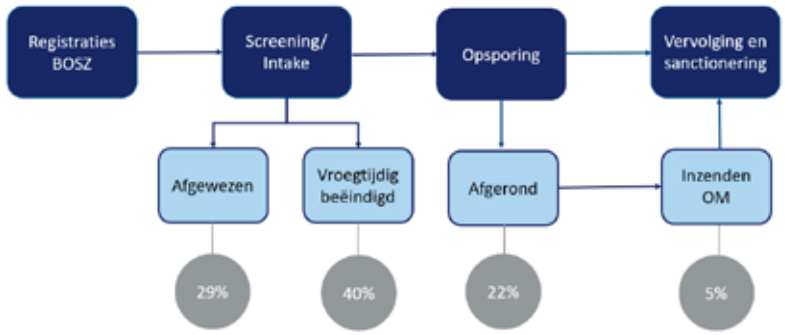
In BOSZ wordt geregistreerd hoe misdrijven zijn afgehandeld door de opsporing. Registraties die zijn gebleven bij meldingen (en dus niet hebben geresulteerd in aangiften) komen voor een groot deel niet in BOSZ. Van het totaal aantal registraties van door de basisteams afgehandelde digitale criminaliteit (N=240) zijn 195 registraties in BOSZ terechtgekomen en 45 registraties niet. Bij de ontbrekende registraties gaat het in 34 gevallen (76%) om persoonsgerichte delicten. Zoals eerder beschreven gaat het bij deze categorie verhoudingsgewijs vaak om meldingen. Dit kan verklaren dat zaken niet in BOSZ zijn opgenomen.

Van de genoemde 195 registraties in BOSZ blijkt een groot deel door de basisteams niet in behandeling te zijn genomen. Figuur 9 laat zien dat een groot aandeel ofwel

wordt afgewezen (29%) ofwel vroegtijdig wordt beëindigd (40%).[10] Slechts ruim een op de vijf registraties (22%) wordt daadwerkelijk afgerond. Een zaak wordt afgerond in BOSZ wanneer één of meer verdachten in een zaak een afhandeling hebben gekregen, zoals inzending naar het OM, een reprimande en een inzending naar bureau HALT. Daarnaast wordt een zaak in BOSZ afgerond als er geen verdachte is gevonden en er geen opsporingsindicaties meer aanwezig zijn. In slechts 5% van het totaal aantal onderzochte zaken in BOSZ is er sprake van een of meerdere bekende verdachte(n) die zijn ingezonden naar het OM. Dat aantal staat gelijk aan een kwart van de zaken met een afgeronde status.

Bij de afgewezen zaken wordt meestal (75%) aangegeven dat er 'geen opsporingsindicaties plus geen schokkend feit' is. Verder wordt bij 16% van de zaken genoemd dat er geen opsporingsindicatie was in een VVC-zaak. Bij het restant wordt aangegeven dat de afwijzing heeft plaatsgevonden op basis van expliciet beleid of dat er 'geen strafbaar feit' was. Vroegtijdige beëindiging van zaken is meestal gedaan 'wegens capaciteitsoverwegingen' (62%) en bij ruim een derde (37%) was er 'geen kansrijk vervolgbare zaak'. In enkele gevallen in de steekproef (2%) is aangegeven dat een niet-strafrechtelijke interventie effectiever was.

De politie mag de keuzes 'afwijzen' en 'vroegtijdig beëindigen' zelfstandig (dus zonder overleg met het OM) maken als het om VVC-misdrijven zonder bekende verdachte gaat. Bij VVC-zaken met een eenvoudig herleidbare verdachte kan een beslissing tot afwijzen of vroegtijdig beëindigen alleen met mandaat van het OM. Indien het OM akkoord geeft om een zaak vroegtijdig te beëindigen/af te wijzen, dient een eventuele verdachtenrol uit BVH verwijderd te worden.



Figuur 9 Stroomschema opvolging digitale criminaliteit op de basisteams (N=195)[11]

10 Waar dit voorheen anders was, kunnen Centurionfeiten technisch niet meer worden afgewezen.
11 Figuur 9 telt niet volledig op tot 100%, omdat 4% van de zaken tijdens de Quickscan nog in behandeling was.

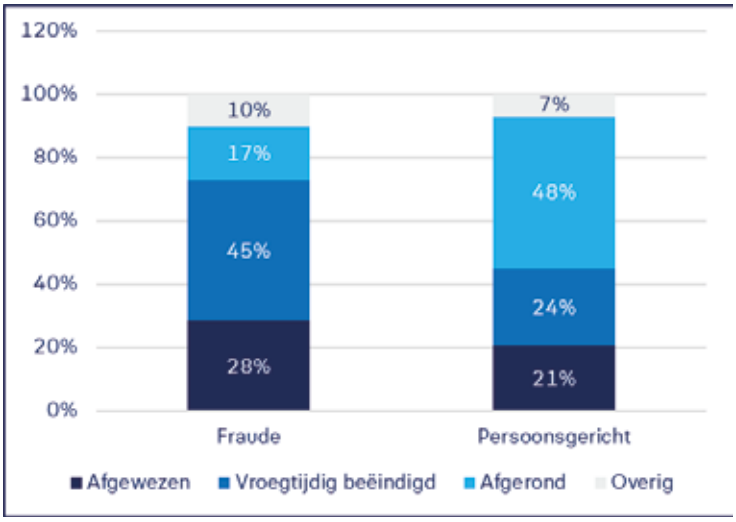
3.4.2 *Afhandeling per type delict*

De afhandeling van digitale criminaliteit door basisteams vertoont grote verschillen per type delict (Figuur 10).[12] Vooral bij online fraude worden zaken in meerderheid afgewezen/voortijdig beëindigd. De onderstaande figuur laat zien dat dit bij elkaar in 73% van de registraties het geval is, terwijl 17% van de zaken wordt afgerond. Het kan hier gaan om zaken waarin vorderingen zijn gedaan die te weinig aanknopingspunten hebben gegeven om tot een verdachte te komen, of dat registraties zijn overgedragen naar andere eenheden. Uit een eerdere politie-interne analyse naar online fraude rijst echter het beeld op van veel afgeronde registraties zonder dat er aanwijsbare vorderingen zijn geweest, er geen andere opsporingshandelingen zijn genoemd en er geen overdracht naar andere eenheden is geweest (Willekers & Schuppers, 2022). Daarmee lijkt het aandeel afgeronde zaken een overschatting te zijn van de mate waarin de politie concrete opsporingshandelingen heeft verricht.

Bij persoonsgerichte delicten is het aandeel zaken die afgewezen/voortijdig beëindigd kleiner (45%). Bijna de helft wordt afgerond. Een verklaring voor het feit dat digitale persoonsgerichte delicten vaker worden afgerond dan online fraudezaken is dat er vaker sprake is van bekende verdachten (woonachtig in het werkgebied van een basisteam). Ook zijn persoonsgerichte zaken vaker van hybride karakter, zodat er tevens bewijzen/getuigen kunnen zijn in het fysieke domein. Dat maakt een zaak kansrijker voor verdere afhandeling. Toch blijkt uit onderhavige analyse dat er bij een substantieel deel van de afgeronde persoonsgerichte zaken zonder gevolg in BOSZ niet duidelijk is wat er gebeurde in de verdere afhandeling. Mogelijk zijn er alternatieve interventies (waaronder een waarschuwing, stopgesprek, bemiddeling, enzovoort) ingezet, maar daarvoor bestaan weinig concrete aanwijzingen.[13]

12 Sextortion is hier buiten beschouwing gelaten omdat het te kleine aantallen betreft om betrouwbare uitspraken over te kunnen doen.

13 In de onderzoeksperiode (oktober 2022 tot en met september 2023) konden in de registratiesystemen van de politie ook geen alternatieve interventies worden ingevoerd. Inmiddels is dat wel het geval voor BOSZ (zie ook hoofdstuk 7).



Figuur 10 Afhandeling online fraude en persoonsgerichte delicten op basisteams (N=195)

3.5 Tot besluit

Op basis van de analyse in dit hoofdstuk kan worden geconstateerd dat het aandeel digitale criminaliteit op het totaal aantal aangiften dat bij de politie binnenstroomt tussen de 12% en 14% bedraagt, en dat dit een ondergrens is. In een eerdere studie van Ruiter en collega's (2024) blijkt dat 4% van alle BVH-registraties digitale criminaliteit betreft. Voorgaande constatering komt niet zozeer doordat er door uiteenlopende onderzoeksmethodieken variaties in aantallen registraties van digitale criminaliteit zijn gevonden, maar vooral door een verschil met betrekking tot het totaal aantal registraties waartegen onderzoeksbevindingen worden afgezet: specifiek meldingen/aangiften versus alle BVH-registraties. Door alle BVH-registraties als referentiepunt te nemen valt de vergelijking tussen meldingen en aangiften van traditionele, offline criminaliteit weg. Die vergelijking hebben wij wel willen maken.

Verder wordt in het genoemde rapport van Ruiter en collega's (2024) aangegeven dat bij 25% van de digitale registraties geen sprake bleek te zijn van een aangifte, maar van een melding. Figuur 4 laat eenzelfde percentage zien, met daarbij een toevoeging: vooral bij persoonsgerichte delicten (online bedreiging, smaad/laster, enzovoort) is er sprake van een hoog aandeel meldingen (rond de 70%). Bij fraude gaat het in 90% van de gevallen om aangiften. Het hoge aandeel meldingen bij persoonsgerichte delicten komt waarschijnlijk (deels) voort uit het feit dat er geen of weinig aanwijzingen zijn voor strafbare feiten en/of dat de politie, in overleg met het slachtoffer, een keuze voor alternatieve afdoeningen heeft gemaakt. Hierdoor is het mogelijk dat er uiteindelijk geen aangifte werd opgenomen.

4. Basisteams nader bekeken

4.1 Inleiding

Met politiemedewerkers van basisteams is tijdens het onderzoek uitvoerig gesproken over de impact die digitale criminaliteit op hun werkzaamheden heeft.[14] In dit hoofdstuk staan de ervaringen van deze medewerkers en hun basisteams centraal. Eerst worden de zes onderzochte basisteams afzonderlijk gekenschetst (4.2). Ieder team heeft namelijk zijn of haar eigen karakteristieken qua werkaanbod, inrichting en mogelijkheden. Daarna volgt een analyse van de rode draden van de ervaringen van de zes basisteams met het afhandelen van digitale criminaliteit. Aldus wordt een beeld geschetst van hoe basisteams handen en voeten geven aan het digitale werk en van de rol die digitale criminaliteit speelt binnen de gebiedsgebonden politie anno 2024 (4.3). Het hoofdstuk sluit af met een korte samenvatting (4.4).

4.2 Kenschetsen zes basisteams

4.2.1 *Team Noord*

Op dit basisteam, gelegen in ruraal gebied, wordt hard gewerkt om de basis op orde te krijgen. Ondertussen wordt men geregeerd door 'de waan van de dag'. Dat maakt vernieuwing, zoals het vormgeven van de digitale transformatie, lastig. Binnen het werkgebied spelen zaken als diefstal, inbraak, mishandeling, verdovende middelen de boventoon, naast problematiek rondom een nabijgelegen asielzoekerscentrum. Er ligt op basisteam-niveau momenteel geen concreet uitvoeringsplan voor de aanpak van digitale criminaliteit.

Bij het VVC-team komen dagelijks via verschillende kanalen vijftien tot twintig aangiften binnen. Daar zit frequent een zaak met een grotere of kleinere digitale component bij. Wanneer dit team een grotere zaak – denk aan een omvangrijke bankhelpdeskfraude met meerdere aangiftes – oppakt, krijgen medewerkers ondersteuning van een digitaal platform van de DR. Dit platform helpt bij het uitlezen van telefoons of computers en met het veiligstellen van beelden en digitale sporen.

14 Zie bijlage 4 voor de methodologie en aanpak van het onderzoek.

Verder beschikt het basisteam over een digitaal wijkagent die via sociale media contacten onderhoudt met burgers. Daarnaast houdt hij medewerkers van het basisteam op 'vlieghoogte' over de laatste ontwikkelingen op het gebied van digitale criminaliteit en digitale vaardigheden. De digitaal wijkagent heeft echter ook een fysiek werkgebied waar veel van zijn tijd naartoe gaat. Volgens verschillende respondenten loopt het basisteam achter op de kennis en kunde die noodzakelijk zijn om aangiften van digitale criminaliteit adequaat op te kunnen pakken. Dat heeft voor een groot deel te maken met het personeelstekort binnen het team, maar ook met het feit dat het basisteam geen prioriteit geeft aan het thema. Daardoor lukt het onvoldoende om online zichtbaar te zijn en de digitale werkzaamheden te integreren in het huidige politiewerk.

4.2.2 *Team Oost*

Het werkgebied van Team Oost bestrijkt voornamelijk een stedelijk gebied. Medewerkers zijn veel bezig met zaken rondom uitgaansgeweld, ondermijnende drugscriminaliteit, woninginbraken en verkeersveiligheid. Tijdens operationele overleggen gaat het veelal niet over digitale criminaliteit. Respondenten stellen dat het grootste deel van hun werk zich op de fysieke wereld richt. Tegelijk zijn zij zich bewust van een steeds groter wordend aandeel digitale delicten.

Het basisteam mist naar eigen idee een goede basis met betrekking tot digitale criminaliteit. In de praktijk krijgen strafrechtelijke delicten die lokaal – in de fysieke wereld – veel impact hebben voorrang. Naar schatting van respondenten komen er wekelijks enkele honderden zaken het basisteam binnen, waarvan minimaal 10% digitale criminaliteit betreft. Op eenheidsniveau streeft men ernaar om in de toekomst het doen van aangiften zo veel mogelijk online (via www.politie.nl) te laten plaatsvinden, tenzij er goede redenen zijn om dat niet te doen. In theorie zal dit 'verlichting' brengen in het aangifteproces, maar dan moet wel de kwaliteit van online aangiften omhoog.

Team Oost is zoekende naar hoe digitale criminaliteit het beste aan te pakken. Een respondent vindt dat de beoogde digitale transformatie 'pittig' is. De aanpak van digitale criminaliteit vergt gedragsverandering, anders werken dan voorheen – en dat lukt niet zomaar. Toch zijn er veel nieuwe ontwikkelingen. Het basisteam was begin 2024 bezig met het opzetten van een digi-team, dat bestaat uit een OS-A digitale transformatie, een digi-coach en twee digitaal wijkagenten. De taak van dit digi-team is om digitale bewustwording onder collega's te stimuleren, hen te ondersteunen en om contacten met slachtoffers te onderhouden. Het is niet de bedoeling dat de digi-specialisten zelf zaken gaan draaien. Zij zijn vooral een vraagbaak op het team. Er is inmiddels ook een digitale hulplijn opgezet die politiemedewerkers 24/7 kunnen bellen met operationele vragen over bijvoorbeeld phishing, WhatsApp-fraude en cryptovaluta. Verder is vanuit het Cybercrimeteam een digi-coach binnen het basisteam geplaatst die de basisteamrecherche ondersteunt. Ook werkt men aan de inrichting van een concrete

plek, een 'digi-punt', waar het toenemende belang van digitale opsporing en OSINT (het monitoren van sociale media) zichtbaar kan worden gemaakt.

Tot slot is sinds begin 2024 het project 'De Digitale Meldkamer' operationeel binnen het basisteam.[15] Daarbij stuurt de meldkamer noodhulpeenheden ter plaatse naar slachtoffers van digitale criminaliteit. Het doel van de digitale meldkamer is tweeledig: om opsporingskansen te vergroten en de dienstverlening richting burgers inzake digitale criminaliteit te verbeteren. Een bijkomend doel is om noodhulpagenten door 'learning-by-doing' beter op digitale criminaliteit toe te rusten. Zij worden in de praktijk getraind over de strafbaarstelling en het veiligstellen van digitale sporen. De werkwijze van deze digitale meldkamer lijkt aan te slaan, want:

> *'Het slachtoffer staat centraal. We merkten dat agenten daar juist iets willen betekenen, ondanks het feit dat ze niet altijd direct weten wat te doen. Veel agenten zijn 'fysiek' ingesteld.'* (aanjager Digitale Meldkamer Team Oost)

4.2.3 *Team Midden*

Het werkgebied van basisteam Midden beslaat een aantal gemeenten die allemaal een ander karakter hebben. Hierdoor kent het politiewerk een grote diversiteit. Per dag komen er twintig tot vijfentwintig zaken bij de casescreener van de basisteamrecherche (VVC-team) terecht waarvan het merendeel zich afspeelt in de fysieke wereld: verkeer, jeugdoverlast, geweld, drugs, diefstal en vernieling. Tegelijk bestaat, naar schatting van de medewerkers, rond 20 tot 30% van de zaken uit gedigitaliseerde criminaliteit en heeft rond wel de helft van de zaken een digitale component.

Alle zaken worden dagelijks op een triagetafel besproken, waarbij I&S, de casescreener, de OPCO (operationeel commandant van dienst), de zaakcoördinator en de kwaliteits-HOvJ aansluiten. Daar bespreekt men gezamenlijk het werkaanbod in het licht van de prioriteiten van het team. Aan bod komen onder andere de aan- of afwezigheid van opsporingsinformatie, datgene waar bij het opnemen van aangiften naar gevraagd moet worden, de omvang van de schade en de 'kansrijkheid' van zaken. Daarbij maakt het team gebruik van selectiviteitskaders en is er frequent overleg met een officier van justitie (OM). De teamchef noemt de triagetafel een belangrijk hulpmiddel voor het team om zaken omtrent digitale criminaliteit af te handelen:

> *'Dit is succesvol, omdat collega's bewust omgaan met zaken die binnenkomen. Er wordt in gezamenlijkheid over nagedacht en dat zorgt voor een gezamenlijk besluit, waarbij zowel de collega's op straat als opsporing betrokken is.'*

15 Zie in dit nieuwsbericht van meer informatie over deze aanpak binnen de eenheid Oost-Nederland: https://www.politie.nl/nieuws/2024/februari/2/02-oost-nederland-slachtoffers-sneller-geholpen-bij-digitale-criminaliteit.html

I&S-medewerkers hebben bij het opnemen van aangiften de beschikking over landelijke formulieren per type criminaliteit. Echter, het tekort aan I&S-medewerkers en de vele personeelswisselingen maken het lastig om alle kennis en kunde up-to-date te houden. Het basisteam beschikt wel over kartrekkers, waaronder de kwaliteits-HOvJ, die nieuwe ontwikkelingen in de opsporing aanjagen.

Wat de eenheid waar dit basisteam onder valt bijzonder maakt, is de aanwezigheid van een digitaal district. Dit district heeft richting de basisteams een 'vliegwielfunctie' ter advisering en ondersteuning van politiemensen, zoals wijkagenten en I&S-medewerkers, bij de aanpak en afhandeling van digitale criminaliteit. Naast eigen medewerkers kan het district hierbij ook een beroep doen op cybervrijwilligers: burgers die hun IT-achtergrond inzetten ter ondersteuning van de politie. Binnen het digitaal district zijn digitale platformen georganiseerd voor politiecollega's die concrete vragen hebben over de afhandeling van zaken. De platforms leveren ook kennis, expertise en documentatie over digitale criminaliteit.

Verder bestaat er een Team Digitale Opsporing (TDO) dat het basisteam kan assisteren bij onderzoeken van voornamelijk de DR. Op het TDO werken specialisten op onder andere cybercrime, plaats delict-assistentie, het (heimelijk) veiligstellen van gegevens en digitale opsporingsmethoden. Naast assistentie bij het uitvoeren van opsporingsonderzoeken fungeren deze specialisten ook als vraagbaak.

Bovendien is sinds 2024 Cyclops – een projectmatig team van de eenheid Midden-Nederland dat bestaat uit een mix van de basisteamrecherche, de DR en medewerkers op eenheidsniveau – operationeel.[16] Cyclops houdt zich bezig met cybercrime en gedigitaliseerde criminaliteit die te complex zijn voor het VVC. Daarnaast is een doel van Cyclops om een 'kennisimpuls' over cybercrime en gedigitaliseerde criminaliteit aan het basisteam te geven door een medewerker gedurende een halfjaar te laten meedraaien met de digitaal experts van de DR. Het idee daarachter is: 'Neem collega's mee in wat je kan', want 'dat werkt beter dan enkel de zaken samen bespreken op een tafel. We moeten het samen dóén' (digitaal specialist).

Op het Team Midden was een digitaal wijkagent werkzaam, maar die plek is momenteel niet ingevuld. Het team hoopt een nieuwe kracht te werven met als taken het oppikken van signalen van onder andere 'sociale onrust' op sociale media, meedraaien in opsporingsonderzoek en het met digitale expertise ondersteunen van de wijkagenten op straat. In navolging van de eerder genoemde pilot 'Digitale Meldkamer' gaan noodhulpagenten in deze eenheid – en dus ook in het basisteam – vaker ter plaatse bij een melding waarbij sprake is van digitale criminaliteit. Dat doen zij sinds april 2024 onder de noemer 'DigiPrio'.

16 Deze alinea is gebaseerd op een ongepubliceerde 'book of knowledge', waarin de ervaringen en werkwijze van het Cyclops-team zijn vastgelegd.

4.2.4 *Team Stad*

Dit basisteam, dat in een drukke binnenstad ligt, heeft te maken met veel dynamiek op straat: toeristen, uitgaansgeweld, demonstraties, ondermijning, evenementen en bewaken & beveiligen. Een van de medewerkers stelt: '*De urgentie in de buitenwereld is groot en vraagt veel van ons.*' Daardoor blijven er voor het team relatief weinig tijd en capaciteit over voor de aanpak van digitale criminaliteit. Duidelijk zicht op het aantal digitale zaken is niet aanwezig. De indruk is dat het 'digitaal bewustzijn' van het team achterloopt vanwege de enorme vraag naar politiecapaciteit in de binnenstad. Specifieke sturing op digitale criminaliteit binnen het basisteam ontbreekt. Speerpunten liggen bij de openbare orde en criminaliteit in de fysieke buitenwereld.

De inschatting van respondenten is dat de helft van de aangiften inmiddels een digitale component kent. In internetaangiftes van digitale criminaliteit ontbreekt vaak cruciale opsporingsinformatie en het team heeft geen capaciteit om aangevers na te bellen, waardoor zaken niet worden opgepakt. LMIO levert het team sporadisch pakketjes met aangiften aan. Dit soort zaken is echter wel meteen omvangrijk en daar loopt het basisteam snel tegen grenzen aan vanwege de tijd en menskracht die moet worden vrijgemaakt.

Team Stad heeft geen baliefunctie. Een naburig basisteam is wel open voor het publiek, maar er bestaat geen nauwe werkrelatie tussen beide teams. Er is op het basisteam met de baliefunctie wel een cyberexpert aanwezig die kan ondersteunen bij het opnemen van aangiften over digitale criminaliteit. Binnen het Team Stad screent een digitaal specialist dagelijks aangiften met een digitale component voor het hele district. Dit type aangiften krijgt op het VVC-team meestal een lage prioriteit, waardoor zaken niet (snel) worden opgepakt.

Volgens respondenten zijn de kennis en kunde over digitale delicten op het basisteam suboptimaal. De nadruk van het politiewerk ligt op het werk op straat. Medewerkers op het team krijgen relatief weinig te maken met zaken die een digitale component hebben, waardoor het hun aan routine ontbreekt. Binnen de eenheid is een gebrek aan helder beleid en aan opleidingsplaatsen, waardoor het voor het basisteam lastig is om voldoende digitale specialisten op het team te krijgen. Volgens respondenten heeft de eenheid geen gebrek aan expertise, maar die landt niet goed op het basisteam. Daarom kiest men ervoor collega's op de werkvloer via een zelf ingehuurde 'digi-coach' te ondersteunen. Ook investeert het basisteam in taakaccenthouders die digitale zaken oppakken en collega's ondersteunen.

Het basisteam beschikt niet over een eigen digitaal wijkagent. Wel heeft een digitaal wijkagent van een aanpalend basisteam zitting in een werkgroep die de digitale transformatie in het hele district begeleidt. Conform landelijk beleid krijgt deze transformatie gestalte in het optuigen van een 'digi-hub' met een aantal standalone laptops. De

hub is bedoeld om het onderzoek naar digitale criminaliteit te faciliteren en om sociale media te monitoren. Maar vooralsnog is het onduidelijk voor respondenten wat deze hub exact gaat brengen:

> *'Er is nog geen duidelijk idee over hoe invulling te geven aan de hub en er zijn onvoldoende specialisten om mensen hierin mee te nemen. Hier is kennis, kunde en capaciteit voor nodig.'* (digitaal specialist Team Stad)

Op het moment van schrijven is er een aantal politiemedewerkers aangenomen die de digitale transformatie op het basisteam verder gestalte gaat geven.

4.2.5 *Team Strand*

Dit basisteam heeft veel werk aan onder andere ambassades, internationale organisaties, dagelijkse demonstraties en ondermijning. Verder is er een werkaanbod aan veelvoorkomende criminaliteit, waaronder fietsdiefstal, winkeldiefstal, bedreiging en mishandeling. Vanwege personeelstekorten pakt de VVC voornamelijk prio1- en heterdaadzaken op. Er zijn twee senior-medewerkers opsporing op het VVC-team die, waar nodig, door de VVC van een aanpalend basisteam worden ondersteund. Dagelijks komen er veertig tot vijftig zaken bij het district binnen waarvan een 'aanzienlijk deel' een digitale component heeft – en dit aandeel lijkt toe te nemen.

De casescreeners van het basisteam zijn opgegaan in de DR en de werkvoorbereiding van de basisteams vindt in dit district dan ook bij de DR plaats. De werkvoorbereiding omvat, naast de screening en prioritering van zaken, het voldoen aan termijnverplichtingen, het bieden van ondersteuning, zoals het doen van vorderingen en het uitlezen van smartphones en andere digitale apparaten, het evenredig verdelen van werk over de betreffende basisteams, en het monitoren van zaken. Bij de DR is er een medewerker die socialemediakanalen scant (OSINT) op de gebruikersprofielen van verdachten en op het opsporen van digitale criminaliteit.

De zaken betreffende digitale criminaliteit worden door het basisteam niet altijd in behandeling genomen. Dit heeft te maken met beperkte recherchecapaciteit, geldende prestatieafspraken en selectiviteitskaders. Alle cyberzaken en zaken met betrekking tot Centurion-feiten worden voorgelegd aan een cyberofficier. Deze officier bepaalt welke zaken voorrang krijgen. De afhandelunit van het basisteam verwerkt nauwelijks digitale criminaliteit, dit omdat de focus op heterdaadzaken ligt.

Het is voor I&S-medewerkers op het basisteam niet eenvoudig om de ontwikkelingen rondom gedigitaliseerde criminaliteit en cybercrime bij te benen. I&S-medewerkers worden door cyberexperts wel van de benodigde kennis voorzien. Zij werken zo veel mogelijk met standaardvragenlijsten voor verschillende vormen van veelvoorkomende online criminaliteit. Voorafgaand aan de aangifte hebben I&S-medewerkers contact

met burgers over het bewaren van gegevens en het niet (per ongeluk) wissen van bestanden op hun telefoons en computers.

Het basisteam beschikt nog niet over een digitaal wijkagent. De wens om er een aan te nemen bestaat wel, waarbij de inrichting van deze functie en de verbinding met andere wijkagenten een onderwerp van gesprek is. De jeugdagent op het basisteam houdt zich echter al stevig bezig met digitale criminaliteit. Er zijn namelijk signalen dat jongeren in de wijk zich bezighouden met online dealen en heling en met cyberpesten.

4.2.6 *Team Zee*

Dit team, gesitueerd in een stedelijk gebied met een zeehaven binnen het werkgebied, moet prioriteit geven aan veelvoorkomende en ondermijnende criminaliteit. Daardoor is er minder tijd over dan dat men zou wensen voor digitale delicten en de digitale transformatie. Binnen het basisteam heeft de aanpak van gedigitaliseerde criminaliteit en de digitale transformatie op papier prioriteit, maar op de werkvloer is er '*nog weinig beweging*'. Politiemedewerkers focussen hoofdzakelijk op criminaliteit in de fysieke buitenwereld. Medewerkers van het team schatten dat 25 tot 40% van de zaken die het basisteam verwerkt een 'aanzienlijke' digitale component heeft. Een casescreener wijst op de hoeveelheid online fraudezaken die het team allemaal probeert op te pakken, maar wat niet lukt vanwege capaciteitsgebrek. LMIO-zaken zijn er ook. Die worden veelal afgedaan met een waarschuwingsbrief in combinatie met een gesprek.

Ook bij dit team blijkt dat respondenten van mening zijn dat niet alle collega's er voldoende van op de hoogte zijn hoe met digitale criminaliteit om te gaan. Een respondent meldt dat zij '*geen specialisten*' zijn. Het ontbreekt I&S-medewerkers aan een duidelijk aanspreekpunt als ze vragen hebben of als ze vastlopen. Een ander probleem bij I&S is dat de wachttijd voor het doen van een aangifte flink kan oplopen. Een casescreener merkt op dat aangiften van gedigitaliseerde criminaliteit sneller worden afgewezen dan van traditionele delicten. Hij benoemt dit als een '*ethisch lastige keuze*' waar het team voor staat. Impactvolle zaken worden niet altijd opgepakt vanwege het lage schadebedrag, terwijl: '*Honderd euro is voor iemand die niet kan rondkomen zonder die honderd euro heel veel geld.*'

Daarnaast is er bij het VVC-team relatief weinig expertise op het terrein van digitale criminaliteit aanwezig. De ruimte om deze te ontwikkelen is ook niet vanzelfsprekend. Eén van de VVC-medewerker geeft aan vanuit eigen interesse de zaken op te pakken, in eigen tijd kennis bij te spijkeren en op eigen initiatief een OSINT-opleiding te volgen. Wel is er een digitaal wijkagent op het basisteam aangesteld. Deze wijkagent is actief op sociale media en houdt zich met OSINT bezig. Het team beschikt vooralsnog niet over een digihub, omdat het aanvragen van de benodigde financiële middelen stroef verloopt.

4.3 Rode draden door de basisteams

4.3.1 *Impact van digitale criminaliteit op de basisteams*

Uit de kenschetsen van de basisteams wordt duidelijk dat de prioriteit op basisteams voornamelijk ligt bij de aanpak van traditionele en fysieke vormen van criminaliteit. De meeste capaciteit gaat bovendien naar heterdaadzaken. Hierdoor lopen andere zaken, waaronder digitale criminaliteit, een hoger risico om te blijven liggen. Digitale criminaliteit is er in de loop van de tijd voor de politie 'bij gekomen' en heeft zeker de 'klassieke' criminaliteit niet vervangen. Niettemin maakt digitale criminaliteit inmiddels een substantieel, en een steeds groter wordend, deel uit van het werkaanbod van de onderzochte basisteams. Ook al is de wijze van afhandelen – van aangifte tot en met opsporing – niet wezenlijk anders dan bij klassieke delicten, de modus operandi van verdachten is dat wel. Bovendien worden informatie en bewijs via andere – veelal digitale - wegen verzameld. Digitale criminaliteit vergt van basisteams dus een andere mindset en aanpak. Daar zit voor veel teams een vraag: hoe die goed vorm te geven?

Qua omvang van het werkaanbod lopen de schattingen uiteen, maar respondenten schatten dat ergens tussen de 10 en 30% van het totaal aan aangiften dat op basisteams binnenkomt digitale criminaliteit betreft. Men spreekt van een '*frequent*' aanbod of een '*aanzienlijk deel*' van het werkaanbod. In het bijzonder is het aandeel online fraudezaken, waaronder aan-en verkoopfraude, hulpvraagfraude en bankhelpdeskfraude, groot. Verder zijn er persoonsgerichte delicten, zoals online bedreiging, die zich met regelmaat aandienen.

Ook veel traditionele criminaliteit kent tegenwoordig een digitale component. Sommige respondenten durven zelfs te stellen dat er in elke zaak wel een digitale component zit. Volgens schattingen van casescreeners en rechercheurs heeft in ieder geval rond de helft van de binnenkomende aangiften en meldingen een substantiële digitale kant. Bij deze hybride vormen van criminaliteit vervagen de grenzen tussen 'fysiek' en 'digitaal'. Ter illustratie: in menige bedreigings- of stalkingzaak wordt voor het plegen van het strafbare feit niet alleen gebruikgemaakt van fysieke middelen, maar ook vaak van sociale media of andere digitale kanalen.

De op het fysieke domein getrainde en ervaren basisteams worden geacht het digitale werk voortvarend op te pakken. Tijd, aandacht en capaciteit voor de aanpak hiervan is echter vaak beperkt – een sluitstuk zelfs. Toch leeft onder medewerkers van de onderzochte basisteams alom het besef dat digitale criminaliteit inmiddels een vorm van veelvoorkomende criminaliteit is. Hoe met dit besef om te gaan, blijft een worsteling: respondenten willen enerzijds een zichtbare en aanwezige politie op straat blijven, maar er anderzijds voor de burgers in hun werkgebied ook op het digitale vlak zijn.

4.3.2 *Belang van blauwe teams in de aanpak digitale criminaliteit*

De rol die basisteams spelen in de aanpak van digitale criminaliteit was, en wordt, nog steeds, onderschat binnen de politie, zo is de indruk van mening respondent. De nadruk binnen het beleid en de inrichting van basisteams ligt in eerste instantie op hun fysieke aanwezigheid in, en kennis van, het eigen werkgebied. Tot voor kort was er weinig tot geen specifieke aandacht voor de rol van basisteams in de aanpak van digitale criminaliteit. De nadruk lag in eerste instantie op de aanpak van cybercrime door gespecialiseerde teams. En nog steeds is op basisteams zelf de aandacht voor 'het digitale' in beperkte mate aanwezig; het blijkt veelal niet in plannen verankerd. Wel wordt op alle onderzochte blauwe teams ingezet op bewustwording rond digitale criminaliteit en werkt de politie op pragmatische wijze aan het scheppen van randvoorwaarden voor de aanpak hiervan binnen de eigen mogelijkheden. Dit in navolging van initiatieven zoals Centurion en de Digitale Transformatie. Hiermee komt een zeer gemêleerd beeld naar voren van basisteams die ieder een eigen snelheid in hun digitale ontwikkeling volgen.

Respondenten leggen op welhaast vanzelfsprekende wijze de link tussen 'fysiek' en 'digitaal' politiewerk. Ze maken het digitale fysiek (en vice-versa), vanwege het fysieke contact met slachtoffers en/of verdachten in hun werkgebied. Vanuit dit contact is het – in ieder geval voor basisteams zelf – meer dan duidelijk dat ze van grote waarde (kunnen) zijn in de aanpak van digitale delicten. Basisteams staan binnen de politie het dichtst bij de burger. Zij zijn de eerste toegang en het eerste aanspreekpunt voor slachtoffers, kennen en verhoren (veelal) lokale verdachten en hebben specifieke kennis van het eigen werkgebied. *'Fraude vindt bijvoorbeeld vaak plaats door personen die bij wijkagenten al in beeld zijn omdat ze bijvoorbeeld ook winkeldiefstallen plegen,'* aldus een casescreener.

Medewerkers van basisteams, en met name de agenten op straat, hebben een signalerende rol en zijn van belang in het onderhouden van connecties met lokale partners. Wijkagenten zien en onderkennen problemen in de wijk rond digitale criminaliteit, zoals geldezels en herhaald slachtofferschap. Naar eigen zeggen kunnen zij er vaak (te) weinig tijd aan besteden, ook al zien wijkagenten het toenemend belang van het digitale domein en delicten daarbinnen in. Wat betreft de inzet van digitaal wijkagenten zijn er grote verschillen tussen de onderzochte basisteams zichtbaar. Ten eerste heeft niet ieder team een digitaal wijkagent. Ten tweede is niet altijd voor ieder helder wat zijn of haar werkzaamheden zijn: gaat het om het beheren van de socialemedia-accounts van het team of ook om de afhandeling en eventueel preventie van digitale criminaliteit?

Qua opsporing ligt de rol van basisteams in het afhandelen van 'kort-cyclische' en 'eenvoudige' zaken. Dit is van oudsher corebusiness van de basisteamrecherche (of het VVC-team). Ook veel digitale criminaliteit behoort in eerste aanleg tot de categorie

'eenvoudige zaken'. Denk aan het afhandelen van een 'simpele' aan- en verkoopfraude, waarbij een stopgesprek met een verdachte volstaat. Een groot deel van de digitale criminaliteit is echter schaalbaar en al snel complex, bijvoorbeeld waar sprake is van meerdere slachtoffers en/of daders verspreid over meerdere werkgebieden en/of eenheden. Dergelijke zaken zijn omvangrijk en blijken niet eenvoudig te behappen voor afzonderlijke basisteams.

Door de werkwijze van Centurion hebben basisteams wel een taak in de afhandeling van schaalbare criminaliteit. Sommige teams krijgen 'af en toe' of 'sporadisch', maar andere teams juist 'met regelmaat' zaken van LMIO aangeleverd. Dit zijn zaken met aangiften tegen één verdachte woonachtig binnen het werkgebied van de basisteams. Meestal gaat het om 'hapklare' aan- en verkoopfraude zaken, waardoor de benodigde handelingen voor het VVC-team beperkt blijven tot het aanhouden en verhoren van de verdachte(n). Soms blijken de pakketjes minder kant-en-klaar als verwacht of blijkt het om een grote zaak te gaan, waarvoor additioneel analyse- en uitzoekwerk nodig is. Meerdere teams geven aan dat de verwerking van LMIO-zaken daardoor alsnog veel capaciteit kost.

4.3.3 *'Bottom-up' ontwikkeling en innovatie op 'diverse snelheden'*

Tijdens het onderzoek kwamen diverse initiatieven en acties naar boven die vanuit basisteams of eenheden lokaal zijn ontwikkeld. Hiermee hopen zij de aanpak van digitale criminaliteit te bevorderen. Veelal zijn deze initiatieven gericht op het verbeteren van politie-interne samenwerking en werkprocessen. Eerder kwamen al Cyclops, De Digitale Meldkamer en DigiPrio aan de orde. Daarnaast zijn op diverse teams de inzet van cybervrijwilligers en digitale experts voorbijgekomen. Ook organiseren afzonderlijke eenheden informatiemiddagen en seminars om digitale kennis te delen en te verspreiden, en zijn er specialistische hulp(telefoon)lijnen en informatieproducten opgetuigd.

Elk basisteam is uniek in hoe zaken zijn georganiseerd. Dit is afhankelijk van het werkaanbod in de eigen wijk, de samenstelling van het basisteam en de wijze waarop de eenheid is ingericht en georganiseerd. Daardoor bestaan er flinke verschillen in de digitale transformatie die door de politie wordt nagestreefd. Er zijn teams die focussen op '*kleine stapjes*', waar men spreekt over '*het maken van een inhaalslag*' of stelt: '*het is een olietanker en verandering gaat langzaam*'. Er zijn echter ook teams waar de transformatie voortvarender verloopt. Daar verandert er daadwekelijk iets aan de inrichting en interne samenwerking rondom de aanpak van digitale criminaliteit en komen er innovatieve praktijken van de grond, veelal met steun en facilitering vanuit de eigen eenheid.

Ieder onderzocht basisteam zit in een andere fase van de digitale transformatie en geeft naar eigen inzicht vorm aan de aanpak van digitale criminaliteit. Zo doet het ene team

goede ervaringen op met dagelijkse triage van (een beperkt aantal) zaken, samen met een kwaliteits- HOvJ. Tegelijk werkt het andere team met roulerende casescreeners om het werk behapbaar te houden. Niet ieder team heeft een digitaal wijkagent of een kwaliteits-HOvJ, niet overal is er een taakaccenthouder voor digitale zaken aanwezig, en evenmin beschikt ieder team over een digi-hub of digi-kamer om expertise te halen en te delen met collega's. Ook beschikt niet iedere eenheid over een zogenoemde Centurion-hub, een team waar kansrijke zaken kunnen worden opgewerkt alvorens ze bij een VVC-team of DR terechtkomen. Dit zijn wel allemaal zaken en ambities waaraan wordt gewerkt of waarnaar wordt gestreefd.

Vooralsnog overheerst het beeld dat basisteams zich op diverse snelheden ontwikkelen. Daaruit komen waardevolle ervaringen naar voren die lokaal (of op eenheidsniveau) voorzien in een behoefte die er blijkbaar is. Tegelijkertijd leeft er een 'houtje-touwtje-gevoel' onder de respondenten. Zij missen vanaf centraal niveau een eenduidige sturing op de expertise, toerusting en werkverdeling die nodig zijn voor de effectieve aanpak van digitale criminaliteit, maar ook op zaken zelf wordt sturing en coördinatie gemist.

4.3.4 *'Er zijn' voor de burger*

Medewerkers van basisteams zien en spreken geregeld slachtoffers en horen daardoor hun verhalen uit de eerste hand. Het besef dat de impact van digitaal slachtofferschap groot kan zijn is er dan ook wel degelijk. Een digitaal specialist geeft aan: '*We rennen als politie naar een winkeldiefstal, maar moeten digitale zaken afwegen via een selectiviteitskader. Als je kijkt naar de impact van het één en het ander, dan is dat lastig.*' Bij digitale zaken die de politie – noodgedwongen – moet afwijzen, kan het gevoel spelen '*je mensen in de steek te laten*'. Dit gevoel van tekortschieten kwam in gesprekken met respondenten regelmatig naar voren. Een casescreener geeft aan ernaar te streven de 'maatschappelijke context' mee te nemen in zijn afweging:

> *'Het kan zijn dat iemand die tienduizenden euro's verliest na beleggingsfraude dit nauwelijks mist, terwijl oplichtingszaken in arme wijken voor minder geld veel grotere gevolgen hebben omdat mensen direct in de financiële problemen komen.'*

Van politiemedewerkers wordt verwacht dat er tijdens gesprekken met slachtoffers wordt doorgevraagd, zodat aangiften volledig zijn. Persoonlijke aandacht is daarbij altijd van belang, zeker bij delicten met een persoonsgerichte component. Het (h)erkennen van slachtofferschap van een digitaal delict kan echter lastig zijn. Hierbij speelt mee dat sommige slachtoffers van digitale criminaliteit niet altijd begrijpen, laat staan in een internetaangifte kunnen verwoorden, wat hen is overkomen en van welk strafbaar feit ze het slachtoffer zijn. Maar ook wordt er tijdens het opnemen van aangiftes op het bureau niet altijd voldoende doorgevraagd. Het kan daarbij voorkomen dat een slachtoffer wél meer weet heeft van hoe een en ander in z'n werk gaat dan de politieme-

dewerker aan de balie: '*Vaak heeft de aangever meer verstand van de verschijningsvorm dan wij.*' (medewerker VVC).

4.3.5 *Keuzes, eigenaarschap en behapbaarheid*

Meldingen van digitale criminaliteit komen na internetaangiftes bij de basisteams terecht. Daarnaast stromen zij via telefonische of fysieke aangiften op de teams in. Ook zijn er 'pakketjes' aangiften die via LMIO binnenkomen. Het is voor basisteams ondoenlijk om al deze zaken op te pakken. Er moeten keuzes worden gemaakt en daarvoor gebruiken casescreeners toewijzingskaders, selectiviteitskaders en/of prioriteringstools. Ook al wordt er gestreefd naar landelijke uniformiteit in het hanteren van deze kaders, per team blijkt het net weer even anders welk kader op welke wijze wordt gebruikt. De selectiviteitskaders blijven echter van belang bij het scheppen van orde in het aanbod. Want '*qua delicten heb je op een basisteam veel appels en peren*', zo stelt een respondent.

Een screener beoordeelt de binnenkomende zaken aan de hand van een van de geldende kaders en tools op de vraag of een zaak zal worden opgepakt of afgewezen. Zij stellen dat zaken vaak niet worden opgepakt door gebrek aan opsporingsinformatie of daderkenmerken, omdat deze in internetaangiftes ontbreken en er geen tijd is om (alle) aangevers na te bellen. Bewijsmateriaal wordt pas veiliggesteld als er een onderzoek is gestart, wat weken na aangifte kan zijn. Daardoor gaat 'het momentum' voorbij en gaan sporen verloren.

In het screeningsproces worden constant keuzes gemaakt over toewijzing en afwijzing. Aan dat proces geven basisteams eigen invulling. Op het ene team is sprake van een dagelijks triagemoment, op een ander team werkt men met een maandelijkse 'sprint'. Hierbij worden er via de 'scrum-methode' vijfentwintig zaken geselecteerd waarmee het VVC-team de komende vier weken aan de slag gaat. Ook beschikt het ene team over een vaste screener, terwijl een ander team met roulerende casescreeners werkt.

Een ander punt is dat het voor respondenten niet altijd duidelijk is waar 'het eigenaarschap' van digitale zaken ligt. Basisteams zijn zoekende in de samenwerking met het cybercrimeteam, DR en DRR. Het risico op 'tussen wal en schip' geraken van zaken is hierdoor aanwezig. Daarom leeft op basisteams de vraag: wat als een zaak ons team ontstijgt, wie pakt zulke zaken dan op? Meerdere respondenten melden dat ze moeite hebben zaken te *'slijten'* of dat er sprake is van '*gesoebat'* of '*geping-pong'* tussen teams over wie een zaak gaat oppakken:

> *'Je hebt soms een zaak die tussen district en het basisteam in valt. Dan gaan we met elkaar in overleg en dan willen we wel samenwerken, maar dat is niet vanzelfsprekend.'* (medewerker Team Midden)

Met name grotere zaken met meerdere slachtoffers en/of verdachten, en team- en eenheidsgrenzen overschrijdende zaken, ontgroeien snel de scope van een VVC-team. Zeker waar sprake is van grensoverschrijdende internationale criminaliteit, buitenlandse rekeningen worden gebruikt en internationale rechtshulpverzoeken aan de orde zijn, worden deze op basisteams meestal op voorhand afgewezen. Dergelijke zaken vergen veel inzet, duren lang, en lopen vaak op niets of op een sepot uit, aldus de ervaringen van respondenten.

Toch pakken VVC-teams grote zaken soms op, omdat die anders tussen wal en schip zouden kunnen vallen. Zo kan het gebeuren dat binnen meerdere teams tegelijkertijd aan dezelfde zaak wordt gewerkt. Daarover vertelt een medewerker van een VVC-team:

> *'Een vrouw werd opgelicht voor een bedrag van 4.000 euro en 6.000 euro aan sieraden. Als basisteam wilden we die zaak oppakken en er kwam een zaaksofficier op de zaak. Al snel werd duidelijk dat elders collega's bezig waren met dezelfde verdachte. Deze zaak ging naar dat andere team omdat zij net iets verder waren. Het nadeel is wel dat wij doorhadden dat het hier om een geldezel ging en het andere team niet voornemens was om naar de achterliggende daders te gaan kijken. Zo jammer, maar ja, je moet zaken afbakenen.'*

Ondanks de komst van een nationale politie is er nog steeds sprake van 'hokjes denken'. Ook is er is (nog) geen handboek voor welke zaak door welk team (BT, DR, CCT, enzovoort) opgepakt zou moeten worden. Bovendien voeren basisteams doorgaans niet de bredere zoekslagen naar aanleiding van aangiftes uit om te zien of er elders in het land meerdere slachtoffers met identieke verdachten of modus operandi zijn. Het gevoel vanuit basisteamperspectief is dat veel van deze grotere zaken uiteindelijk in een '*zwart gat'* verdwijnen.

Medewerkers op basisteams geven aan op voorhand graag meer betrokkenheid te wensen van het OM in het meedenken en meebepalen van de 'kansrijkheid' van zaken. Politie en OM hebben elkaar nodig om goede keuzes te maken, niet alleen op basis van afdoeningscijfers, maar ook geredeneerd vanuit maatschappelijke impact. Respondenten op alle onderzochte teams ervaren dat digitale criminaliteit, waaronder de via Centurion gerouteerde zaken, vaak eindigt in een sepot. Waar het OM nauw betrokken is bij de triage zijn daar goede ervaringen mee:

> *'We verhoren verdachten pas wanneer zaken kansrijk zijn. Zo gaan we efficiënter om met capaciteit, juist ten behoeve van de burger.'* (teamchef Team Midden)

Het kan zo zijn dat OM en politie hierdoor wél kiezen voor een zaak met hoge impact op het slachtoffer in plaats van een zaak met een hoog schadebedrag.

4.3.6 *Toegerust zijn op digitale criminaliteit*

Het daadwerkelijk opbouwen van digitale expertise op basisteams lijkt voorbehouden aan enthousiaste individuen. Niet alle medewerkers op basisteams zijn toegerust om goed met digitale criminaliteit om te gaan. De afhandeling van deze zaken vraagt om bepaalde – digitale – vaardigheden. Er moet bijvoorbeeld opsporingsinformatie van een smartphone of van een socialemediaplatform worden gehaald. Vooral bij de hoeveelheid digitale platforms die er tegenwoordig zijn, is het vorderen van gegevens bij internationale en anonieme organisaties niet eenvoudig.

Er leeft onder politiemedewerkers ook 'terughoudendheid' of 'koudwatervrees' ten aanzien van de digitale vormen van criminaliteit. Het is voor veel medewerkers lastig om de – snelle – ontwikkelingen rondom gedigitaliseerde criminaliteit en cybercrime bij te benen. Ontwikkelingen vergen elke keer weer nieuwe informatie en '*groeien medewerkers snel boven de pet*'. Denk bijvoorbeeld aan de vele verschijningsvormen en classificaties van digitale criminaliteit die bovendien vaak op elkaar lijken en elkaar kunnen overlappen. Daarnaast biedt het Wetboek van Strafrecht ook weer andere indelingen.

Basiskennis over digitale criminaliteit wordt verondersteld aanwezig te zijn bij alle basisteammedewerkers, maar dat is (nog) niet het geval. Respondenten ervaren een gebrek aan training en opleiding. Zij worden geacht vooral zelf de benodigde kennis bij te spijkeren. Een medewerker van een VVC-team heeft daarom af en toe het gevoel '*aan het zwemmen*' te zijn. Voor I&S-medewerkers geldt dat zij een goede aangifte kunnen opnemen van een breed scala aan delicten met diverse verschijningsvormen, inclusief soms gecompliceerde digitale delicten over bitcoins en cybercrime. Voor verschillende vormen van veelvoorkomende digitale criminaliteit (zoals online fraudezaken) werken zij met vragenlijsten als hulpmiddel. De ervaringen daarmee verschillen van *'positief'* tot '*niet fijn*' – of: '*het maakt een onbeholpen indruk*' om tijdens een aangifte een lijst te moeten raadplegen. In de praktijk blijkt dat deze lijsten niet standaard overal worden gebruikt.

Tegen deze achtergrond hebben respondenten behoefte aan meer opleiding, training en scholing. Dit wil niet zeggen dat iedere medewerker op een basisteam over dezelfde digitale vaardigheden en expertise moet (gaan) beschikken. De aanwezigheid van digitale experts, taakaccenthouders, cybercrimeteams en kennisproducten helpt, vooral als zij laagdrempelig en liefst in interpersoonlijk contact beschikbaar zijn. De beschikbaarheid en toegankelijkheid van deze 'hulplijnen' wisselt echter van team tot team. Een medewerker van een VVC-team vertelt meldingen van fraude met bitcoins lastig te vinden en baat te hebben bij een kundige collega of hulp vanuit een digitaal platform of cybercrimeteam. Tegelijk zegt een andere VVC-medewerker vaak niet te weten waar hij terechtkan met vragen; het is niet altijd duidelijk '*wie je waarvoor moet hebben*'.

Dit laatste heeft ermee te maken dat veel specialistische teams en platforms binnen de politie met digitale criminaliteit bezig zijn. Hierbij weegt mee dat, zoals beschreven, de wijze waarop de digitale transformatie per basisteam handen en voeten krijgt verschilt. Dat heeft gevolgen voor de aan- of afwezigheid van taakaccenthouders en digidagen, maar ook voor faciliteiten als bijvoorbeeld een digikamer. Ondertussen is er binnen de landelijke politie een grote hoeveelheid aan informatieproducten en tools beschikbaar gekomen die gaan over digitale criminaliteit en digitale vaardigheden. Menig medewerker heeft het over '*een oerwoud*' of '*door de bomen het bos niet meer goed kunnen zien*' in de hoeveelheid factsheets, platforms, informatiekanalen, handboeken, tips en tricks, vragenlijsten en webinars. Daarnaast wordt veel informatie via de mail en intranet gedeeld, maar die wordt lang niet altijd gelezen. Daarom schakelen respondenten het liefst via 'korte lijntjes'; zij zoeken (en vinden) expertise via persoonlijk contact. Zij bellen liever met een bekende collega dan op intranet een zoektocht te beginnen. Een respondent verwoordde het kort maar bondig: '*Kennis maakt macht, maar kennissen maken machtiger.*'

Wat basisteams nodig hebben, is gerichte toerusting op het 'blauwe digitale vak'. Op datgene wat nodig en functioneel is in het licht van 'de blauwe rol' bij de aanpak van digitale criminaliteit. Naast opleiding en expertise gaat het hierbij ook om 'gerichte intelligence' die door respondenten wordt gemist. Meerdere basisteams zeggen dat ze gebaat zouden zijn bij meer betrokkenheid vanuit intelligencemedewerkers om digitale zaken beter in beeld te brengen, te verrijken en nader te kunnen duiden. '*Er ligt veel informatie in de systemen,*' aldus een casescreener. Tot slot geven respondenten mee dat het 'echte' politievak in de praktijk geleerd moet worden. Dat geldt voor zowel fysieke als digitale criminaliteit: door met slachtoffers in aanraking te komen, incidenten af te handelen, onderzoeken te draaien – simpelweg door *'iets met digitale criminaliteit te moeten*'. Zodoende kunnen medewerkers op basisteams '*digitale vlieguren maken*' en raken zij beter toegerust voor hun werk.

4.4 Tot slot

De kenschetsen van de zes onderzochte basisteams en de rode draden uit hun ervaringen geven een gemêleerd beeld van de lokale politiepraktijk ten aanzien van digitale criminaliteit. Een constante die door de beschrijvingen heen zichtbaar wordt, is dat hoewel de focus (nog) hoofdzakelijk ligt op de fysieke vormen van criminaliteit er meer en meer van basisteams gevraagd en verwacht wordt. Basisteams zijn op het digitale vlak in beweging, veelal organisch en zonder strak vooropgezet plan, al dan niet met ondersteuning vanuit hun eigen eenheid. Zij ontwikkelen – veelal 'bottom-up' – werkwijzen die binnen de eigen wensen en mogelijkheden liggen. Sommige teams opereren hierbij steviger en voortvarender dan andere. Eenduidige sturing en toerusting vanuit het nationale niveau zou volgens respondenten helpen om de aanpak van digitale criminaliteit naar een hoger plan te tillen. Tot op heden blijft de digitale transformatie een ontwikkeling die binnen basisteams op verschillende snelheden plaatsvindt.

5. Reconstructies van digitale zaken op basisteams

5.1 Inleiding

Zoals in hoofdstuk 3 uiteengezet stroomt naar schatting rond 41% van het digitale werkaanbod van de politie in via de basisteams; rond 67% van het totale digitale werkaanbod wordt op basisteams afgehandeld. Om meer zicht te krijgen op hoe de basisteams in de dagelijkse praktijk aangiften en meldingen van digitale criminaliteit verwerken, zijn 77 zaken van de zes aan dit onderzoek deelnemende basisteams geanalyseerd.[17] Aan de teams is gevraagd om drie zaken aan te leveren: een LMIO-zaak, een zaak waar men 'trots' op is en een zaak met 'leerpunten'. Daarnaast zijn per team tien zaken geselecteerd uit de periode oktober 2022 tot en met september 2023. Hierbij is gelet op een zo representatief mogelijke verdeling naar typen digitale criminaliteit. Van alle zaken zijn reconstructies gemaakt vanaf het moment van melding of aangifte.

Dit hoofdstuk beschrijft de rode draden die naar voren komen uit de analyse van de 77 zaken, aangevuld met de reflectie op, en duiding van, de bevindingen door medewerkers van de zes onderzochte basisteams. De volgende paragrafen behandelen zeven thema's: het herkennen en onderkennen van digitale criminaliteit (5.2), keuzes maken in zaken (5.3), samenwerking in zaken (zowel binnen de politie als met externe partijen) (5.4), het omgaan met schaalbare criminaliteit (5.5), de afloop en resultaten van zaken (5.6), het omgaan met slachtoffers (5.7) en het omgaan met verdachten (5.8). Het hoofdstuk eindigt met een korte impressie van inzichten en bevindingen (5.9).

5.2 Herkennen van digitale criminaliteit

5.2.1 *Veel verschijningsvormen*

Er komt bij basisteams een breed scala aan digitale delicten binnen, waaronder ook zeer complexe. Het blijkt dat het voor politiemedewerkers soms wel, maar veelal niet, eenvoudig is om het digitale werkaanbod direct te herkennen en te classificeren. Er zijn

17 Zie bijlage 5 voor de methodologie en aanpak van de zaakreconstructies.

vele 'maatschappelijke klassen'[18] waaronder digitale criminaliteit kan worden weggezet. Daarbij gaat het bij dit type criminaliteit vaak om telkens veranderende modus operandi, fenomenen, verschijningsvormen, gebruikte digitale middelen en platforms. Hierdoor leeft onder politiemedewerkers het gevoel dat er met de digitalisering van criminaliteit een nieuw soort strafbaar feit bij is gekomen. Het vergt kennis en doorvragen om patronen in zaken te doorzien en te begrijpen wat voor delict er al dan niet heeft plaatsgevonden.

De classificatie die aan een melding of aangifte wordt gegeven, de zogenoemde 'maatschappelijke klasse', is niet altijd de best passende. Binnen de 77 gereconstrueerde zaken was dit in twaalf van de zaken het geval. Ook waren er acht zaken waarbij, achteraf gezien, een andere classificatie voorhanden was. Zo blijkt iets wat als identiteitsfraude of beleggingsfraude wordt geregistreerd, eigenlijk cybercrime te betreffen. Verder zijn er algemene mutaties die stalking of sextortion betreffen, maar wat bij nader inzien een ruzie/twist blijkt te zijn waarbij sprake is van sexting. Medewerkers van de basisteams herkennen deze observatie:

> *'De een schijft een zaak weg onder horizontale fraude, terwijl de ander zegt: dit valt onder diefstal.'* (terugkoppelsessie Team Zee)

Een digitaal delict kan vaak onder meerdere klassen worden weggeschreven en daar worstelen basisteams in de praktijk mee.

Ook al komt men er meestal wel uit, politiemedewerkers geven aan dat er regelmatig discussie over mutaties is: wat is er nu precies aan de hand? Gaat het om cybercrime of om gedigitaliseerde criminaliteit – en welk type delict dan exact? Deze onduidelijkheid heeft mede te maken met onvolledige informatie. Slachtoffers weten vaak niet alle relevante feiten en omstandigheden te benoemen bij het reconstrueren van wat hen (zojuist) is overkomen. Zeker internetaangiftes blijken geregeld onvolledig. Het stellen van de juiste vragen over feiten, omstandigheden en opsporingsindicaties door politiemedewerkers is dus nodig. Dit vergt doorvragen en – idealiter – het (tijdig) ter plaatse gaan bij een slachtoffer om snel gerichte actie te kunnen ondernemen en digitale sporen veilig te stellen.

5.2.2 *Bijblijven*

De kennis en kunde op gebied van digitale criminaliteit – en nieuwe ontwikkelingen daarbinnen – is niet bij iedere politiemedewerker en bij ieder basisteam hetzelfde (zie ook hoofdstuk 4). Van medewerkers, zowel aan de balie als bij recherche, wordt verwacht dat ze zichzelf in- en bijlezen en dat ze ontwikkelingen bijhouden. Bovendien

18 Incidenten worden binnen de politie aan de hand van 'maatschappelijke klassen' geclassificeerd in het registratiesysteem BVH weggeschreven.

zijn er hulpmiddelen, zoals vragenlijsten, bij de balies van basisteams voorhanden, maar die worden niet altijd en overal en door iedereen gebruikt. Voor veel medewerkers is digitale criminaliteit mede daardoor onbekender terrein dan traditionele criminaliteit.

Het 'complexe' gaat echter van zaken af naarmate politiemedewerkers er meer bekend mee zijn. Aangiften of meldingen van digitale criminaliteit hoeven niet voor iedereen en in alle gevallen moeilijk te zijn. Online aan- en verkoopfraude is bijvoorbeeld relatief eenvoudig af te handelen. Dus hoe meer politiemedewerkers met digitale criminaliteit te maken hebben, hoe beter zij zaken herkennen en oppakken. Omgaan met aangiften van digitale criminaliteit is een kwestie van 'doen' en 'ervaring':

> *'Het is niet ingewikkelder dan een ander strafbaar feit. Het hoeft niet zo moeilijk te zijn wanneer je er even voor gaat zitten.'* (terugkoppelsessie Team Strand)

Respondenten op de zes onderzochte basisteams beamen: scholing en training blijven van belang, want de ontwikkelingen in modus operandi gaan snel. Daarom is het belangrijk om continu bij te blijven wat betreft trends en verschijningsvormen op het vlak van digitale criminaliteit.

5.2.3 *Beoordeling strafbaarheid*

Onbekendheid met digitale verschijningsvormen van criminaliteit onder politiemedewerkers kan bijdragen aan onzekerheid en een zekere vorm van 'digitale koudwatervrees'. Dat kan ertoe leiden dat medewerkers van de basisteams bijvoorbeeld besluiten tot het maken van een mutatie in plaats van een aangifte. Of zij benaderen digitale criminaliteit als louter een civiele zaak, terwijl er een strafrechtelijke component aan zit. Respondenten bevestigen desgevraagd dat het beoordelen van 'strafbaarheid' als moeilijker wordt ervaren als het gaat om digitale criminaliteit. Veel zaken spelen zich af op het snijvlak van civiel recht en strafrecht, bijvoorbeeld als een slachtoffer schadeloosgesteld wordt door een bank of waar een slachtoffer na misleiding geld heeft overgemaakt naar een malafide partij. Daardoor kan worden besloten een zaak als civiel te beoordelen en er geen strafrechtelijk opvolging aan te geven.

Uit de analyse van de 77 zaken komt naar voren dat de beoordeling van de strafbaarheid van digitale delicten lastig blijkt, vragen oproept en niet eenduidig is. In meerdere zaken werden delicten niet herkend als strafbaar feit of was daar onduidelijkheid over. Dan valt terug te lezen dat aan slachtoffers werd meegedeeld dat hetgeen hen overkomen was geen strafbaar feit betrof, terwijl dit feitelijk onjuist was. Zo werd een zaak afgewezen met als reden 'geen strafbaar feit', waar het identiteitsfraude betrof en er met persoonsgegevens van het slachtoffer frauduleuze bestellingen waren gedaan (ZEE 48). Een andere zaak, met een ton schade na oplichting met cryptovaluta, werd afgedaan als een civiele zaak (STRAND12), omdat er geen sprake zou zijn van een strafbaar feit.

Want, zo stelde men, *'het slachtoffer heeft het geld zelf overgemaakt'*. Een zaak met als label 'misbruik accounts voor bestellingen' werd afgewezen met de reden 'geen strafbaar feit', omdat er onduidelijkheid bestond over wie nu feitelijk de benadeelde partij was: de melder op wiens naam goederen zijn besteld of de leverancier van de goederen? (OOST36).

Ook pogingen tot digitale criminaliteit blijken allerlei vragen op te roepen wat betreft de strafbaarstelling. Voorbeelden zijn wanneer er een phishing-mail of whatsapp werd verstuurd, maar het slachtoffer daar niet op is ingegaan (o.a. OOST22). Hierbij werd gesteld: er is niets buitgemaakt dus het strafbare feit heeft niet plaatsgevonden. Daarnaast komen er nieuwe vragen naar voren: kan het liken van een beledigende video op TikTok een strafbaar feit zijn, of is alleen het plaatsen van dat filmpje strafbaar? (OOST48). En hoe om te gaan met online bedreigingen: wat zijn daar de strafbare componenten? Bijvoorbeeld waar een verdachte zich bedreigend en seksistisch uitlaat in onlinefilmpjes (ZEE8). Verder kan het sturen van een foto van een wapen of van agressieve berichten via sociale media door de ontvanger – of door degene over wie de berichtgeving gaat – als zeer bedreigend worden ervaren. Maar is het dan ook strafbaar? In meerdere zaken worstelen teams met dit soort vragen.

5.3 Keuzes maken

5.3.1 *Beoordeling van opsporingsindicaties*

Niet alle zaken die binnenkomen op een basisteam kunnen worden opgevolgd. Het maken van keuzes over het wel of niet (verder) acteren op een melding of aangifte is onvermijdelijk. De zaakreconstructies overziend, valt het op dat de gemaakte keuzes tijdens het verloop van zaken niet of heel summier worden geëxpliciteerd en onderbouwd in het registratiesysteem. Deels is dit te verklaren doordat de mogelijkheden in BOSZ om keuzes te motiveren beperkt waren (inmiddels zijn de opties in BOSZ uitgebreid). Vaak werden zaken afgerond of beëindigd vanwege het ontbreken van opsporingsindicaties of capaciteit of omdat het '*geen kansrijke zaak*' betreft. Uit de geanalyseerde zaakregistraties kan worden opgemaakt dat opsporingsindicaties regelmatig ontbreken, terwijl deze in principe wél voorhanden of in ieder geval (eenvoudig) te verkrijgen zijn. Denk bijvoorbeeld aan telefoonnummers, IP-adressen, bankgegevens en digitale data (zoals appcontact) over het delict. Ook blijkt dat als dit soort opsporingsindicaties wel aanwezig is, zij niet altijd werden opgevolgd. Bovendien gaan politiemedewerkers niet standaard op zoek naar zaken met identieke opsporingsindicaties (zie verderop ook over schaalbare criminaliteit).

Politiemedewerkers wijzen erop dat vooral tijd, middelen en capaciteit beperkende factoren zijn. Dit heeft te maken met het aanbod van andere (fysieke) zaken met een hoge(re) prioriteit die inzet vergen, maar ook met de beoordeling van opsporingsindicaties: de verwachte inzet die de opvolging zal vergen om tot opsporing en vervolging

te komen. Bij digitale zaken valt die balans nogal eens negatief uit: het ontbreekt aan zicht op een succesvolle aanhouding van een verdachte. Zo is motivering van een screener bij een online fraude (misbruik van accounts voor bestellingen):

> *'Geen indicatie met kans van slagen, gelukkig geen schade. VBE [vroegtijdig beëindigd] i.v.m. capaciteit.'* (STRAND31)

Politiemedewerkers hebben ook te maken met verschillen in digitale (sociale media) platforms, wat het vorderen van gegevens bemoeilijkt. Soms stuiten politiemensen op het zwijgrecht van verdachten. Bij digitale zaken gaat het ook relatief vaak om het uitpluizen van grote hoeveelheden data, wat een zeer arbeidsintensieve klus is.

Digitale criminaliteit die klein begint met een aangifte of melding kan al snel 'te groot' worden voor een basisteam. Een omvangrijke online fraude met meerdere aangiftes of meldingen die over eenheidsgrenzen heen gaat, groeit dan uit tot een 'DR-waardige' zaak. Al dan niet op aangeven van het OM dragen basisteams deze zaak over of pakken ze een zaak niet verder op. Het is voor de teams al lastig om met digitale criminaliteit aan de slag te gaan zodra zaken delicten districts- en eenheidsgrenzen overschrijden, maar het wordt helemaal ingewikkeld als zaken ook een internationale component hebben en opsporing over landsgrenzen nodig is. Het opsporen van verdachten die niet in Nederland verblijven of delicten die in het buitenland hun oorsprong hebben, wordt snel dermate complex dat een basisteam besluit een zaak af te sluiten.

Daarnaast blijkt de 'menselijke factor' een rol van belang te spelen in de beoordeling van zaken. Er zijn basisteams die 'net iets meer' willen doen in zaken waar een slachtoffer in het bijzonder is geraakt vanwege leeftijd of andere omstandigheden. Datzelfde geldt als er een verdachte bekend is. Met in het achterhoofd: wanneer je er als politie direct naartoe gaat, dan stoppen verdachten hopelijk gelijk en worden toekomstige delicten, en daarmee het groter groeien van een zaak, voorkomen. Tegelijk valt op dat er voortvarender te werk wordt gegaan in zaken waaraan behalve een digitale ook een fysieke component zit (hybride zaken). Bijvoorbeeld camerabeelden bij een pinautomaat kunnen dan helpen bij de opsporing van een verdachte.

Andere zaken die kansrijker lijken te zijn betreffen persoonsgerichte delicten, waarbij verdachte en slachtoffer bekenden van elkaar zijn. Daardoor komt de verdachte logischerwijs vrij gemakkelijk in beeld. Zo werd er snel doorgepakt door een basisteam in een zaak waarbij sprake was van oproepen via WhatsApp en socialemediakanalen om een persoon te belagen (MIDDEN16). Politiemedewerkers verklaren de voortvarendheid in dit soort hybride zaken vanuit het feit ze in lijn liggen met (traditionele) fysieke zaken, zoals stalking, die een persoonsgericht karakter hebben en door slachtoffers als zeer impactvol worden ervaren. Aangiften of meldingen van stalking krijgen over het algemeen ook politieprioriteit.

5.3.2 *Kaders en afspraken*

Er bestaan afspraken over het al dan niet oppakken van zaken. Zo kennen de zaken die via LMIO gerouteerd binnenkomen op een basisteam een (bepaalde) verplichting tot oppakken. Verder is ieder basisteam gebonden aan (nationale en lokale) selectiviteitskaders en prioriteringstools waarin richtlijnen zijn vastgelegd over het wel/niet oppakken van zaken, waaronder een richtlijn voor schadebedragen. Zo wordt de geringe omvang van een schadebedrag, in lijn met het selectiviteitskader, regelmatig aangevoerd als reden om een zaak af te wijzen of vroegtijdig te beëindigen. Bijvoorbeeld waar de schade 'slechts' € 860, € 1.000 of € 5.500 was (MIDDEN 5; MIDDEN 6; OOST42). Ook een zaak van een oudere dame die na een hulpvraagfraude € 2.000 schade leed, werd niet opgepakt (STRAND45).

Het gebruik van (diverse) selectiviteitskaders wordt in registraties niet altijd expliciet genoemd. De indruk is dat het toepassen daarvan (onder andere aan de hand van vermelde schadebedragen) per basisteam verschilt. In een aantal van de 77 zaken is sprake van ingrijpende gebeurtenissen voor slachtoffers of van grote schadebedragen die niettemin werden afgedaan als '*niet schokkend*'. Zo werd een schade van in totaal $92.000 (STAD17) met die reden niet opgepakt. Desgevraagd beamen politiemedewerkers dat de beoordeling van zaken idealiter overal gelijk is, maar dat het per definitie mensenwerk blijft. Ook zijn zij afhankelijk van hoe het OM een zaak beoordeelt.

De mogelijkheid van – of in ieder geval het zicht op – financiële schadeloosstelling van het slachtoffer door bijvoorbeeld een bank lijkt een andere (impliciete) afspraak om zaken niet verder op te volgen. Immers: dan is het individuele slachtoffer geholpen, al betekent het dat opsporing van de verdachte uitblijft. Een basisteam besloot bij een bankhelpdeskfraude met € 11.000 schade niet door te rechercheren op leads die er wel waren (waaronder camerabeelden, telefoonnummers en bankgegevens) nadat bekend was dat het slachtoffer schadeloosgesteld werd door de bank (MIDDEN7).

5.4 Samenwerken

5.4.1 *Samenwerken binnen de politie*

Het is in de gereconstrueerde zaken terug te zien dat samenwerking loont als afdelingen of onderdelen binnen de politie met elkaar aan digitale zaken werken. Dit wordt door medewerkers van de basisteams beaamd. Toch blijkt het vinden van de weg naar de juiste expertise en naar 'wie moet wat doen' binnen de organisatie diffuus. Dat geldt ook voor de vraag waar het 'eigenaarschap' van zaken ligt. Er wordt in de afhandeling van zaken geschakeld met specifieke expertises, zoals het Cybercrime Team, een digitale HUB, het team digitale expertise, OSINT (Open Source Intelligence) en het Team Zeden. Voorts vindt er interactie plaats met andere afdelingen binnen het eigen basis-

team, met basis- en rechercheteams binnen of buiten de eigen eenheid, met het LMIO en met de RSC.

Waar diverse teams samenwerken aan een zaak en gebruikmaken van elkaars kennis, expertise en hulplijnen komen zaken in beweging, zo blijkt uit de zaakreconstructies. Politiemedewerkers geven aan baat te hebben bij het kunnen sparren met digi-specialisten, binnen welk team ze ook werkzaam zijn. Als voorbeeld: medewerkers in een stalkingszaak met een sterke digitale component (ZEE8) werkten samen met collega's van OSINT, Zeden en Intelligence om de maker te achterhalen van YouTubefilmpjes met seksistische en bedreigende uitlatingen. De wijkagent kon op basis daarvan binnen afzienbare tijd een stopgesprek met een verdachte voeren. In een omvangrijke aan- en verkoopfraudezaak speelde het Cybercrimeteam een belangrijke rol bij het bijeenbrengen en duiden van allerlei informatie, inclusief die rondom de mogelijke verdachte (MIDDEN27). Waar samenwerking tussen basisteams en digitaal experts van de grond komt, ervaren politiemedewerkers hier meerwaarde van.

Dergelijke samenwerkingsverbanden zijn echter niet altijd vanzelfsprekend en ontstaan niet vanzelf. Het lijkt erop dat er meer potentie in interne samenwerking rondom digitale criminaliteit zit dan momenteel wordt benut. Politiemedewerkers zien de mogelijkheden niet altijd of zijn zich er niet van bewust. Er is binnen de organisatie bijvoorbeeld expertise aanwezig op cryptovaluta, maar dat betekent niet dat medewerkers van een basisteam die expertise meteen weten te vinden en benutten. Zo was er een zaak (STAD40) over diefstal van € 95.000 aan cryptomunten via een hack, waarbij gegevens van de wallets (digitale portefeuilles) en camerabeelden van verdachten voorhanden waren. Deze zaak werd vroegtijdig beëindigd, zonder dat er een cryptospecialist betrokken werd om nader onderzoek te doen naar de wallets.

Als verklaring geven politiemedewerkers aan dat er weliswaar allerlei digitale expertise beschikbaar is binnen het korps, maar dat deze zich op 'eilandjes' concentreert die niet altijd even goed worden gevonden. Het blijkt niet eenvoudig de weg te vinden naar alle nieuwe voorhanden zijnde expertises, middelen en teams die door de volop gaande zijnde 'digitale transformatie' binnen de politie zijn ontstaan. Er bestaan vele hulplijnen, factsheets, documenten, checklists, e-learnings en netwerken. Daarom is het voor politiemedewerkers niet meteen helder waar te beginnen met zoeken; lijntjes verlopen daardoor snel via persoonlijke netwerken.

Een ander punt is het 'eigenaarschap' van een zaak. Weliswaar ligt die in eerste instantie bij het basisteam waar een aangifte of melding binnenkomt, maar bij meerdere aangiften en meldingen – en dus een grotere complexiteit van een zaak – komen ook andere basisteams en politieonderdelen in beeld. Waar het een omvangrijker zaak betreft met meerdere aangiften, oordelen politiemedewerkers vaak dat deze niet bij een basisteam thuishoort. In een aantal registraties is inderdaad te zien dat een zaak wordt overgedragen van het basisteam naar de DR (bijvoorbeeld: OOST14).

Toch valt op dat relatief kleine zaken bij een DR belanden en omvangrijke (met een uitschieter van negentig aangiftes) bij een basisteam blijven (MIDDEN27). Daarnaast is het mogelijk dat er meerdere basisteams aan een lopende zaak werken, waardoor deze op een gegeven moment door een ander team dan de oorspronkelijke eigenaar wordt overgenomen (OOSTtrots). Dit soort onduidelijkheid over eigenaarschap en het 'schuiven' van zaken tussen teams kan ertoe leiden dat aangiften door niemand worden opgepakt (en zaken dus blijven liggen), omdat de onderlinge taakverdeling diffuus is:

> *'We hebben veel met bankhelpdeskfraude te maken. Als je daarin duikt, dan zie je dat er veel slachtoffers zijn. Dan is-ie al snel te complex voor het basisteam en zelf soms voor de DR. En dan hebben we geen idee wie zo'n zaak wel oppakt.'* (terugkoppelsessie Team Midden)

Een zaak kan blijven liggen waar deze te complex is voor een basisteam of waar specifieke expertise nodig is en collega's niet de mogelijkheid hebben om het werk op te pakken. Ondertussen wordt er 'bottom-up' naar oplossingen gezocht voor obstakels die het tussentijds overdragen van zaken in de weg kunnen staan. Zo is er een basisteam (Team-Zee) waar men 'het schot' tussen de VVC (de basisteamrecherche) en de DR heeft weggenomen door gezamenlijk de casescreening op te pakken.

5.4.2 *Samenwerken met externe partijen*

Het OM is een partner die vrijwel in alle zaken betrokken is in verband met de leiding over het opsporingsonderzoek. Politiemedewerkers geven aan dat de sturing vanuit het OM als 'stevig' of als 'beperkend' kan worden ervaren, bijvoorbeeld met betrekking tot het aantal 'te draaien' zaken of het aantal aangiften dat gevoegd mag worden aan een zaak. In de meeste van de gereconstrueerde zaken is er nauwelijks betrokkenheid van andere partners buiten het OM. Als er al externe partijen betrokken zijn, dan gebeurt dat eerder bij persoonsgerichte delicten dan bij fraude- of afpersingszaken. Denk daarbij aan Veilig Thuis, Halt, GGZ en gemeentelijke instanties. Zij zijn er om slachtoffers te helpen, ondersteunen of weerbaarder te maken. Politiemedewerkers verwijzen na aangifte ook standaard door naar Slachtofferhulp.

Bij online fraude of afpersing komen met regelmaat private partijen in de gereconstrueerde zaken als belangrijke spelers naar boven. Banken waarschuwen bijvoorbeeld hun klanten op basis van verdachte transacties en zetten mensen aan tot het doen van aangifte. Voorts komen banken in beeld als partij die slachtoffers schadeloosstelt. Het maken van heldere afspraken met partners zoals banken, winkelketens en andere instanties is iets waar geïnterviewde politiemedewerkers behoefte aan hebben.

Tot slot doen banken en bedrijven zelf onderzoek in fraudezaken. Zo werd er door een supermarkt eerst uitvoerig onderzocht waar het via een app gestolen geld was gebleven, alvorens het bedrijf voor aangifte naar de politie stapte (ZEE41). Daarnaast huur-

de een werkgever een specialistisch bedrijf in om digitale sporen van phishing te zoeken en veilig te stellen. Toen dat niet afdoende bleek, ging de werkgever over tot aangifte (STRAND10). Deze vooraf, door of namens slachtoffers, gedane onderzoeken maken het politiewerk aan de ene kant makkelijker, omdat er al informatie is verzameld en uitgezocht. In het beste geval hoeft enkel nog de verdachte te worden gehoord. Ook kunnen verdachten op een 'zwarte lijst' komen bij een bank of bedrijf, wat de kans op toekomstige delicten verkleint. Anderzijds betekent dit soort 'private opsporing' dat informatie niet op voorhand en zonder meer met de politie wordt gedeeld, omdat slachtoffers het delict zelf proberen op te lossen. Daarmee blijft het strafbare feit buiten het blikveld van politie en justitie.

5.5 Schaalbare criminaliteit

5.5.1 *LMIO-zaken*

Digitale criminaliteit, met name de online fraude, is 'schaalbaar'. Daarmee wordt bedoeld dat wat op het eerste gezicht 'kleine' en 'losse' zaken lijken, bij nader inzien samenhangen en daardoor naar een omvangrijke zaak leiden. Dit vraagt om een andere benadering dan de traditioneel 'blauwe' aanpak die zich richt op fysieke en gebiedsgebonden criminaliteit. Zoals een medewerker van de projectgroep Centurion stelt:

> *'Vanaf een laptop kunnen veel slachtoffers tegelijk gedupeerd worden. […] Dit vraagstuk leidt ertoe dat de focus in de aanpak verschuift van slachtoffergericht naar dader gerouteerd.'*[19]

Via de routering door LMIO verschijnen verdachten van aan- en verkoopfraude op de radar van een basisteam.[20] Dit zijn vaak zaken met meerdere aangiftes en, bij elkaar opgeteld, aanzienlijke schadebedragen. Van de basisteams wordt verwacht dat zij acteren richting de verdachten die binnen hun werkgebied verblijven en vervolgens hun zaak afhandelen.

Onder de 77 geanalyseerde zaken bevonden zich 11 LMIO-zaken. Het ging om aan- en verkoopfraudes via Markplaats en webwinkels. Er waren grote zaken bij met een internationaal gesignaleerd staande verdachte (STADlmio), maar ook kleinere met vier aangiftes (ZEElmio). De doorlooptijd van de LMIO-zaken kan lang zijn. Soms zit er al een paar maanden tussen het moment dat een zaak bij LMIO wordt opgepakt tot deze bij een basisteam terechtkomt. Tussen aangifte(n) via internet en het verhoor van een verdachte varieert de doorlooptijd tussen vier en tien maanden. Er zijn altijd meerdere

19 In Van der Wiele (2024).

20 Alleen voor aan- en verkoopfraude is er door LMIO-stapeling van aangiften: pas bij drie aangiftes tegen een rekeninghouder worden deze zaken zichtbaar in BOSZ van een basisteam, tenzij de rekeninghouder een minderjarige betreft (LMIO, 2023).

aangiftes in het spel, variërend van vier tot 27 (met een uitschieter van negentig). Schadebedragen zijn aanzienlijk: tussen € 750 en € 30.000. Slachtoffers van deze aan-en verkoopfraudes zijn meestal de 'kopers' die hun geld zagen verdwijnen.

Politiemedewerkers vertellen dat de LMIO-werkwijze hen helpt, maar dat het nog niet vlekkeloos verloopt. Een respondent spreekt van 'kinderziektes' en realiseert zich dat deze vrij nieuwe werkwijze nog volop in ontwikkeling is. In negatieve zin worden LMIO-zaken gezien als een 'moetje': ze moeten opgevolgd worden. Dat kan het basisteam serieus capaciteit kosten. Respondenten zijn zowel positief als kritisch over de bundeling van informatie om tot een grotere zaak te komen. Positief is dat er op voorhand al een hoop werk is verzet en de werkwijze is 'afgetikt' met het OM. LMIO-zaken leiden vrij snel tot een 'ronde zaak', ook al volgt er niet altijd een aanhouding. Een kritische kanttekening is dat de informatie die vanuit LMIO wordt aangeleverd soms minder 'hapklaar' is dan verwacht. Er komen bijvoorbeeld fouten voor die vervolgens door het basisteam moeten worden rechtgezet of aangevuld.

5.5.2 *Koppeling van zaken is complex*

Respondenten beseffen dat digitale criminaliteit, ook buiten de aan-en verkoopfraudes waar het LMIO zich op richt, bijna nooit op zichzelf staat. Elke aangifte of melding kan een puzzelstukje zijn in een grotere zaak. Medewerkers van de basisteams zijn ervan doordrongen dat er bij de meeste zaken per definitie sprake is van schaalbaarheid en dus van een groter patroon en meerdere (toekomstige) slachtoffers. Dit besef betekent echter niet meteen dat basisteams eraan toekomen om patronen te doorzien en zaken te stapelen. In een bankphishing zaak (STRAND34) waren relatief eenvoudig indicaties te vinden om vergelijkbare zaken te koppelen, maar hier werd niet op ingezet. Verder komt het voor dat een officier van justitie of een politieteam bepaalt dat er een maximum van aangiftes wordt gekoppeld aan een zaak om deze behapbaar te houden (en toch te komen tot een mogelijke veroordeling). Tegelijk zouden de respondenten vanuit slachtofferperspectief graag meerdere aangiftes met elkaar willen verbinden.

Respondenten vinden het frustrerend te weten dat er meer zaken te koppelen zijn maar dat dit niet gebeurt. Zij wijzen erop dat informatie te versnipperd over basisteams voorhanden is, waardoor zaken niet in samenhang worden opgepakt. Het koppelen gebeurt ad hoc in plaats van structureel. Bijvoorbeeld waar een politiemedewerker informatie door het registratiesysteem haalt en daardoor – haast bij toeval – op verbanden met andere zaken stuit. Of waar na aangiftes bij een cybercrimeteam en een lopende zaak op een basisteam contact werd gezocht met het LMIO en er zodoende nog een aangifte toegevoegd kon worden (NOORDlmio). Tegen deze achtergrond bestaat er onder politiemedewerkers behoefte om betere ondersteuning te krijgen bij de koppeling en stapeling van zaken. Sinds kort worden binnen diverse eenheden (screening) hubs ingericht die aan het bundelen en opwerken van zaken moeten bijdragen.

5.6 Afloop en resultaten

Ruim 60% van de geselecteerde zaken (N=77) werd vroegtijdig beëindigd of afgewezen. Die afwijzingen betroffen met name online fraudezaken. De afwegingen die hieraan ten grondslag liggen kwamen eerder al aan de orde: zij blijken voornamelijk ingegeven door beschikbare capaciteit in combinatie met een beoordeling van opsporingsindicaties. Eenderde van alle 77 zaken werd afgerond – wat echter niet zonder meer betekent dat deze een strafrechtelijk vervolg kregen[21] – en de overige zaken waren na afloop van onze onderzoeksperiode nog in behandeling.[22] In 34 van de 77 zaken was er een verdachte in beeld en achttien van deze verdachten zijn verhoord. In negen zaken vond het verhoor plaats na een aanhouding (ZEE15; ZEE23; ZEElmio/trots; STADtrots; OOSTleerpunt; MIDDEN16; MIDDENtrots/lmio; NOORDlmio; NOORDleerpunt), waarvan twee een heterdaad aanhouding (STADtrots; NOORDleerpunt). In de negen andere zaken werden verdachten wel aan het bureau ontboden voor verhoor maar niet aangehouden (ZEElmio; ZEEmoeizaam; STAD20; STAD24; STADlmio; MIDDENlmio; MIDDENlmio2; NOORD21; STRANDleerpunt).

Hoewel een groot aantal zaken in dit onderzoek niet heeft geleid tot verdachten en/of aanhoudingen, zijn er ook successen te melden. Respondenten op de basisteams zijn desgevraagd 'trots' op de volgende uitkomsten:

- De aangifte van een ouder slachtoffer van bankhelpdeskfraude leidde naar acht verdachten doordat acht zaken samengevoegd konden worden. Er zijn diverse aanhoudingen verricht en Veilig Thuis (VT)-meldingen gedaan in verband met minderjarigen. Deze zaak ligt bij het OM (STRANDtrots).
- Twee geldezels kwamen in beeld bij de politie in verband met online aan- en verkoopfraude. De achterliggende verdachte kon veroordeeld worden. Dit gebeurde mede op basis van digitaal onderzoek op een telefoon, wat zicht op meerdere slachtoffers opleverde (ZEEtrots).
- In een zaak bankhelpdeskfraude konden 14 zaken gekoppeld worden aan drie verdachten. De zaak startte op het basisteam en werd overgenomen door de DR. Via buurtonderzoek en camerabeelden kwam de politie verdachten op het spoor. (NOORDtrots).
- Tijdens een poging bankhelpdeskfraude schakelde het slachtoffer met de politie. Dit leidde tot een 'actie-in-burger' en een heterdaadaanhouding van de verdachte (STADtrots).
- Nadat een slachtoffer thuis was beroofd via bankhelpdeskfraude kwam de politie ter plaatse en verspreidde beelden van de verdachte. Collega's in het land herkenden deze verdachte en meerdere zaken konden worden gekoppeld. De zaak werd te

21 Het was niet uit de politieregistraties af te leiden hoeveel van de zaken een strafrechtelijk vervolg kregen. Evenmin is bekend of inzending al dan niet tot een veroordeling leidde. Dit komt doordat OM-data niet betrokken is in dit onderzoek.

22 BOSZ-status van de 77 zaken: 25 afgehandeld/afgerond, 23 vroegtijdig beëindigd, 14 afgewezen en 15 nog lopend.

groot voor het basisteam en werd overgedragen aan de DR van een andere eenheid (OOSTtrots).
- In een aan- en verkoopfraudezaak met negentig aangiftes die via LMIO gerouteerd werden kon een verdachte aangehouden. De zaak ligt bij het OM (MIDDENtrots).

Via een 'afdoeningenwaaier' brengt het LMIO alternatieve afdoeningen (interventies buiten het strafrecht om) bij fraude met online handel speciaal onder de aandacht bij basisteams, en geeft het opties als een waarschuwingsbrief, een stopgesprek en directe aansprakelijkheid (LMIO, z.d.).[23] Bij fraudezaken kan ook een deurwaarder worden gestuurd. Uit de quickscan in hoofdstuk 5 kon niet goed worden opgemaakt in hoeverre de politie alternatieve afdoeningen bij digitale criminaliteit inzet. De geanalyseerde 77 zaken en gesprekken met respondenten laten zien dat deze interventies af en toe worden ingezet. Met uitzondering van één team geven medewerkers van de onderzochte basisteams aan dat alternatieve afdoening inmiddels op het netvlies staat en ook in de praktijk wordt toegepast. In een online bedreiging/stalkingzaak (ZEE23) werd voor alle betrokken jongeren een VT-melding gemaakt, pleitte de gemeente voor bemiddeling in plaats van aangifte en werd een gemeentelijk hulpproject ingezet. Een eenmalige online aan- en verkoopfraude laat zien dat die ook afgedaan kon worden met een stopbrief en een stopgesprek (ZEE 46). De politie experimenteert met dit soort stopgesprekken, zodat verdachten vroegtijdig hun criminele activiteiten staken en aangiften zich niet opstapelen.

Het lijkt erop dat de politie voornamelijk bij digitale persoonsgerichte zaken tot alternatieve interventies overgaat. Bij (online) stalking zijn stopgesprekken sowieso onderdeel van de reguliere aanpak. Van de zeventien persoonsgerichte delicten was er in acht gevallen sprake van een bepaalde vorm van stalking. Bij vier van deze acht zaken is de politie tot een stopgesprek overgegaan. Toch probeert de politie volgens onze respondenten juist ook bij online fraudezaken alternatieve interventies toe te passen. Eén van de doelen van de triagetafel op in het Team Midden is dat er in alle digitale zaken in ieder geval een alternatieve afdoening plaatsvindt en ook op andere teams organiseren medewerkers speciaal daarvoor aangewezen actieweken waarin stopgesprekken worden gehouden. Respondenten vinden alternatieve afdoeningen in het bijzonder relevant bij minderjarige verdachten en bij geldezels. Inmiddels zijn er in het registratiesysteem BOSZ meerdere opties opgenomen, waaronder alternatieve interventies na vroegtijdige beëindiging, zoals doorverwijzing naar derden, een waarschuwing of een stopgesprek.

23 Van Leuken, Van der Rest & Van 't Hoff-de Goede (2024) deden onderzoek naar de praktische uitvoering en juridische grondslag van civielrechtelijke afdoening van online fraude door onder meer de politie. Daarbij keken zij ook naar de ervaringen van slachtoffers met deze manier van afdoen. Slachtoffers zijn gemotiveerd om een civielrechtelijke procedure op te starten om financiële schade te verhalen, daders af te schrikken/te straffen en voor gerechtigheid te zorgen. Hun ervaringen liepen zeer uiteen. Vooral slachtoffers die hun geld (nog) niet terugkregen ervaarden frustratie en/of teleurstelling. Soms reageerden slachtoffers verbaasd als ze hun geld wel terugkregen, omdat zij dit van tevoren niet hadden verwacht.

5.7 Omgaan met slachtoffers

De grote impact die digitale criminaliteit kan hebben op slachtoffers wordt door basisteams onderkend: medewerkers spreken en zien slachtoffers, horen hun verhaal uit de eerste hand en treffen mensen die verhuizen of zelfs suïcide willen plegen als gevolg van hetgeen hen is overkomen. Uit onderzoek is ook steeds meer bekend over de impact van 'nieuwe' digitale vormen van criminaliteit op slachtoffers (zie ook hoofdstuk 2 en 8). Het valt op dat digitale criminaliteit waarbij sprake is van kwetsbare slachtoffers door de politie met hogere prioriteit en voortvarend wordt opgepakt. Dit blijkt onder meer uit het direct actie ondernemen bij oudere slachtoffers (onder andere STRANDtrots, OOSTtrots). Onder politiemedewerkers is de verontwaardiging daarover groot. Een respondent vertelt dat de politie haar best doet zich in te spannen voor dit soort kwetsbare slachtoffers:

> *'"Pogingen tot" oplichting pakken we niet op; daar hebben we de capaciteit niet voor. Maar wel als het slachtoffer iemand uit 1945 is […]. Dan laten we de wijkagent langskomen om toch even met het slachtoffer in gesprek te gaan.*' (terugkoppelsessie Team Noord)

Toch overheerst bij hen het gevoel dat de politie bij digitale criminaliteit tekortschiet richting slachtoffers. Een politiemedewerker zegt: *'Je wil voor het slachtoffer met voldoening een zaak af kunnen ronden en dat gebeurt nu niet altijd.*' (terugkoppelsessie Team Midden). De cijfers die het aantal af te handelen zaken dicteren nemen op de basisteams een dermate belangrijke plek in dat het belang van slachtoffers op de achtergrond lijkt te geraken. Bovendien staat het belang om slachtoffers van digitale criminaliteit direct te zien en te spreken op gespannen voet met de wijze waarop het contact met politie meestal verloopt, namelijk via internet of een later te plannen afspraak voor aangifte. Ook slachtoffers met aanzienlijke schade (€ 10.000 of meer) worden geacht via internet aangifte te doen. Het al besproken initiatief Digitale Meldkamer (of DigiPrio1), waarbij de politie ter plaatse gaat bij digitale criminaliteit, ervaren respondenten als een welkome aanvulling om hierin verbetering te brengen.

Eerder kwam al aan de orde dat na het doen van aangifte een ruime meerderheid van de zaken vroegtijdig werd beëindigd of ogenschijnlijk snel en zonder opsporingshandelingen werd afgehandeld. Het is mogelijk dat er ondertussen een betekenisvolle afdoening heeft plaatsgevonden, bijvoorbeeld als een slachtoffer schadeloos is gesteld. Ook is het mogelijk dat een slachtoffer besluit van aangifte af te zien (MIDDEN12).[24] Daartegenover staat dat slachtoffers soms naar huis worden gestuurd zonder dat ze aangifte kunnen doen van voor hen ingrijpende gebeurtenissen of strafbare feiten. Zo

24 Het ging hier om een zogeheten 'klachtdelict', waarbij de verdachte pas vervolgd kan worden als het slachtoffer van het delict zelf heeft aangegeven strafrechtelijke vervolging te wensen. Of de vervolging daadwerkelijk zal plaatsvinden, bepaalt het Openbaar Ministerie.

kreeg een slachtoffer van een als heftig ervaren online bedreiging te horen dat aangifte nu niet mogelijk is, *'maar als de pleger voor je deur staat, kan je 112 bellen'* (STAD15). Een ander slachtoffer werd na een online bedreiging vanuit het buitenland met het spreekwoordelijke kluitje in het riet gestuurd met de mededeling dat hij/zij in het betreffende land aangifte moest doen (ZEE8).

In enkele van de geselecteerde zaken is sprake van 'victim blaming': de verantwoordelijkheid voor het gebeurde wordt (deels) bij het slachtoffer gelegd. Zo valt er in een sextortionzaak te lezen dat het ook *'een beetje eigen verantwoordelijkheid'* was (NOORD20). Daarna nam de politie geen aangifte op. Over een slachtoffer van cryptofraude met een ton schade staat dat ze het geld zelf had overgemaakt, waarna de zaak werd afgesloten met de opmerking: '*Geen strafbaar feit, civiel, aangever maakt zelf geld over*' (STRAND12). Desgevraagd herkennen de meeste respondenten deze 'ondertoon' die bij zowel politie, OM als de maatschappij richting slachtoffers aanwezig kan zijn, ook al mag deze professioneel nooit meewegen in besluiten. Respondenten zijn zich ervan bewust dat digitale criminaliteit iedereen kan overkomen. Soms heeft een slachtoffer ook een groot crimineel en professioneel opererend netwerk tegenover zich.

Het is bekend dat politiecontact over het verloop van een zaak door slachtoffers wordt gewaardeerd: *'Mensen geven aan hoe fijn het is om contact te hebben, ook wanneer we niets kunnen doen'* (Terugkoppelsessie team Stad). Dit is mede de reden dat Team Noord het triageproces heeft aangepast. Het team streeft ernaar ieder slachtoffer te bellen en te peilen over het vervolg van de zaak om hen goed te informeren en hun tevredenheid over de politie te vergroten. Politiemedewerkers geven toe dat er lang niet altijd aan de verwachting van slachtoffers kan worden voldaan. Regelmatig krijgen slachtoffers te horen dat de politie helaas niets (meer) kan doen en dat de zaak wordt gesloten. Die boodschap is uiteraard onbevredigend en frustrerend voor slachtoffers.

Tot slot zijn er onder de gereconstrueerde zaken meerdere voorbeelden waarbij de politie tegen de grenzen van haar eigen mogelijkheden aanliep. Een (zeer angstig) slachtoffer van smaad en laster leverde uitgebreide informatie over de internationale zaak die haar trof. Voor de politie was de zaak niet kansrijk, omdat de dreiging afkomstig was uit het buitenland (STRAND48). De zaak zou volgens het eindoordeel van de officier van justitie onevenredig veel capaciteit kosten, zonder dat dit zou leiden tot een verdachte. Ook komt het voor dat de verantwoordelijkheid om stappen te ondernemen primair bij slachtoffers komt te liggen. Iemand kreeg na het hacken van een account de vraag voorgelegd om zelf informatie te verzamelen (NOORD 19), een ander slachtoffer kreeg het verzoek om met de eigen werkgever onderzoek te doen naar sporen (STRAND10).

5.8 Omgaan met verdachten

Eerder kwam al aan de orde dan in meer dan tweederde (69%) van de 77 zaken geen verdachte in beeld is bij de politie. Dit geldt vooral voor online fraude. Bij persoonsgerichte digitale delicten, zoals stalking, is verhoudingsgewijs wel vaak een verdachte in beeld. Waar een verdachte in beeld is, blijken zij geregeld 'bekenden' van het basisteam te zijn vanwege betrokkenheid bij andere vormen van criminaliteit of overlast. Een door LMIO aangedragen verdachte van online aan- en verkoopfraude stond bij de politie als veelpleger geregistreerd (STADlmio). Evenzo heeft een andere verdachte, naast online aan- en verkoopfraude, ook politieregistraties op zijn naam staan over overlast, huiselijke twisten en wijkproblematiek (OOSTlmio). Een verdachte van marktplaatsfraude was al bij HALT bekend en staat bij de politie te boek als 'probleemjongere' (MIDDENlmio2).

Net als verdachten van veelvoorkomende fysieke criminaliteit zijn verdachten van digitale criminaliteit niet eenvoudig te traceren. Zo bleek het in een zaak onmogelijk om binnen een familie van vijf personen, verblijvend op hetzelfde adres, te achterhalen wie van hen de verdachte was (OOSTlmio). Dat een verdachte van digitale criminaliteit ook bij meerdere fysieke delicten is betrokken, kan de aanpak van digitale delicten vergemakkelijken. Andersom kan de verdenking van een digitaal feit voor een basisteam het spreekwoordelijke 'haakje' zijn om in contact te komen met criminele en overlast gevende personen in de wijk. In de regel onderneemt de politie richting minderjarige verdachten actie door middel van een verhoor en/of een (stop)gesprek.

In de geanalyseerde zaken is terug te zien dat geldezels zich met regelmaat bij de politie melden op het moment dat hun bankrekening is geblokkeerd. Dit kan plaatsvinden binnen een context van *'vriendendiensten'*, waarbij personen elkaar *'een bankrekening lenen'* (ZEEmoeizaam), al komen dwang en intimidatie ook voor. Zo was er een slachtoffer van sextortion die, via dit delict, gedwongen werd zijn bankrekening ter beschikking te stellen aan een afperser (NOORD32). Dat geldezels formeel worden aangemerkt als verdachte wil niet zeggen dat zij altijd de dader van een strafbaar feit zijn. In twee zaken verwees de politie naar een geldezel als *'onterecht aangemerkte verdachte'* (MIDDENtrots, STAD24). Het is in dergelijke zaken duidelijk dat personen door criminelen worden gebruikt.

Hoewel geldezels formeel als verdachte worden aangemerkt, benadert de politie hen daarom in specifieke gevallen als 'dader-slachtoffer'. De achterliggende (intellectuele) dader blijft in dergelijke gevallen buiten beeld. Een uitzondering die de regel bevestigt betreft de zaak van een bekende veelpleger die kwetsbare jongeren in zijn omgeving ronselde als geldezel. Hij liep wel tegen de lamp (NOORDlmio). Politiemedewerkers vertellen echter dat geldezels uit angst en schaamte niet gemakkelijk verklaren over hun betrokkenheid. De drempel om naar de politie te stappen kan hoog zijn. Geldezels beroepen zich vaak op hun zwijgrecht. Daardoor is het voor de politie moeilijk om

grotere criminele netwerken op het spoor te komen. Medewerkers op de basisteams willen graag de 'echte criminelen' aanpakken, maar hebben daartoe onvoldoende mogelijkheden door een gebrek aan capaciteit, maar ook door onvoldoende coördinatie en sturing.

5.9 Tot besluit

De 77 zaakanalyses vormen een soort 'foto' van hoe politiemedewerkers van lokale basisteams aangiften en meldingen van digitale criminaliteit verwerken. In lijn met hoofdstuk 4 is de algemene indruk dat er op dit punt geen eenduidige werkwijze bestaat. Basisteams zijn zoekende naar wat de beste aanpak en afhandeling van delicten is. Geïnterviewde politiemedewerkers zien een scala aan digitale en hybride delicten voorbijkomen en ervaren daarbij geregeld een gebrek aan capaciteit, kennis en expertise. Selectiviteitskaders worden verschillend gebruikt. Samenwerking met digi-specialisten helpt, maar het blijkt binnen de politieorganisatie niet gemakkelijk om de juiste weg naar hen toe te vinden. Behalve met het OM vindt samenwerking met partijen buiten de politie in de onderzochte zaken nauwelijks plaats. Wel verwijzen politiemedewerkers door naar hulpverlenende instanties. De 'schaalbaarheid' van digitale criminaliteit maakt dat zaken snel het niveau van een basisteam overstijgen. Het clusteren van online aan- en verkoopfraudezaken door LMIO is van toegevoegde waarde voor de basisteams om tot een 'ronde zaak' te komen. Politiemedewerkers onderkennen de hoge impact die digitale criminaliteit op slachtoffers kan hebben. De afhandeling van meldingen en aangiften kan volgens hen op dit punt beter. Voor verdachten van online criminaliteit geldt dat zij ook 'bekende' van het team kunnen zijn als plegers van fysieke delicten.

6. Ervaringen van slachtoffers van digitale criminaliteit

6.1 Inleiding

Het eerste deel van dit hoofdstuk bevat de resultaten van een kwantitatieve studie naar de impact die digitale criminaliteit heeft gehad op slachtoffers, de behoeften die zij hebben bij aangifte en hun tevredenheid met de politie na aangifte, waarbij telkens een vergelijking wordt gemaakt tussen aangevers van digitale criminaliteit en aangevers van traditionele vormen van criminaliteit (6.2).[25] Hierbij is gebruikgemaakt van de Politiemonitor,[26] een grootschalig enquêteonderzoek onder aangevers van criminaliteit dat door de politie in de periode 2022-2023 werd uitgevoerd. Dat leverde in totaal 25.760 respondenten op.

Hoewel de aangevers van digitale criminaliteit bestaan uit een gevarieerde groep van slachtoffers van bijvoorbeeld hacken, helpdeskfraude, marktplaatsfraude en fraude via apps, is het in de Politiemonitor niet mogelijk uitsplitsingen te maken naar deze verschillende vormen van digitale criminaliteit. Daarmee kan er dus niets worden gezegd over mogelijke variatie binnen de groep aangevers van digitale criminaliteit. Overigens is de variatie binnen de groep aangevers van traditionele vormen van criminaliteit waarschijnlijk nog groter, maar deze studie beperkt zich tot het onderscheid tussen digitale criminaliteit en traditionele criminaliteit.

Binnen de kwantitatieve studie is nagegaan in hoeverre de respondenten representatief waren voor alle aangevers van criminaliteit. Daartoe is een logistische regressieanalyse uitgevoerd om respondenten met niet-respondenten te vergelijken op geslacht, nationaliteit, leeftijd en het type criminaliteit waarvan ze aangifte hadden gedaan. De Politiemonitor bleek niet volledig representatief voor de aangevers van criminaliteit in Nederland. Om de resultaten in dit hoofdstuk zo goed mogelijk generaliseerbaar te maken naar de gehele populatie slachtoffers die aangifte hebben gedaan in Nederland, zijn op basis van de representativiteitsanalyse weegfactoren berekend en toegepast bij de verdere analyse van de enquêtegegevens.

25 Zie bijlage 6 voor de methode en aanpak van de kwantitatieve studie naar slachtoffers van digitale criminaliteit.

26 De items uit de Politiemonitor over behoeften, impact en deels ervaring van slachtoffers van digitale criminaliteit zijn overgenomen uit het promotieonderzoek 'Slachtofferimpact Cybercrime' van Jildau Borwell.

Deel twee van dit hoofdstuk bevat een kwalitatieve analyse van interviews met slachtoffers van digitale criminaliteit (6.3).[27] Het was mogelijk om in totaal de verhalen van zestien respondenten telefonisch of per Teams (beeldbellen) op te tekenen. Hun verhalen dienen als illustratie bij en nadere interpretatie van de kwantitatieve analyse, met bijzondere aandacht voor de thematieken die in deze analyse aan de orde komen: de impact van digitale delicten op slachtoffers, hun behoeften bij het doen van aangiften en hun tevredenheid over de politie nadat er aangifte is gedaan. Het hoofdstuk sluit aan de hand van de bevindingen af met een reflectie op bestaande wetenschappelijke literatuur (6.4).

6.2 Kwantitatief onderzoek

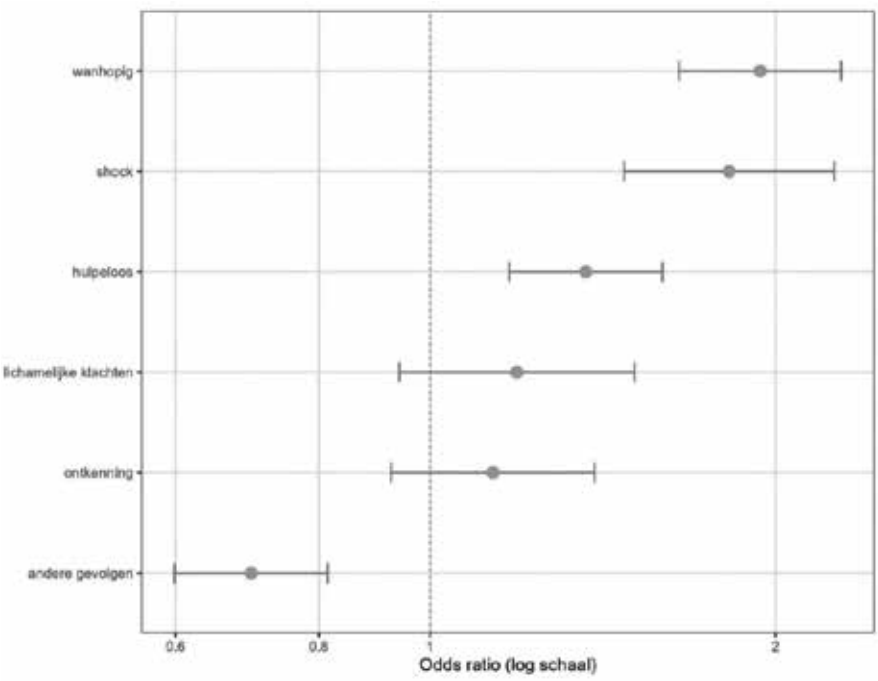
In de onderstaande paragrafen worden de volgende drie onderzoeksvragen beantwoord: (1) in welke mate verschilt de impact van criminaliteit tussen slachtoffers van digitale en traditionele criminaliteit?, (2) in welke mate verschillen de behoeftes van personen die aangifte hebben gedaan van digitale criminaliteit met die van personen die aangifte hebben gedaan van traditionele criminaliteit? en (3) in welke mate verschilt de tevredenheid met de politie tussen personen die aangifte hebben gedaan van digitale en traditionele criminaliteit?

6.2.1 *Impact van (digitale) criminaliteit*

Figuur 11 geeft de odds ratio's (OR's)[28] weer voor digitale criminaliteit zoals deze geschat worden voor de impact die slachtoffers kunnen ervaren direct nadat ze slachtoffer zijn geworden. Uitkomsten zijn gerangschikt van groot naar klein. Wat opvalt is dat slachtoffers van digitale criminaliteit zich vaker wanhopig voelden (OR=1,9), ook vaker in psychische shock waren (OR=1,8), en zich vaker hulpeloos voelden (OR=1,4) dan slachtoffers van traditionele criminaliteit, terwijl ze juist minder vaak andere directe gevolgen rapporteerden (OR=0,70). Er was geen statistisch significant verschil in de mate waarin slachtoffers van digitale en traditionele criminaliteit lichamelijke klachten als hartkloppingen, duizeligheid, trillen of hoofdpijn ervoeren. Ook de mate waarin ze ontkenden of konden geloven wat er was gebeurd verschilde niet tussen beide groepen.

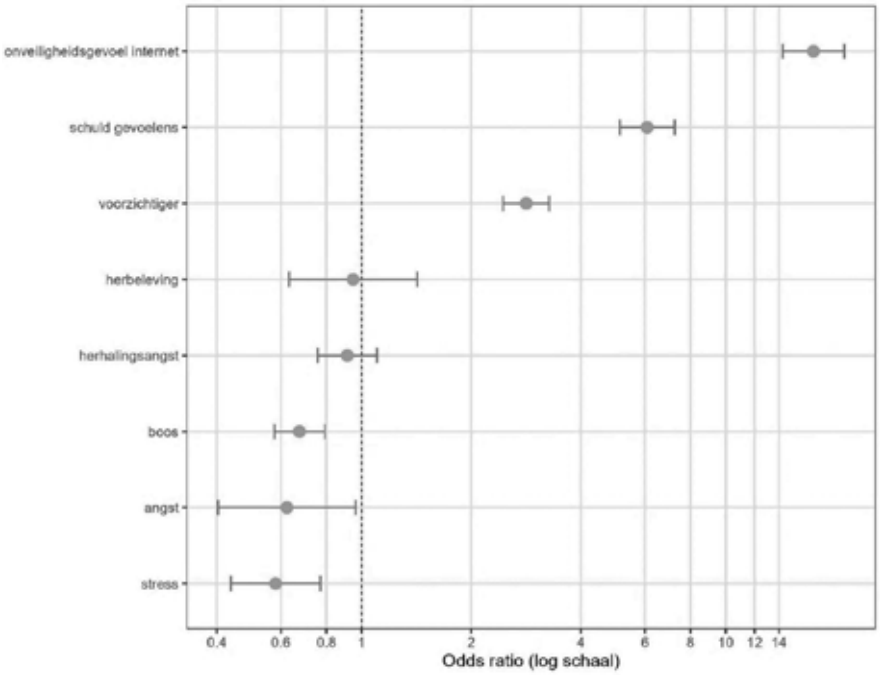
27 Zie bijlage 7 voor de methode en aanpak van de kwalitatieve studie naar slachtoffers van digitale criminaliteit.

28 De odds ratio drukt de verhouding uit tussen twee *odds*. Dit is een Engelse term voor een associatiemaat voor variabelen met twee uitkomstcategorieën. De odds worden berekend als de ratio van het aantal keren dat een gebeurtenis plaatsvond en het aantal keren dat een gebeurtenis niet plaatsvond.



Figuur 11 OR's digitale criminaliteit voor de verschillende vormen van directe impact

Figuur 12 geeft de resultaten weer voor de langdurige impact. Wat direct opvalt zijn de veel grotere odds ratio's dan in de vorige figuren. Dit wijst op grote verschillen in langdurige impact tussen slachtoffers van digitale criminaliteit en slachtoffers van traditionele criminaliteit. Slachtoffers van digitale criminaliteit ervaren veel vaker onveiligheidsgevoelens op het internet (OR=17,4), hetgeen vanwege de aard van het delict niet verwonderlijk is. Ze geven zichzelf ook veel vaker de schuld van wat gebeurd is dan slachtoffers van traditionele criminaliteit (OR=6,1) en zijn ook vaker voorzichtiger geworden (OR=2,8). Slachtoffers van traditionele criminaliteit rapporteren juist vaker boosheid (OR=0,7), angst- of paniekklachten (OR=0,6) en stress of spanning (OR=0,6), terwijl beide groepen niet statistisch significant verschilden in de mate waarin ze herbeleving of herhalingsangst rapporteerden.

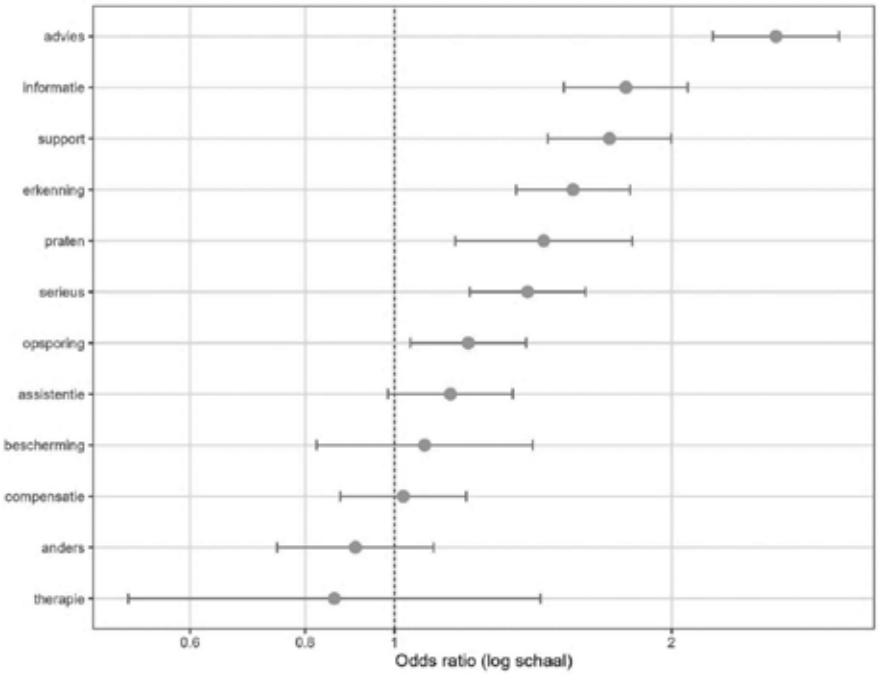


Figuur 12 OR's digitale criminaliteit voor de verschillende vormen van langdurige impact

6.2.2 *Behoeftes bij aangifte*

Figuur 13 geeft de odds ratio's weer voor digitale criminaliteit zoals deze geschat werden in de afzonderlijke modellen voor de verschillende behoeftes die slachtoffers kunnen ervaren. De figuur laat duidelijk zien dat slachtoffers van digitale criminaliteit met name veel vaker aangaven behoefte te hebben aan advies om herhaling van hetzelfde strafbare feit te voorkomen (OR=2,6) dan slachtoffers van traditionele criminaliteit. Daarnaast komen ook de behoefte aan informatie over hoe het incident plaats heeft kunnen vinden (OR=1,8), de behoefte aan hulp en ondersteuning (OR=1,7) en de behoefte aan erkenning dat hen een strafbaar feit is overkomen (OR=1,6) vaker voor bij de slachtoffers van digitale criminaliteit. Tevens blijkt dat slachtoffers van digitale criminaliteit meer behoefte hebben aan iemand van de politie om mee te praten of om hun gevoelens te delen (OR=1,5), aan serieus genomen te worden als slachtoffer (OR=1,4), en aan de opsporing, aanhouding en vervolging van de dader (OR=1,2). De odds ratio's voor praktische hulp bij de door het strafbare feit ontstane problemen (assistentie), bescherming door de politie (bescherming), financiële compensatie voor de geleden schade (compensatie), een andere behoefte (anders), en professionele therapie of begeleiding om de gevolgen van het strafbaar feit te verwerken (therapie), blij-

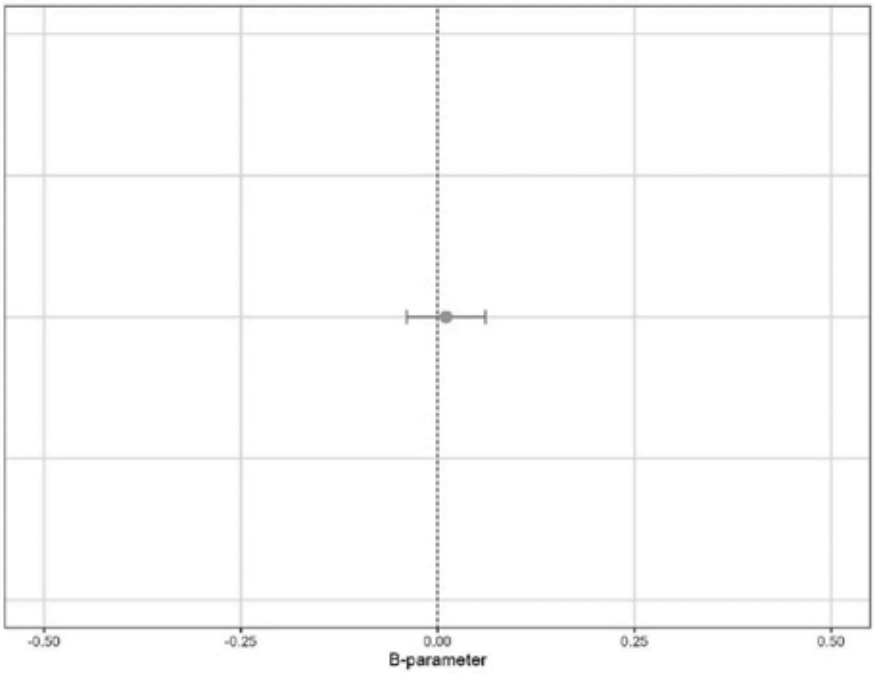
ken allemaal niet statistisch significant te zijn. De slachtoffers van digitale criminaliteit verschillen dus kennelijk niet op die behoeftes van slachtoffers van traditionele criminaliteit.



Figuur 13 OR's digitale criminaliteit voor de verschillende behoeftes van slachtoffers

6.2.3 *Tevredenheid over de politie*

Ondanks het feit dat slachtoffers van digitale criminaliteit verschillen op directe en langdurige impact en ook andere behoeftes rapporteerden dan slachtoffers van traditionele criminaliteit, laat Figuur 14 zien dat ze even tevreden zijn over de politie wanneer er rekening wordt gehouden met dit soort verschillen tussen beide groepen. De enquêteresultaten bieden geen duidelijke uitkomst voor deze bevinding. De volgende paragraaf over de resultaten die voortvloeien uit interviews met slachtoffers van digitale criminaliteit komt hierop terug.



Figuur 14 Ongestandaardiseerde regressiecoëfficiënt digitale criminaliteit voor tevredenheid

6.3 Kwalitatief onderzoek

Het kwalitatieve onderzoek, interviews met zestien slachtoffers van digitale criminaliteit, is bedoeld als illustratie bij en interpretatie van de hiervoor gepresenteerde generieke kwantitatieve resultaten.[29] Veertien van de zestien verhalen betreffen een vorm van online fraude of oplichting verbonden aan de aan- of verkoop van spullen, een valse date en gesjoemel met iemands identiteit (naam, mailadres, huisadres). Een persoonsgerichte zaak gaat over smaad/laster in de vorm van het illegaal publiceren van contactgegevens met seksuele beloften erbij. Een andere zaak betreft chantage met intieme beelden.

6.3.1 *Impact*

De impact van online fraude en oplichting op slachtoffers gaat gepaard met financiële schade, meestal enkele honderden euro's, met uitschieters naar € 7.000 en zelfs € 175.000. Hierbij valt op dat respondenten de financiële schade bij kleinere bedragen niet heel erg vinden, en vooral zichzelf de schuld geven:

29 Zie bijlage 7 voor de methode en aanpak van de kwalitatieve studie naar slachtoffers van digitale criminaliteit.

'Ik ben honderd euro kwijt, […] Ik ben er gewoon ingetrapt, dus wat doe je eraan? Misschien is het mijn eigen fout geweest.' (slachtoffer #1)

'De tweehonderd euro kon ik wel missen. Ik was vooral verrast dat ik wel meer in dit soort dingen trap. Mijn vriendin vindt me te naïef.' (slachtoffer #2)

Tegelijk nemen de gevolgen toe als de financiële schade stijgt. Zo zegt slachtoffer #12: *'Ik ben wel meer gaan werken om het geld terug te verdienen. Toen ik het terug had verdiend kon ik het wat meer loslaten.'* Daarnaast wijzen slachtoffers op andere, meer emotioneel getinte, gevolgen:

'Ik ben nu heel wantrouwig om via Marktplaats iets te kopen. Zou ik niet weer opgelicht worden?' (slachtoffer #3)

'Ik ben er wel van geschrokken, want er zat wel iemand aan mijn bankrekening. Ik ben niet per se angstiger, maar ik ben wel alerter. […] Ik controleer nu alles voordat ik iets doe.' (slachtoffer #6)

'Je staat zelf redelijk machteloos. […] Ik was echt gespannen. Je weet aan het begin niet zo goed hoe je er [diverse pogingen tot online oplichting] grip op kan krijgen.' (slachtoffer #7)

'Na een week twee of drie was het weer gezakt, maar op het moment zelf was ik van het pad af. Ik dacht in eerste instantie niet dat het mij zou overkomen. Ik had het gevoel alsof die oplichters in mijn huis zijn geweest, dat koste mij wel wat tijd. Mijn man voelde ook een bepaalde schaamte.' (slachtoffer #16)

De respondent van wie haar gegevens door een onbekende dader op internet werden gepubliceerd, vertelt over schaamte als gevolg van het delict:

'Voor mij is het nu al drie jaar geleden, maar nog steeds heb ik dat ik mensen niet zo makkelijk vertrouw. […] Ik krijg tot op de dag van vandaag nog steeds volgverzoeken van jongens, maar die kan ik gelukkig afwijzen. […] Ik heb wel dat ik me schaam.' (slachtoffer #5)

Een slachtoffer dat werd gechanteerd met intieme beelden vertelt ook over schaamte en bijkomende stress die het delict met zich meebracht:

'Ik was wel echt heel erg gestrest, want ik wilde niet dat ze deze filmpjes door zou sturen. Ik zou dit niet nog een keer doen. […] Ik heb het met niet zo veel mensen gedeeld [en] wil dat het anoniem blijft. Ik heb het zelfs niet met mijn ouders besproken.' (slachtoffer #9)

Uit bovenstaande citaten spreekt een breed spectrum aan gevolgen van digitale delicten – van 'eigen fout', 'schaamte', 'angst', 'verdriet', 'stress', 'machteloosheid', 'alerter zijn', tot 'zich minder veilig voelen' en 'wantrouwen' – en is conform aan inzichten uit de literatuurstudie over slachtofferschap van digitale criminaliteit (hoofdstuk 2) en sluit ook aan bij inzichten uit bovenstaande kwantitatieve analyse over de impact van delicten.

6.3.2 *Behoeften*

Slachtoffers geven met regelmaat aan behoefte te hebben aan financiële schadevergoeding en/of een strafrechtelijke vervolging van daders. Dat geldt vooral bij oplichting voor hoge bedragen en in de zaak over smaad/laster:

> *'Het mooiste zou zijn als ik mijn geld terug zou krijgen waar ik hard voor moet werken.'* (slachtoffer #3)

> *'Ik wilde eigenlijk dat de dader werd opgepakt, dat was mijn voornaamste doel. Ik had die verwachting eerlijk gezegd wel.'* (slachtoffer #5)

> *'Ik wil heel graag mijn geld terug. Ik ben 175.000 euro kwijtgeraakt. Dat wil ik graag terug. Ik wil ook heel graag dat hij opgepakt wordt. Ik heb de behoefte om niet over mij heen te laten lopen.'* (slachtoffer #13)

Daarnaast geven verschillende slachtoffers aan behoefte te hebben aan een 'luisterend oor', aan 'serieus genomen worden' en aan 'emotionele ondersteuning' en aan 'hulp' of 'tips':

> *'Voor mij heeft de politie goed naar me geluisterd. Ik ben twee of drie keer gebeld en ze hebben mij echt serieus genomen. Dat vond ik erg fijn en had ik niet verwacht.'* (respondent #1)

> *'Ik ben wel gehoord, dus ik vind dat de politie genoeg heeft gedaan. Ik ben serieus genomen.'* (slachtoffer #3)

> *'Het was vooral dat ik mijn verhaal kwijt kon. […] Ik had behoefte aan hulp, een luisterend oor. Ik had behoefte aan tips. […] Ik had niet echt een hoge verwachting, maar de politie heeft het echt netjes gedaan.'* (slachtoffer #16)

Deze behoeften liggen in lijn met de eerdere kwantitatieve analyse waarin 'hulp' en 'advies' (hulpbehoeften) alsook een 'luisterend oor' en 'serieus genomen worden' (emotionele behoeften) al naar voren kwamen. Als bedragen kleiner zijn of als de bank de financiële schade vergoedt, vertellen respondenten niet zozeer behoefte te hebben aan

financiële compensatie voor zichzelf of vervolging van verdachten te wensen. Zij willen veeleer dat dat de dader stopt met het maken van nog meer slachtoffers.

> *'Ik wilde eigenlijk dat die jongen niet verder ging met zijn strafbare feiten, dus daarom heb ik aangifte gedaan.'* (slachtoffer #1)

> *'Ik dacht: wellicht maakt deze dader meer slachtoffers en ik wilde dit graag voorkomen.'* (slachtoffer #6)

Meerdere respondenten gaven expliciet aan dat zij het doen van aangifte puur deden voor 'dossieropbouw' en vanuit '(burger)plicht'. Drie voorbeelden:

> *'Ik ging er bij aangifte vanuit dat ik mijn geld niet terug zou krijgen. […] Ik denk dat de politie daar niet toe in staat is vanwege capaciteitsgebrek. Het ging mij vooral om dossieropbouw. Er waren al andere meldingen en ik dacht: als ze in de toekomst wel onderzoek zouden kunnen doen is het prettig dat ze weten dat ik ook slachtoffer van deze praktijk ben geworden.'* (slachtoffer #11)

> *'Ik had het aspect "ik wil mijn geld terug" een beetje laten varen. […] Ik hoopte dat de dader gepakt zou worden en dat hij schuldig bevonden zou worden. […] Ik dacht ook: wie weet lopen er meerdere aangiftes en kan dit toegevoegd worden aan een grotere casus. […] Het voelde als een plicht.'* (slachtoffer #12)

> *'Ik wilde graag aangifte doen, omdat het wel meerdere mensen overkomt. Ik dacht: ik wil aangifte doen, zodat het ergens geregistreerd wordt. […] Ik deed dus aangifte voor dossiervorming.'* (slachtoffer #15)

Hun verhalen getuigen van slachtoffers die minder persoonlijke behoeften hebben en vooral in het algemeen belang aangifte doen. Zij willen de politie en medeslachtoffers een dienst bewijzen.

6.3.3 *Verwachting van en tevredenheid over de politie*

Drie respondenten kregen het bericht dat het de politie was gelukt om een dader op te pakken nadat losse aangiften tot een samenhangende, grote zaak (schaalbare criminaliteit) waren opgewerkt. Dat was op voorhand niet verwacht, waardoor zij hier des te tevredener over waren:

> *'Ik heb een brief gehad […] dat ze die jongen te pakken hadden. […] Dat is een goede afloop.'* (slachtoffer #1)

> *'Ik verwachtte niets van de politie. Ik dacht: ik doe aangifte, mijn burgerplicht, zodat de politie data heeft. […] Er zijn waarschijnlijk meerdere aangiftes gedaan en toen is*

die jongen gepakt. Ik ben positief verrast door de aanpak van de politie.' (slachtoffer #2)

Zeker bij kleinere bedragen is de verwachting onder respondenten dat de politie iets met hun melding of aangifte ging doen gering. Drie slachtoffers geven aan:

'Ik wist niet wat ik van de politie kon verwachten. […] Ze zeiden tijdens de aangifte ook al dat ze er waarschijnlijk weinig mee kunnen, maar dat het wel goed is om aangifte te doen. […] Als ik een cijfer zou moeten geven… Ik vind dit een lastige vraag… Een zeven, omdat het wel duidelijk was.' (slachtoffer #6)

'Ik ben niet echt op de hoogte gehouden van mijn zaak. De vrouw van de politie zei: "Dit belandt op een stapel en ze gaan er wat mee doen wanneer ze er iets mee kunnen." Het maakt mij niet zoveel uit, maar ik heb niks meer van ze gehoord.' (slachtoffer #14)

'De politie heeft me direct al verteld dat ze niks met de aangifte konden. Dit was ook niet mijn intentie. […] Ja, ze hebben de aangifte netjes opgenomen, ik kan niks anders zeggen.' (slachtoffer #15)

Bovenstaande antwoorden geven een verklaring voor waarom er tussen aangevers van digitale criminaliteit en aangevers van traditionele criminaliteit geen verschil bestaat in tevredenheid over de politie, zoals uit de kwantitatieve analyse naar voren kwam. Als de politie slachtoffers vertelt niet veel voor hen te kunnen betekenen, wat die slachtoffers van tevoren al verwachtten, zijn zij niet per se ontevreden over de politie.

Zoals al uit de passage over behoeften van slachtoffers blijkt, zijn respondenten vooral tevreden als er contact is met een politiemedewerker die de tijd neemt om te luisteren en een vriendelijke houding aanneemt. In de woorden van respondent #8:

'Er zat een jonge meneer die gewoon open vroeg naar het verhaal. Hij wilde weten wat er was gebeurd.'

Respondenten laten weten dat ze ook tevreden zijn over de politie als een medewerker achteraf iets laat horen via een brief of persoonlijk contact. Dat contactmoment moet niet te snel na aangifte zijn (een dag of paar dagen later een standaardafwijzingsbrief krijgen voelt niet goed), maar moet ook niet te lang duren. Tegelijk zijn er slachtoffers die kritiek hebben op de handelwijze van politie:

'Ik wilde natuurlijk serieus genomen worden, dat iemand écht naar je luistert en dat iemand zegt wat je kan doen. […] Ik vind het fijn dat je op de hoogte wordt gehouden, maar dat is dus ook niet gebeurd.' (slachtoffer #4)

> *'Ik wilde dat de politie mij zou helpen, maar dat hebben ze niet gedaan.'* (slachtoffer #10)

Een slachtoffer uit specifieke teleurstelling, omdat zij bewijsmateriaal heeft ingeleverd, maar desondanks van de politie te horen krijgt dat haar zaak is afgewezen:

> *'Ik hou er toch een gevoel van teleurstelling aan over, juist omdat ik zoveel moeite had gedaan.'* (slachtoffer #12)

Kortom, of respondenten bij relatief geringe schadebedragen hun geld terugkrijgen en of de dader wordt gepakt lijken minder belangrijk voor hun gevoel van tevredenheid over de politie dan of zij prettig bejegend zijn, of er na aangifte nog contact is opgenomen en of de politie door slachtoffers aangeleverd bewijsmateriaal heeft meegenomen in het onderzoek.

6.4 Tot besluit

Bovenstaande inzichten uit de kwantitatieve en kwalitatieve studie kunnen in het licht worden geplaatst van bestaande literatuur over slachtofferschap digitale criminaliteit (zie hoofdstuk 3). Dan vallen ten minste twee zaken op. Ten eerste: waar onder andere Bluhm en collega's (2023) geen verschillen in impact tussen slachtoffers van digitale criminaliteit en slachtoffers van traditionele criminaliteit vonden, komen deze verschillen wel degelijk uit onderhavig onderzoek naar voren. Ook Borwell en collega's (2024, 2025) concluderen dat de impact van delicten op slachtoffers van digitale criminaliteit anders – en soms groter – is vergeleken met slachtoffers van traditionele criminaliteit.

Ten tweede, en in lijn met Bluhm en collega's (2023), hebben slachtoffers van digitale criminaliteit, naast emotionele behoeften, relatief veel behoeften aan hulp en ondersteuning. Contra Bluhm en collega's (2023) die juist het omgekeerde vonden, wijst de kwantitatieve analyse uit dat aangevers van digitale criminaliteit, in vergelijking met aangevers van traditionele criminaliteit, iets meer behoefte hebben aan de opsporing, aanhouding en vervolging van de dader. Deze behoefte aan strafrechtelijke vervolging komt minder sterk naar voren uit de zestien interviews met slachtoffers van digitale criminaliteit. Resultaten uit het kwalitatieve onderzoek zijn echter illustratief, niet representatief.

Tot slot is er gekeken naar de tevredenheid van slachtoffers van digitale criminaliteit en van slachtoffers van traditionele criminaliteit over de afhandeling van hun zaak door de politie. Daar blijkt geen verschil tussen de groepen. Slachtoffers van digitale criminaliteit zijn dus even tevreden over de politie als slachtoffers van traditionele criminaliteit. In de literatuur zijn er wel aanwijzingen dat slachtoffers die internetaangifte hebben gedaan van een (digitaal) delict, significant minder tevreden zijn dan slachtoffers

die in persoon op een bureau of per ter telefoon aangifte deden (Jansen en collega's, 2024). Aangiftekanalen doen er in de praktijk toe. In bovenstaande kwantitatieve studie is echter gecontroleerd voor de invloed van deze variabele. Daarmee is de specifieke invloed van aangiftekanalen op tevredenheid over de politie uit de resultaten gefilterd.

7. Samenvattende conclusie en reflectie

7.1 Inleiding

Dit rapport gaat over de belangrijke, maar onderbelichte en vaak ook ondergewaardeerde rol die basisteams spelen in de aanpak van digitale criminaliteit. Basisteams zijn vaak het eerste aanspreekpunt voor burgers die online zijn opgelicht of bedreigd/belasterd. De gewenste stap van een 'transformatie' naar een meer op digitale criminaliteit gerichte politie is echter niet zomaar gezet. Ondertussen neemt het aantal slachtoffers van digitale criminaliteit toe en hebben deze delicten een flinke impact op hen. Daarom is zowel het perspectief van medewerkers op basisteams als het perspectief van slachtoffers op deze materie onderzocht. Het eerste deel van dit hoofdstuk geeft antwoord op de onderzoeksvragen. Hiermee ontstaat een samenvattende conclusie van de gevonden resultaten (7.2). Het tweede deel bevat een reflectie op deze resultaten met handreikingen voor beleid en praktijk bij de politie (7.3).

7.2 Antwoorden op de onderzoeksvragen

Wat is er in de wetenschappelijke literatuur bekend over definities, slachtofferschap en politiële aanpak van digitale criminaliteit op basisteams?

Digitale criminaliteit is een niet eenvoudig te definiëren concept. Een definiërend aspect van dit type criminaliteit is dat er door criminelen gebruik wordt gemaakt van informatie- en communicatietechnologie – computers, computernetwerken, smartphones, iPads en andere gegevensdragers – om strafbare feiten mee te plegen. Basisteams richten zich in de praktijk hoofdzakelijk op veelvoorkomende vormen van digitale criminaliteit die soms ook met fysieke criminaliteit samengaan en daarmee een hybride karakter hebben. Een categorisering van deze veelvoorkomende vormen van digitale criminaliteit bestaat uit delicten met financieel gewin, persoonsgerichte delicten en chantage/afpersing.

Net als bij fysieke, traditionele criminaliteit geldt voor slachtoffers van digitale criminaliteit dat hoe ernstiger het delict, hoe eerder er aangifte bij de politie wordt gedaan. Ook blijkt uit onderzoek dat slachtoffers delicten bij banken en verzekeraars melden met het oog op schadevergoeding. Als slachtoffers aangifte bij de politie doen willen ze graag dat het probleem stopt, dat ze erkenning en desnoods een schadevergoeding

krijgen, dat de dader wordt gepakt (en wordt vervolgd), dat geschonden relaties worden hersteld, dat de online omgeving veiliger wordt en dat informatie wordt gedeeld over het delict en de vervolging daarvan. Verder komt uit onderzoek naar voren dat een combinatie van persoonskenmerken leidt tot een groter risico op (herhaald) slachtofferschap: extraversie, bereidheid om risico's nemen (openheid), verminderde emotionele stabiliteit, (te) goed van vertrouwen zijn (altruïsme) en conformeren aan de sociale omgeving ('doen wat moet'). Tevens laat onderzoek zien dat de impact van digitale criminaliteit op slachtoffers fors kan zijn. Afhankelijk van het delict doet de impact niet onder voor en is die soms groter dan bij traditionele, fysieke criminaliteit. De impact van digitale criminaliteit heeft financiële (verlies van geld), emotionele (shock, stress, woede, schaamte, enzovoort), sociale (stigmatisering, eenzaamheid, enzovoort) en fysieke (gezondheidsklachten) dimensies.

Voor de bestrijding van grootschalige digitale criminaliteit zijn er op nationaal en regionaal niveau operationele rechercheteams ingericht. Basisteams houden zich voornamelijk bezig met relatief 'eenvoudige' zaken. Daarnaast zetten RSC (afspraken voor) aangiften aan basisteams door en spelen zij een rol bij het verwerken van online aangiften bestemd voor deze teams. Basisteams krijgen via verschillende kanalen – onder andere via online aangiften, aangiften op het bureau en via LMIO – zaken binnen die betrekking hebben op digitale criminaliteit. Nadat zaken I&S zijn gepasseerd, maken casescreeners een prioritering en selectie, en volgt er eventueel een opsporingstraject. Vanuit bestaand onderzoek rijst het beeld op van zowel capaciteitsgebrek als achterblijvende kennis en kunde bij politiemedewerkers. Digitaal wijkagenten belichamen in dit verband een relatief nieuwe functie.

Hoe zien het werkaanbod, de afhandeling en de opvolging van digitale criminaliteit er op basisteams in kwantitatieve zin uit?

De totale omvang van het werkaanbod van digitale criminaliteit bij de politie ligt in de onderzoeksperiode oktober 2022 tot en met september 2023 naar schatting tussen de 111.000 en 127.000 registraties. Het gaat hierbij om meldingen en aangiften van delicten met een substantiële digitale component. Op basis van deze schatting bedraagt het aandeel digitale criminaliteit op het totaal aantal aangiften op z'n minst tussen de 12% en 14%. Bijna driekwart van het werkaanbod digitale criminaliteit betreft fraude, een vijfde bestaat uit persoonsgerichte criminaliteit (meestal bedreiging of stalking) en 5% gaat over chantage/afpersing (geregeld sextortion). Ruim de helft van de online fraudedelicten gaat over aan- en verkoopfraude. Andere veelvoorkomende fraudedelicten zijn bankhelpdeskfraude, misbruik van accounts voor bestellingen en hulpvraagfraude. Veel persoonsgerichte delicten worden zowel digitaal als in de fysieke ruimte gepleegd en hebben daardoor een hybride karakter.

Persoonsgerichte delicten komen meestal binnen in de vorm van een melding (ruim 70% van de onderzochte gevallen). Van fraudedelicten doen slachtoffers juist vaker

aangifte (90%). Ruim 40% van de aangiften/meldingen wordt direct op een basisteam, bijvoorbeeld aan de balie, gedaan. Een kwart van de aangiften stroomt landelijk binnen via het LMIO en nog een kwart komt bij een RSC van de regionale eenheden vandaan. Basisteams zijn in ruim tweederde van de gevallen verantwoordelijk voor de verdere afwikkeling van de zaak. Het LMIO pakt in eerste aanleg de internetaangiften over aan- en verkoopfraude op. Na een veredelingsslag door LMIO wordt een pakket aangiften voor verdere afhandeling aangeboden aan een basisteam waar de verdachte binnen het werkgebied woont.

Kijkend naar de door de basisteams afgehandelde zaken in BVH komt naar voren dat deze teams – in vergelijking met het totaalbeeld van digitale criminaliteit – verhoudingsgewijs vaak te maken krijgen met fraudedelicten (tweederde van het werkaanbod). Daarnaast is de instroom van persoonsgerichte delicten (ruim een kwart van het werkaanbod) fors. Het gaat hierbij vooral om bedreiging en stalking. Een meerderheid van de zaken die over digitale criminaliteit gaat wordt door de basisteams niet in behandeling genomen. Bijna 70% van de onderzochte zaken is afgewezen of vroegtijdig beëindigd. In verhouding worden fraudedelicten vaker afgewezen of vroegtijdig beëindigd dan persoonsgerichte delicten. Bij zaken met een afgeronde status is niet altijd duidelijk in hoeverre de politie ook echt opsporingshandelingen heeft verricht. Het is mogelijk dat er alternatieve interventies zijn ingezet. Van de zaken met een afgeronde status worden door de basisteams in bijna een kwart van de gevallen één of meerdere verdachten ingezonden naar het OM. Dit komt neer op 5% van de totaal onderzochte instroom in BOSZ, een cijfer dat niet veel afwijkt van veel andere, qua ernst min of meer vergelijkbare, delicten.

Hoe is de aanpak van digitale criminaliteit binnen basisteams ingebed?

De zes onderzochte locaties – Team Noord, Team Oost, Team Midden, Team Stad, Team Strand en Team Zee – hebben allemaal hun eigen karakteristieken qua werkaanbod en inrichting. Bovendien kennen ze allemaal een andere snelheid waarop ze zich digitaal ontwikkelen. Een aantal eenheden bevindt zich in de voorhoede van de digitale transformatie. Dat leidt tot meer innovatie en aandacht voor de aanpak van digitale zaken op basisteams. Waar er vanuit de eigen eenheid minder wordt gefaciliteerd en georganiseerd op digitaal vlak, moeten basisteams hard werken om de digitale basis op orde te krijgen. Basisteams missen een eenduidige sturing vanaf centraal niveau.

Op basisteams ligt de prioriteit bij de aanpak van traditionele (voornamelijk fysieke) vormen van criminaliteit, bij 'prio-1'- en heterdaadzaken. Digitale criminaliteit komt er voor basisteams een soort van 'bij'. Het enthousiasme of de 'drive' van enkelingen op de teams zorgt voor extra aandacht voor de aanpak van digitale criminaliteit. Maar het blijft een worsteling hoe goed om te gaan met het spanningsveld tussen fysiek en digitaal politiewerk, zeker in een tijd waarin basisteams kampen met hoge werkdruk door onderbezetting.

Blauwe teams spelen een belangrijke rol in de aanpak van digitale criminaliteit, ook al wordt hun rol vooralsnog onderschat en onvoldoende gezien. Het zijn de medewerkers van deze teams die in direct contact staan met 'hun' burgers. Deze medewerkers hebben een signalerende rol, waarbij zij het digitale domein en fysiek contact bij elkaar brengen – en dat is van grote waarde. Veel digitale criminaliteit behoort ook tot de 'eenvoudiger' zaken die op een VVC afgehandeld kunnen worden. Hierdoor komt er nogal wat op de basisteams af.

Tegelijk blijkt het voor medewerkers lastig om een precieze schatting te maken van 'hoe groot' de omvang en het werkaanbod van digitale criminaliteit op hun teams is. Zij vertellen dat aangiften en meldingen 'frequent' binnenkomen en dat 'de helft' dan wel een 'aanzienlijk' of 'groot' deel een digitale component heeft. Bovendien lopen fysieke en digitale aspecten van criminaliteit in elkaar over ('hybride' delicten) en komt op basisteams veel 'schaalbare' en 'grensoverschrijdende' digitale criminaliteit voorbij. Dergelijke zaken zijn omvangrijk en niet eenvoudig te behappen voor afzonderlijke blauwe teams, ook al wordt er vanuit diverse kanten (waaronder Centurion) gewerkt aan het uniformer inrichten van het bundelen van zaken.

Doordat medewerkers van basisteams de verhalen van slachtoffers uit de eerste hand horen, leeft er bij hen het besef dat de impact van digitaal slachtofferschap groot kan zijn. Bij basisteams komt een gevoel van 'tekortschieten' richting de burgers naar voren. Medewerkers zouden graag meer willen en kunnen betekenen voor slachtoffers in de afhandeling van zaken. Immers, veel digitale zaken worden niet opgevolgd. Wel doen basisteams extra hun best als er sprake is van kwetsbare slachtoffers, zoals ouderen of juist kinderen en jongvolwassenen.

Keuzes maken in het wel of niet oppakken van zaken is binnen de teams voortdurend aan de orde. Er wordt daarbij gewerkt volgens kaders en tools die helpen in het nemen van beslissingen. Toch blijft ook daar, in samenspraak met het OM, enige ruimte voor maatwerk, zoals het laten meewegen van 'maatschappelijke impact' of 'context'. De wijze waarop dit proces is ingericht (onder andere via 'triage') en hoe keuzes worden gemaakt verschillen – wederom – van team tot team. Keuzes maken betekent automatisch dat niet alles 'gedaan' kan worden. In veel gevallen krijgen digitale delicten geen opvolging vanwege de lage prioriteit die eraan wordt gegeven, het gebrek aan opsporingsinformatie en/of het ontbreken van zicht op daders.

Zoals eerder opgemerkt: het opbouwen van digitale expertise op basisteams lijkt momenteel voorbehouden aan gedreven enkelingen. De aanwezigheid van ondersteuning in de vorm van kennisproducten, maar bijvoorbeeld ook cyberdeskundigen en digitaal experts, wisselt per team. Er leeft binnen de basisteams terughoudendheid of koudwatervrees ten aanzien van (nieuwere) digitale vormen van criminaliteit. Medewerkers geven aan behoefte te hebben aan gerichte toerusting op het 'digitale blauwe werk': op wat nodig en functioneel is in het licht van ieders 'blauwe rol' in de aanpak van digita-

le criminaliteit, waarbij een combinatie van generieke basiskennis bij iedereen in combinatie met specialistische kennis voor enkelen ideaal lijkt.

Hoe vindt de afhandeling van digitale criminaliteit op zaakniveau binnen basisteams plaats?

Om deze vraag te kunnen beantwoorden zijn reconstructies van 77 digitale zaken gemaakt. Het is op basis van deze reconstructies duidelijk dat op basisteams het besef leeft dat digitale criminaliteit (ook in combinatie met fysieke delicten) integraal deel uitmaakt van hun werk. Tegelijk wijzen de zaakreconstructies uit dat het 'online blauwe' werk niet eenduidig is ingericht op de basisteams. In lijn met het vorige onderdeel: sommige basisteams gaan voortvarend te werk, maar het blijft voor medewerkers ook zoeken, proberen en worstelen hoe met digitale zaken om te gaan.

Uit de zaakreconstructies blijkt dat een breed scala aan – soms zeer complexe – delicten bij basisteams binnenkomt. Ook de beoordeling van digitale criminaliteit is geen sinecure. De aanpak van dit soort criminaliteit vergt kennis van wisselende verschijningsvormen om patronen te doorzien, te begrijpen wat er exact heeft plaatsgevonden en de strafbaarstelling te kunnen doorgronden. Die kennis verschilt per politiemedewerker. Vanwege snel veranderende ontwikkelingen in digitale criminaliteit (bijvoorbeeld in modus operandi) is constante bijscholing noodzakelijk.

Keuzes van politiemedewerkers om zaken al dan niet op te pakken zijn vooral ingegeven door beschikbare capaciteit in combinatie met de aanwezigheid van opsporingsindicaties. Circa 63% van de geanalyseerde zaken wordt afgewezen of vroegtijdig beëindigd (volgens de quickscan is dit zelfs 70%). Politiemedewerkers werken met selectiviteitskaders en een prioriteringstool om zaken te beoordelen op impact, omvang en haalbaarheid. De toepassing daarvan verschilt per basisteam en ook de menselijke beoordelingsfactor speelt een rol. Alternatieve afdoening (onder andere waarschuwingen en stopgesprekken) inzake digitale criminaliteit lijkt in opkomst.

Waar basisteams en digi-specialisten in zaken samenwerken, leidt dit tot positieve resultaten. Toch blijkt het vinden van de juiste weg naar elkaars expertise en naar 'wie wat moet doen' regelmatig diffuus. Hetzelfde geldt voor het 'eigenaarschap' van zaken. Op basis van de geanalyseerde zaken komt naar voren dat de politie bij digitale persoonsgerichte delicten vaker externe hulpverleners en zorgpartners (zoals Veilig Thuis) betrekt dan bij online fraudezaken. Bij de laatste soort zaken komen wel andere partijen, waaronder banken en verzekeraars, in beeld. Vanuit de basisteams bestaat er behoefte om de samenwerking met dit soort private partijen structureler te maken, maar die behoefte ontstijgt hun invloedssfeer.

Zoals hierboven al aangestipt zijn aangiften van digitale criminaliteit 'schaalbaar'. Het LMIO ondersteunt bij het koppelen van zaken. Geïnterviewde politiemedewerkers zijn

doorgaans tevreden over deze werkwijze, al verloopt het niet in alle opzichten vlekkeloos. Eenvoudige zaken van aan- en verkoopfraude, maar ook grotere zaken met aanzienlijke schadebedragen, verschijnen nu via LMIO op de radar van een basisteam. Maar omdat digitale criminaliteit snel schaalbaar is, hebben basisteams ook behoefte om andere zaken dan online aan-en verkoopfraude te koppelen en te routeren. Dat kan bijvoorbeeld door de inzet van digitale (screening)hubs binnen eenheden.

Conform eerdere bevindingen, vertellen politiemedewerkers in hun reflectie op zaken dat zij het idee hebben niet altijd genoeg te kunnen doen voor slachtoffers van digitale criminaliteit. Dit geldt met name voor de wijze waarop het contact met politie verloopt: via internet of via een (later in te plannen) afspraak voor aangifte. Zij onderkennen de hoge impact die digitale criminaliteit op slachtoffers kan hebben, maar dit komt volgens hen niet voldoende terug in de afhandeling van aangifte en meldingen. Ter nuancering: het valt op dat basisteams zaken met kwetsbare slachtoffers (waaronder ouderen of minderjarigen) wel voortvarend oppakken.

Tot slot tonen de 77 geanalyseerde zaken aan dat verdachten van persoonsgerichte delicten vaker bij de basisteams in beeld komen dan verdachten van online fraude. Verdachten van online fraude kunnen echter ook 'lokale types' zijn die in het werkgebied van basisteams traditionele delicten plegen. Deze verdachten zijn soms reeds bekenden van de politie of geven het basisteam een haakje om in contact te komen met andere overlast gevende dan wel criminele personen in hun werkgebied. Daarnaast komen geldezels op de radar van de basisteams. Zij worden verdacht van witwassen, maar kunnen soms ook als slachtoffer worden gezien. Het vinden van de achterliggende (intellectuele) dader van online fraudezaken, waarbij geldezels zijn ingezet, blijkt niet eenvoudig voor een basisteam.

Wat is de impact van digitale criminaliteit op slachtoffers, welke behoeften hebben zij bij aangifte en hoe tevreden zijn zij met de politie na aangifte, in vergelijking met slachtoffers van traditionele vormen van criminaliteit?

Ten eerste tonen de resultaten van het kwantitatieve onderzoek (N=25.760) aan dat slachtoffers die aangifte van digitale criminaliteit hebben gedaan meer impact ervaren dan slachtoffers van traditionele criminaliteit. Slachtoffers van digitale criminaliteit ervaren zowel meer directe als bepaalde typen langdurige gevolgen. Direct na het incident ervaren slachtoffers van digitale criminaliteit vaker gevoelens van wanhoop, psychische shock en hulpeloosheid dan slachtoffers van traditionele criminaliteit. Op lange termijn is er variatie in welke gevolgen beide groepen vaker ervaren. Logischerwijs komen onveiligheidsgevoelens op het internet veel vaker voor bij slachtoffers van digitale criminaliteit, en ook schuldgevoelens en voorzichtiger (online) gedrag komen regelmatiger voor bij de groep slachtoffers van digitale criminaliteit. Ook uit het kwalitatieve onderzoek (N=16) spreken gevoelens van kwetsbaarheid, angst, schaamte en onveiligheid onder respondenten. Andere gevolgen komen juist meer voor bij de

slachtoffers van traditionele criminaliteit; deze groep ervaart vaak later nog boze en angstige gevoelens en ook meer stress dan aangevers van digitale criminaliteit.

Ten tweede blijkt dat slachtoffers van digitale criminaliteit meer behoeftes hebben dan slachtoffers van traditionele criminaliteit. Van de elf onderzochte behoeftes worden er zeven vaker ervaren door slachtoffers van digitale criminaliteit. Met name de behoefte aan advies om herhaling van hetzelfde strafbare feit te voorkomen is aanzienlijk hoger bij deze groep. Daarnaast komen de behoeftes aan hulp en ondersteuning, erkenning, en informatie over hoe het incident heeft kunnen plaatsvinden, aanzienlijk vaker voor bij slachtoffers van digitale criminaliteit. Ook blijken slachtoffers van digitale criminaliteit meer behoefte te hebben aan iemand bij de politie om mee te praten, om gevoelens mee te delen en serieus te worden genomen als slachtoffer, dan aangevers van traditionele criminaliteit. Dit soort behoeften wordt ook door de respondenten in het kwalitatieve onderzoek genoemd. Voorts hebben aangevers van digitale criminaliteit iets meer behoefte aan de opsporing, aanhouding en vervolging van de dader. Dit blijkt overigens niet per se uit de – niet-representatieve – kwalitatieve studie (veel hangt waarschijnlijk af van de ernst van het delict). Ook gaven respondenten tijdens de interviews aan dat zij het doen van aangifte zien als hun 'burgerplicht'.

Tot slot is er geen duidelijk verschil gevonden in hoe tevreden slachtoffers van digitale criminaliteit en van traditionele criminaliteit zijn over de politie. Beide groepen scoren min of meer gelijk. Slachtoffers van digitale criminaliteit zijn dus even tevreden over de politie als slachtoffers van traditionele criminaliteit. Het is speculeren waarom de kwantitatieve analyse hier geen verschil laat zien. Een mogelijke verklaring is dat beide groepen andere verwachtingen hebben van de politie. Uit de interviews komt naar voren dat slachtoffers van digitale criminaliteit niet altijd de verwachting hebben dat de politie hun zaak ook echt oppakt. Als politiemedewerkers slachtoffers hierover eerlijk informeren en hen vriendelijk en fair bejegenen, leidt dat wellicht toch tot een zekere mate van tevredenheid – of in ieder geval niet tot een grote mate van ontevredenheid – over de politie.

7.3 Betekenis voor de politie: verschil maken met 'online blauw'

Dit onderzoek wil een bijdrage leveren aan het benadrukken van het belang van de rol die basisteams spelen in de aanpak van digitale criminaliteit, een rol die te lang onderbelicht is gebleven.[30] Deze situatie is niet meer van deze tijd en moet anders. Op basis van bevindingen uit het onderzoek gaat deze reflectie in op de rol van basisteams bij de aanpak van digitale criminaliteit en het belang van 'online blauw' politiewerk. Wil de politie echt werk maken van de aanpak van digitale criminaliteit en slachtoffers helpen,

30 Lopende het onderzoek, tussen de regels door, maar vooral uit de zaakreconstructies, terugkoppelsessies en expertsessies kwamen ideeën naar voren over dat wat (nu al) goed blijkt te werken en wat verbeterpunten zijn in het online blauwe werk. Deze ideeën vormen de basis voor deze reflectie.

dan is het zaak om de 'digitale basis' van basisteams grondig op orde te brengen, medewerkers te faciliteren en, waar mogelijk, te ontlasten. Het is cruciaal om digitale criminaliteit ook als veelvoorkomende criminaliteit te gaan zien en te behandelen en om de positionering van blauwe teams in de aanpak van digitale criminaliteit te professionaliseren. Er zal gewerkt moeten worden aan blauwe kennis en expertise en aan meer eenduidigheid in de aansturing van de teams. Het online blauwe werk heeft, kortom, extra aandacht, begeleiding en inzet nodig.

7.3.1 *Digitale criminaliteit is veelvoorkomende criminaliteit*

Digitale criminaliteit is veelvoorkomende criminaliteit en is daarmee in toenemende mate een zaak van het 'blauwe', gebiedsgebonden politiewerk. Rond 41% van het digitale werkaanbod van de politie komt binnen via de basisteams en rond 67% van het totale digitale werkaanbod wordt op basisteams afgehandeld. Voorliggend onderzoek maakt duidelijk dat dit besef is doorgedrongen in alle geledingen van de politie. Tegelijkertijd is digitale criminaliteit een relatief nieuw werkveld voor de veelal op fysieke criminaliteit ingerichte basisteams. Wat de aanpak van digitale delicten ingewikkeld maakt, is dat het hier gaat om vormen van criminaliteit waarvan de modus operandi voortdurend aan verandering onderhevig zijn. Daarbij komt dat digitale vormen van criminaliteit en analoge (fysieke) vormen van criminaliteit steeds vaker in elkaars verlengde liggen en in elkaar overgaan. De grens tussen 'fysieke' en 'digitale' criminaliteit vervaagt.

Parallel aan deze ontwikkeling wordt er via de 'digitale transformatie' ingezet op het incorporeren van digitale technologie in het politievak. Via diverse initiatieven, zoals Centurion en de Digitale Meldkamer, geeft de politie impulsen aan de aanpak van digitale criminaliteit. Wat opvalt is dat er in beleidsplannen tot voor kort relatief weinig, en zeker niet specifieke aandacht is geweest voor het belang van basisteams in de aanpak van digitale criminaliteit.

7.3.2 *Meerwaarde van basisteams in de aanpak van digitale criminaliteit*

Experts benadrukken de noodzaak te komen tot toekomstbestendige en op digitaal vlak goed toegeruste basisteams. Want basisteams blijken van cruciaal belang in de aanpak van digitale criminaliteit. Niet alleen omdat daar een groot aandeel van digitale zaken binnenkomt en wordt afgehandeld, maar vooral ook vanwege hun binding met, en kennis van, het eigen werkgebied. Politiemedewerkers van basisteams hebben direct contact met 'hun' burgers, slachtoffers en verdachten, alsook met lokale partners. Richting lokale criminelen die zich (ook) met digitale criminaliteit bezighouden, zijn het wederom politiemedewerkers van basisteams die ontwikkelingen signaleren en mogelijkheden hebben om (beginnende) criminele activiteiten te verstoren. Denk bijvoorbeeld aan het 'aanlopen' van verdachten en het voeren van stopgesprekken met

geldezels en 'first offenders'. De inzet van 'alternatieve interventies' – herstelgericht optreden buiten en naast het strafrecht – is binnen de politie in ontwikkeling.

Ook voor slachtoffers zijn basisteams het eerste aanspreekpunt. Het zijn veelal medewerkers van I&S die de aangiften en meldingen opnemen. Van hen wordt verwacht dat ze met kennis van zaken handelen en kwaliteit leveren: dat er tijdens gesprekken met slachtoffers wordt doorgevraagd en dat aangiften volledig zijn. Persoonlijke aandacht is altijd, en zeker bij delicten met een persoonsgerichte component als stalking of bedreiging, van grote waarde voor slachtoffers. Het gaat dan om (h)erkenning van slachtofferschap en het voorkómen van 'self blaming' of 'victim blaming'. Hierbij is het zaak de bijdragen van basisteams inzake digitale criminaliteit te begrenzen tot daar waar hun daadwerkelijk toegevoegde waarde ligt, en om dat beter in beleid en processen te verankeren en te faciliteren. Samengevat komt dit neer op: de kennis van en binding met de eigen wijk, het directe contact met burgers, slachtoffers en verdachten, de betrokkenheid direct na het delict en het afhandelen van eenvoudige zaken.

7.3.3 *Blauwe kennis en expertise*

Generalistische basiskennis is waar medewerkers van een basisteam over moeten beschikken. Het gaat daarbij om kennis over verschijningsvormen, impact, reikwijdte en werking van digitale criminaliteit. Daarnaast dienen zij te beschikken over basisvaardigheden om 'digitaal boeven te vangen'. De veranderlijke aard van digitale criminaliteit vraagt om een continu lerende houding van medewerkers. Niet anders dan bij andere vormen van criminaliteit is het zaak bij te blijven qua kennis over fenomenen, modus operandi, werkwijzen om 'de juiste vragen' te kunnen stellen en terminologie te kennen. Tot hoever het niveau van basiskennis moet reiken is vooralsnog niet goed gedefinieerd en zal vanuit de praktijk nader gestalte moeten krijgen. Bovendien lijkt het qua (basis)kennis van en inzet op digitale criminaliteit in de onderzochte basisteams meestal goed te gaan dankzij het enthousiasme van individuele medewerkers, dit in plaats van door goede organisatorische borging. Dat maakt basisteams kwetsbaar, zeker als medewerkers daar vertrekken of met pensioen gaan.

Een andere organisatorische kwetsbaarheid is dat basisteammedewerkers momenteel worden overstelpt met verschillende soorten informatieproducten en tools. Het gaat hier om factsheets, platforms, informatiekanalen, handboeken, tips en tricks, enzovoort, waardoor zij soms door de bomen het bos maar moeilijk kunnen vinden. Er is onder deze medewerkers behoefte aan eenduidige en goed toegankelijke producten en hulpmiddelen. Medewerkers van basisteams leren het echte politievak in de praktijk door met slachtoffers in aanraking te komen, incidenten af te handelen, onderzoeken te draaien – simpelweg door 'iets met digitale criminaliteit te moeten'. Essentieel is dan ook het opdoen van ervaring ('vlieguren maken') in de praktijk van alledag, al dan niet in samenwerking met specialistische teams binnen politie of met in- en externe experts. Aanvullend werkt het hebben en delen van successen, zowel op als tussen basis-

teams, voor politiemedewerkers motiverend. Succes behalen zet een ander perspectief tegenover de vele niet-kansrijke en afgewezen digitale zaken.

7.3.4 *Eenduidigheid en sturing*

Het valt op dat het de onderzochte basisteams ontbreekt aan voldoende mensen en middelen voor de taak die voor hen ligt en dus ook voor de aanpak van digitale criminaliteit. Basisteams worden in de beleving van politiemedewerkers overvraagd. In feite staan ze staan voor alles aan de lat. Meer en eenduidiger sturing op de aanpak van digitale criminaliteit, waarbij uitdrukkelijk aandacht uitgaat naar de facilitering van basisteams is hard nodig. Daarmee kan worden voorkomen dat, zoals nu het geval is, op diverse plekken het wiel opnieuw wordt uitgevonden en dat eenheden, districten of teams op verschillende snelheden een eigen kant op ontwikkelen. Het is belangrijk om het digitale werk voor basisteams zo makkelijk (c.q. eenduidig) mogelijk te maken en hen zo veel mogelijk te ontlasten. Daarvoor is een steviger en uniformer inrichting van de aanpak van digitale criminaliteit noodzakelijk.

Een terugkerend knelpunt in de aanpak van digitale criminaliteit is het 'eigenaarschap' van zaken. Dit betreft het specialisme wat nodig is (inzet van het basisteam, van de districtsrecherche of toch het cybercrimeteam?), maar gaat ook over de geografische schaal van die inzet (welke eenheid/district/basisteam neemt het voortouw?). Er bestaat een risico dat aangiftes van digitale criminaliteit door niemand worden opgepakt. Want als een zaak 'te groot of complex' blijkt te zijn voor een basisteam, wil dat niet automatisch zeggen dat een DR of een ander team dan wel met de zaak aan de slag gaat. En waar meerdere slachtoffers of verdachten over het land verspreid wonen, is het nog maar de vraag of en waar precies wordt opgepakt. Binnen Centurion zet men stappen op de aanpak van online aan- en verkoopfraude, bankhelpdeskfraude, hulpvraagfraude en bankphishing, maar die sturing ontbreekt op de overige digitale delicten.

Een gedegen aanpak van schaalbare digitale criminaliteit vraagt om schakelen over basisteam- en eenheidsgrenzen heen. Daarvoor is het nodig om samen te werken met specialisten en met teams elders in de eenheid of in het land. Echte impact ontstaat in samenwerking en synergie. Uit voorliggend onderzoek blijkt dat er vaak sprake is van 'hokjesdenken' binnen de politie door 'digitaal werk' als anders dan het traditionele werk te behandelen; en dat werkt belemmerend. Binnen diverse eenheden worden – 'bottom-up' – initiatieven genomen om onderlinge samenwerking te bevorderen. Daar kunnen inspirerende lessen uit worden getrokken. Als aan initiatieven meer ruimte, begeleiding en facilitering wordt gegeven, dan kunnen er mooie nieuwe werkwijzen uit naar voren komen.

Veel digitale criminaliteit is schaalbaar en vergt dat er patronen moeten moet worden doorzien in een geheel aan meldingen en incidenten. Het is niet aan de basisteams om al die patronen te herkennen en daarop te sturen. Het OM heeft bij dit laatste een be-

palende rol; vanuit de teams is er behoefte aan meer afstemming in het beoordelen en opvolgen van zaken. Wel is duidelijk dat het routeren van verdachten van schaalbare criminaliteit en het stapelen van aangiften en meldingen, zoals door LMIO nu al gebeurt, de aanpak van digitale criminaliteit bevordert. Nadat er gestapeld en gerouteerd is en zaken zijn opgewerkt, zijn de blauwe teams voor een deel van deze zaken aan zet in de opvolging op lokaal niveau. Basisteams pleiten voor uitbreiding van het stapelen van zaken en voor het doorzien van patronen, zoals nu al in het LMIO-proces gebeurt, maar dan voor meerdere soorten schaalbare criminaliteit. Dat proces moet gaan plaatsvinden op centrale en gecoördineerde plekken binnen de politieorganisatie, zowel regionaal als landelijk.

7.3.5 *Verbeterpunten vanuit blauw perspectief*

Waar de aanpak van digitale criminaliteit goed van de grond komt, is dat veelal te danken aan gedreven politiemedewerkers, met improvisatievermogen en de benodigde kennis over het digitale werk op basisteams. Dit ondanks een veelal organisatorisch en procesmatig niet-gedegen inrichting en facilitering. Dat maakt dat er vooralsnog sprake is van een kwetsbare inrichting waar een duurzame inzet hard nodig is. Medewerkers van de onderzochte basisteams geven aan behoefte te hebben aan:

- Een steviger en eenduidiger inbedding van gebiedsgebonden politiezorg in de aanpak digitale criminaliteit. Dat geldt zowel voor visie als beleid op het 'online blauwe werk' en – in het verlengde hiervan – op organisatie, toerusting middelen, faciliteren, hulplijnen, opleiding en menskracht. Het is voor basisteams ondoenlijk deze aanpak alleen 'bottom-up' en met 'ieder voor zich' te organiseren.
- Focus op de inzet op kansrijke zaken. Hierbij gaat het hen ook om nauwere samenwerking met de DRIO (intelligence) en met het OM (afdoening).
- Betere afstemming – op landelijk en regionaal niveau – over welk basisteam binnen welke eenheid welke digitale zaak oppakt.
- Uitbreiding van het stapelen van zaken en het doorzien van patronen, zoals nu in het LMIO-proces gebeurt, maar dan voor meerdere soorten (schaalbare) digitale criminaliteit, bijvoorbeeld via de 'hubs' op eenheidsniveau als onderdeel van het landelijke Centurion-beleid.
- Meer tijd, ruimte en middelen om 'er te zijn voor de burger', specifiek voor slachtofferzorg op digitaal vlak.
- Een binnen de politie eenduidig en goed toegankelijk aanbod van kennisproducten, hulpmiddelen, expertise en hulplijnen bij de aanpak van digitale criminaliteit.

Literatuur

Akdemir, N., Sungur, B. & Başaranel, B.U. (2020). Examining the challenges of policing economic cybercrime in the UK through police lenses. *International Security Congress Special Issue*, 113–134. https://doi.org/10.28956/gbd.695956

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R. & Moon, E. (2024). *Veiligheidsmonitor 2023*. CBS.

Barrense-Dias, Y., Berchtold, A., Surís, J.C. & Akre, C. (2017). Sexting and the definition issue. *Journal of Adolescent Health, 61*(5), 544–554. https://doi.org/10.1016/j.jadohealth.2017.05.009

Bekkers, L., Van Houten, Y., Spithoven, R. & Leukfeldt, E.R. (2023). Money mules and cybercrime involvement mechanisms: exploring the experiences and perceptions of young people in the Netherlands. *Deviant Behavior*, *44*(9), 1368–1385. https://doi.org/10.1080/01639625.2023.2196365

Bijleveld, C., Salet, R., Damstra, A. & Stefanovic, D. (2021). *Politiefunctie in een veranderende omgeving*. WRR.

Black, A., Lumsden, K. & Hadlington, L. (2019). 'Why don't you just block them?': police responses to reports of online harassment and their construction of the ideal victim. In K. Lumsden & E. Harmer (eds.), *Online othering: exploring violence and discrimination on the web* (pp. 67–84). Palgrave Macmillan.

Bluhm, K., Borwell, J. & Stol, W. (2023). De slachtofferimpact van cybercrime versus traditionele criminaliteit: Aanknopingspunten voor slachtofferzorg en preventieprioriteiten. *Tijdschrift Voor Veiligheid, 21*(3/4), 13–31. https://doi.org/10.5553/tvv/.00004

Boateng, F.D. (2018). Crime reporting behavior: do attitudes toward the police matter? *Journal of Interpersonal Violence, 33*(18), 2891–2916. https://doi.org/10.1177/0886260516632356

Boekhoorn, P. (2019). *De aanpak van cybercrime door regionale eenheden van de politie: van intake van cybercrime naar opsporing en vervolging*. Politie & Wetenschap.

Boekhoorn, P. & Tolsma, J. (2016). *De aangifte van delicten bij de multichannelstrategie van de politie.* Politie & Wetenschap.

Boelens, M. & Landman, W. (2021). *Pionieren in de gebiedsgebonden politiezorg: een onderzoek naar de digitaal wijkagent in het basisteam*. TwynstraGudde/Politie Nederland.

Bolger, M. A., Lytle, D.J. & Bolger, P.C. (2021). What matters in citizen satisfaction with police: a meta-analysis. *Journal of Criminal Justice, 72*, 101760. https://doi.org/10.1016/j.jcrimjus.2020.101760

Borwell, J., Jansen, J. & Stol, W. (2018). Persoonlijkheidskenmerken van e-fraudeslachtoffers. *Tijdschrift voor Veiligheid, 17*(1/2), 54–65. https://doi.org/10.5553/TvV/187279482018017102005

Borwell, J., Jansen, J. & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions. *Journal of Digital Social Research, 3*(3), 85–110. https://doi.org/10.33621/jdsr.v3i3.66

Borwell, J., Jansen, J. & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: a novel application of the shattered assumptions theory. *Social Science Computer Review, 40*(4), 933–954. https://doi.org/10.1177/0894439320983828

Borwell, J., Schuppers, K., Rooyakkers, J. & Harteveld, A. (2020). Het cybercrimebeeld van de Nederlandse politie: van algemeen beeld naar verdiepende analyse en aanpak. *Cahiers Politiestudies,* (3)56, 39–62.

Borwell, J., Jansen, J. & Stol, W. (2024). Recht doen aan de behoeften van cybercrimeslachtoffers: reflecties op de rol van de politie. *Tijdschrift voor Veiligheid*, *23*(3), 47-78. https://doi.10.5553/TvV/.000076

Borwell, J., Jansen, J. & Stol, W. (2025). Exploring the impact of cyber and traditional crime victimization: impact comparisons and explanatory factors. *International Review of Victimology*, *31*(1), 156-181. https://doi.org/10.1177/02697580241282782

Broekhuizen, J., Mehlbaum, S. & Van den Akker, K. (2022). *Digitaal perspectief: leren van acht digitale projecten binnen de GGP*. Politie Nederland/Bureau Broekhuizen.

Bullée, J.W. (2017). *Experimental social engineering: investigation and prevention* (dissertatie). Universiteit Twente.

Bureau Beke (2024). *Aan de politiebalie: een onderzoek een vergeten groep binnen de politie*. Politie Nederland.

CBS (2022). *Integratie en samenleven 2022*. Centraal Bureau voor de Statistiek.

Cross, C., Richards, K. & Smith, R.G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice, 518*, 1–14. https://doi.org/10.52922/ti148355

Cuyper, R.H. de & Weijters, G. (2016). *Cybercrime in cijfers*. WODC.

Dekker, F., Vleeschouwer, E. de, Bos, D. & De Hartog, M. (2024). *Digitalisering in de GGP: een verkenning naar behoeften van burgers en de werkpraktijken in basisteams*. Erasmus Universiteit.

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

Domenie, M., Leukfeldt, E., Van Wilsem, J., Jansen, J. & Stol, W. (2013). *Slachtofferschap in een gedigitaliseerde samenleving*. Boom Lemma.

Donalds, C. & Osei-Bryson, K.M. (2019). Toward a cybercrime classification ontology: a knowledge-based approach. *Computers in Human Behavior, 92*, 403–418. https://doi.org/10.1016/j.chb.2018.11.039

Doornbusch, R., Heemst, M. van, Imbos, M. & Van der Linden, G. (2023). *Landelijk selectiviteitskader gedigitaliseerde criminaliteit in VVC-zaken*. OM & politie.

Eeden, C.A.J. van den, Berkel, J.J. van, Lankhaar, C.C. & De Poot, C.J. (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*. WODC.

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Halevi, T., Lewis, J. & Memon, N. (2013). A pilot study of cyber security and privacy-related behavior and personality traits. *WWW' 2013 Companion: Proceedings of the 22nd International Conference on World Wide Web*, 737–744. https://doi.org/10.1145/2487788.2488034

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

Hesseling, R. (2021). *Horizontale fraude in de eenheid Den Haag: een strategische quickscan*. Politie Nederland, eenheid Den Haag.

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

Holt, T.J. & Bossler, A.M. (2008). *The Palgrave handbook of international cybercrime and cyberdeviance*. Palgrave Macmillan.

Hoorn, J. van & Van Dijk, A.J. (2024). *De betekenis van de politie in de samenleving: artikel 3 van de Politiewet, de politietaak opnieuw doordacht*. Politie Nederland.

Jansen, J. & Leukfeldt, R. (2018). Coping with cybercrime victimization: an exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology, 6*(2), 205–228. https://doi.org/10.21428/88de04a1.976bcaf6

Jansen, J., Van Valkengoed, T., Veenstra, S. & Stol, W.P. (2020). *Level-up!: kennis voor politiewerk in een digitale samenleving*. NHL Stenden/Politieacademie.

Jansen, J., Westers, S., Twickler, S. M. A. & Stol, W.P. (2019). *Aankoopfraude vanuit het buitenland: alternatieven voor opsporing*. Politie & Wetenschap.

Jansen, R., Ruiter, S. & Van Steden, R. (2024). Crime reporting and victim satisfaction with the police: a large-scale study among victims of crime in the Netherlands. *Crime Science*, 13 (30), 1-11. https://doi.org/10.1186/s40163-024-00231-9

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

Kleij, R. van der, Van 't Hoff-de Goede, S, Weijer, S.G.A. van de & Leukfeldt, E.R. (2020). Ons cybergedrag is veel onveiliger dan we zelf denken. *Justitiële Verkenningen, 46* (2), 113–128. https://doi.org/10.5553/JV/016758502020046002011

Kort, J. & Spithoven, R. (2022). Lokale stappen in de aanpak van digitale criminaliteit. *Tijdschrift voor Veiligheid*, *21*(3-4), 109-119. https://doi.org/10.5553/TvV/.000040

Kort, J. & Spithoven, R. (2021). *De coronacrisis als cyberkeerpunt? Op zoek naar lokaal handelingsperspectief in de aanpak van gedigitaliseerde criminaliteit*. Politie Nederland.

Kunst, M. J.J. & Koster, N.N. (2017). Psychological distress following crime victimization: an exploratory study from an agency perspective. *Stress and Health, 33*(4), 405–414. https://doi.org/10.1002/smi.2725
Landelijk Platform VVC (2021). *Screenings- en selectiviteitskader misdrijven*. Politie Nederland.

Landman, W. (2023). *Politiewerk aan de horizon: technologie, criminaliteit en de toekomst van politiewerk*. Politie & Wetenschap.

Landman, W. & Groothuis, S. (2022). *Politiewerk op het web: een verkennend onderzoek naar online gegevensvergaring door de politie*. Sdu.

Leuken, M. van, Rest, R. van der & Van 't Hoff-de Goede, S. (2024). *De civielrechtelijke afdoening van online fraude*. CCV. Geraadpleegd op: https://ccv-secondant.nl/platform/article/de-civielrechtelijke-afdoening-van-online-fraude

Leukfeldt, E.R., Kentgens, A., Prins, E. & Stol, W. (2015). *Alledaags politiewerk in een gedigitaliseerde wereld, handreiking voor de intake van delicten met een digitale component*. Lectoraat Cybersafety/Open Universiteit.

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

Leukfeldt, E.R. & Roks, R.A. (2020). Cybercrimes on the streets of the Netherlands?: an exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior, 42*(11), 1458–1469. https://doi.org/10.1080/01639625.2020.1755587

Leukfeldt, E.R. & Van 't Hoff-Goede, S. (2023). Slachtofferschap van digitale criminaliteit. In J. van Doorn, J. Brands, M.J.J. Kunst et al. (red.), *Slachtoffers: onderzoek, beleid en praktijk* (pp. 240-269). Kluwer.

Leukfeldt, E.R., Veenstra, S., Domenie, M. & Stol, W. (2012). *De strafrechtketen in een gedigitaliseerde samenleving: een onderzoek naar de strafrechtelijke afhandeling van cybercrime*. Sdu.

Leukfeldt, E.R., Veenstra, S. & Stol, W. (2013). High volume cybercrime and the organization of the police: the results of two emperical studies in the Netherlands. *International Journal of Cyber Criminology, 7*(1), 1–17.

LMIO (z.d.). *Afdoeningenwaaier bij fraude met onlinehandel (F636)*. Landelijk Meldpunt Internetoplichting.
LMIO (2023). *Werkinstructie uitgestelde screening en alternatieve interventies bij fraude met onlinehandel (F636)*. Landelijk Meldpunt Internetoplichting.

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

Modic, D. & Lea, S.E.G. (2011). *How neurotic are scam victims, really? The big five and Internet scams*. Paper presented at the 2011 Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology. Exeter, UK.

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

Odinot, G., de Poot, C. & Verhoeven, M. (2018). De aard en aanpak van georganiseerde cybercrime: Bevindingen uit een internationale empirische studie. *Justitiële verkenningen, 44*(5), 9–22. https://doi.org/10.5553/JV/016758502018044005002

Oerlemans, J.J. & Van der Wagen, W. (2020). Verschijningsvormen van cybercriminaliteit. In W. Van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (red.), *Basisboek cybercriminaliteit* (pp. 55–105). Boom.

OM & Politie (2024). *Cybercrimebeeld Nederland 2024*. Geraadpleegd op: https://fts.politie.nl/cybercrimebeeld/

Parrish, J.L., Bailey, J. L. & Courtney, J.F. (2009). A personality-based model for determining susceptibility to phishing attacks. *University of Arkansas,* 285–296.

Politie (2024a). *Online fraude in beeld: fenomeenbeeld*. Politie Nederland.

Politie (2024b). *Slachtoffers sneller geholpen bij digitale criminaliteit.* Geraadpleegd op: https://www.politie.nl/nieuws/2024/februari/2/02-oost-nederland-slachtoffers-sneller-geholpen-bij-digitale-criminaliteit.html

Politieonderwijsraad (2020). *Let's get digital!: Een solide basis voor een digitaalvaardige politie*. POR.

Ray, A. & Henry, N. (2025). Sextortion: a scoping review. *Trauma, Violence & Abuse, 26*(1), 138–155. https://doi.org/10.1177/15248380241277271

Reisig, M. D. & Parks, R.B. (2000). Experience, quality of life, and neighborhood context: a hierarchical analysis of satisfaction with police. *Justice Quarterly, 17*(3), 607–630. https://doi.org/10.1080/074188200000946810

Roks, R.A., Leukfeldt, E.R., Densley, J.A, (2021). The hybridization of street offending in the Netherlands. *The British Journal of Criminology, 61*(4), 926–945. https://doi.org/10.1093/bjc/azaa091

Ruiter, S., Leuken, M. van, Ruitenburg, T. van, Schiks, J. & Leukfeldt, R. (2024). *In- en doorstroom van digitale criminaliteit in de strafrechtketen*. NSCR.

Schiks, J., Van 't Hoff-de Goede, S. & Leukfeldt, R. (2022). *Op zoek naar de parels bij de regionale en lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit*. Politie & Wetenschap.

Schuppers, K.W., Goudsmit, J. & Willekers, M. (2022). *Aanpak gedigitaliseerde criminaliteit in de eenheid Den Haag*. Politie, eenheid Den Haag.

Shapland, J. & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology, 14*(2), 175–217. https://doi.org/10.1177/026975800701400202

Sipma, T. & Van Leijsen, E.M.C. (2019). *Slachtofferschap van digitale criminaliteit: prevalentie, risicofactoren en gevolgen*. WODC.

Spithoven, R. (2020). *Verbonden risico's: maatschappelijke veiligheid in de black box society*. Boom Criminologie.

Spithoven, R., Jansen, J., Drenth, A. & Leukfeldt, R. (2022). Wijk + web: de noodzaak van een lokale aanpak van cybercriminaliteit. *Tijdschrift voor Veiligheid*, 21(3-4), 3-12. https:// doi.org/10.5553/TvV/.000040

Spithoven, R. & Leukfeldt, R. (2023). *Gemeenten lijden aan digitale koudwatervrees*. Geraadpleegd op: https://ccv-secondant.nl/platform/article/gemeenten-lijden-aan-digitale-koudwatervrees

Spithoven, R. & Van Tuijl, C. (2024). *Cyberpesten: theorie over en onderzoek naar de onbegrensde, digitale leefwereld van kinderen en adolescenten in Nederland*. Boom.

Stol, W. (2020). Digitalisering en criminaliteit: een beknopte inleiding op cybercrime. *Cahiers Politiestudies, 56*(3), 13–22.

Stol, W. & Jansen, J. (2013). *Cybercrime and the police*. Eleven International Publishing.
Stol, W., Jansen, J. & Landman, W. (2024). Digitalisering en de politiefunctie: hoe het speelveld verandert en wat dat van de politie vraagt. *Tijdschrift voor Veiligheid, 23* (1/2), 53–70. https://doi.org/10.5553/TvV/.000071

Struiksma, N., De Vey Mestdagh, C.N.J. & Winter, H.B. (2012). *De organisatie van de opsporing van cybercrime door de Nederlands politie*. Politie & Wetenschap.

Tarling, R. & Morris, K. (2010). Reporting crime to the police. *The British Journal of Criminology, 50*(3), 474–490. https://doi.org/10.1093/bjc/azq011

Terpstra, J., Salet, R., Duijneveldt, I. van & Havinga, T. (2021). *Gebiedsgebonden politiewerk in ontwikkeling: onderzoek naar basisteams in een digitale en superdiverse samenleving*. Politie & Wetenschap.

Thomas, D. & Loader, B. (2000). Cybercrime: law enforcement, security and surveillance in the information age. In D. Thomas & B. Loader (eds.), *Cybercrime: law enforcement, security and surveillance in the information age* (pp. 77–98). Routledge.

Tyler, T.R. & Huo, Y.J. (2002). *Trust in the law: encouraging public cooperation with the police and courts*. Russell Sage.

Van der Plas, T. & Hagenaars, P. (2021). *Operatie Centurion: landelijk actieplan veel voorkomende digitale criminaliteit*. Politie Nederland.

Van de Weijer, S.G.A. & 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.2017.0290

Van de Weijer, S.G.A., Leukfeldt, E.R. & Bernasco, W. (2019). Determinants of reporting cybercrime: a comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology, 16*(4), 486–508. https://doi.org/10.1177/1477370818798343

Van de Weijer, S.G.A., Leukfeldt, E.R. & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal of Police Strategies & Management, 43*(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Van der Wiele, D. (2024). De aanpak van gedigitaliseerde criminaliteit moet beter. CCV. Geraadpleegd op: https://ccv-secondant.nl/platform/article/de-aanpak-van-gedigitaliseerde-criminaliteit-moet-beter

Van Steden, R., Anholt, R. & Boelens, M. (2023). Intake and service staff: practices and challenges of a pivotal yet underexplored police occupation. *Policing: A Journal of Policy and Practice*, paac067. https://doi.org/10.1093/police/pad054

Van Steden, R., Anholt, R. & Koetsier, R. (2021). *De kracht van gebiedsgebonden politiewerk: een internationale literatuurstudie*. Politie Nederland/Vrije Universiteit/NSCR.

Van Wilsem, J. (2013). Hacking and harassment – Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*, 437–453. https://doi.org/10.1177/1043986213482271

Walker, S., Sanci, L. & Temple-Smith, M. (2013). Sexting: young women's and men's views on its nature and origins. *Journal of Adolescent Health, 52*(6), 697–701. https://doi.org/10.1016/j.jadohealth.2012.12.006

Weiss, K.G. (2010). Male sexual victimization: examining men's experiences of rape and sexual assault. *Men and Masculinities, 12*(3), 275–298. https://doi.org/10.1177/1097184X08322632

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

Willekers, M. & Schuppers, K.W. (2022). *Aanpak gedigitaliseerde criminaliteit in de eenheid Den Haag*. Politie, eenheid Den Haag.

Wu, Y. (2014). Race/ethnicity and perceptions of the police: a comparison of White, Black, Asian and Hispanic Americans. *Policing and Society, 24*(2), 135–157. https://doi.org/10.1080/10439463.2013.784288

Yuksel, Y. & Tepe, F. (2013). Citizen satisfaction with police and community policing. *European Scientific Journal, 9*(14), 29–48.

Zuurveen, R. & Stol, W. (2020). *Benutten van digitale sporen*. Politie & Wetenschap.

Bijlage 1 Bijdragen van het onderzoeksteam aan de deelstudies

Dit onderzoek bestaat uit zes deelstudies: literatuuronderzoek (door Daphne Valk-van Waarde en Ronald van Steden), een quickscan (het deelrapport *Online blauw: kwantitatief onderzoek naar digitale criminaliteit op basis van politiedata* door Kristiaan Schuppers, Melissa Willekers en André Merk), locatieonderzoek in de vorm van zes schetsen van basisteams (door Sandra ter Woerds, Ronald van Steden, Kristiaan Schuppers, Melissa Willekers, André Merk en Daphne Valk-van Waarde) en 77 zaakreconstructies (door Sandra ter Woerds, André Merk, Kristiaan Schuppers en Melissa Willekers), een kwantitatieve analyse van de tevredenheid van slachtoffers (aangevers) van digitale criminaliteit over de politie (het deelrapport *Impact van criminaliteit, behoeften van slachtoffers en hun tevredenheid met de politie omtrent het aangifteproces: een grootschalige analyse van aangevers van digitale en traditionele criminaliteit in Nederland* door Roselle Jansen en Stijn Ruiter), en zestien interviews met slachtoffers van digitale criminaliteit die een aangifte of melding hebben gedaan (door Ronald van Steden en Daphne Valk-van Waarde). Ter afronding hebben we een reflectiesessie over de uitkomsten van het onderzoek georganiseerd. In de volgende bijlagen wordt de methodologie van de zes deelstudies afzonderlijk verantwoord.

Bijlage 2 Methode en aanpak literatuurstudie

Het doel van de literatuurstudie was om eerdere publicaties naar digitale criminaliteit in relatie tot de politie en slachtofferschap in kaart te brengen. Deze publicaties dienen als kadering en inspiratie voor ons eigen onderzoeksproject. Het startpunt waren archieven van de afdelingen Analyse & Onderzoek binnen de politie-eenheden Amsterdam en Den Haag met publicaties over de (aanpak van) digitale criminaliteit en documenten die voornamelijk uit 'grijze literatuur' (beleidsstukken, factsheets en handreikingen) bestonden. Vanuit daar hebben we gezocht in databases van onder andere Politie & Wetenschap, het Wetenschappelijk Onderzoek en Documentatiecentrum (WODC) van het Ministerie van Justitie en Veiligheid, en het Centraal Bureau voor de Statistiek (CBS). Voorts hebben we gezocht naar publicaties van ons bekende Nederlandse auteurs (Borwell, Leukfeldt, Spithoven en Stol) over dit thema.

Ter verdieping hebben we via de VU-bibliotheek en Google Scholar gezocht op allerlei zoektermen, waaronder 'digitale criminaliteit/digital crime', 'internetcriminaliteit', 'cybercrime', 'computer-assisted crime', 'computer-related crime', 'e-crime', 'phishing', 'hacken', 'ransomware', 'mallware', 'geldezels/money mules' en verschijningsvormen ('fraude', 'smaad/laster', 'sexting', 'sextortion', enzovoort), in combinatie met 'politie/police', 'community policing' en 'opsporing'. Tot slot hebben we vanuit de Politieacademie tien scripties over bovenstaande onderwerpen ontvangen en daarvan de literatuurlijsten op nog onbekende publicaties gecontroleerd. Dit leverde geen nieuwe informatie meer op. Vervolgens is een nieuwe zoekslag gemaakt naar publicaties over slachtoffers van digitale criminaliteit met termen als '(kenmerken) slachtoffers digitale criminaliteit', 'victimization cybercrime', 'impact digitale criminaliteit/cybercrime', en 'melding/aangifte/crime report digitale criminaliteit/cybercrime'. De verwerking van de literatuurstudie staat met name in hoofdstuk 2.

Bijlage 3 Methode en aanpak quickscan

Afbakening
De quickscan richt zich zowel op digitale delicten die cybercrime betreffen als op delicten die onder de noemer van gedigitaliseerde criminaliteit vallen, waarbij er hiertussen in de analyse geen onderscheid wordt gemaakt. Bij veel verschijningsvormen van digitale criminaliteit is het namelijk lastig een onderscheid te maken tussen cybercrime en gedigitaliseerde criminaliteit. Zoals ook naar voren komt in het literatuuronderzoek ligt onze focus op *digitale aangiftecriminaliteit*: criminaliteit waarvoor burgers bij de politie een aangifte/melding komen doen. Zogeheten 'slachtofferloze delicten' (zoals drugs- en wapenhandel en heling) en 'haalcriminaliteit' (die door eigen inspanning tot de politie komt) vallen daarom af. Dit geldt ook voor zaken in het kader van online aangejaagde ordeverstoringen (online opruiing, desinformatie), tenzij het onderdeel is van de modus operandi bij persoonsgerichte delicten.

Veel aangiftecriminaliteit bevat een of meerdere digitale elementen, of dit nu zit in de voorbereiding, de uitvoering of in het vervolg. Dat vraagt om een nadere afbakening. Daarbij is een belangrijke vraag wat 'digitalisering van criminaliteit' betekent voor de aanpak vanuit de politie, in het bijzonder voor de afhandeling van meldingen/aangiften. De focus in deze analyse ligt op delicten waarbij digitale elementen een rol spelen in de *uitvoering van het delict*, omdat dit onderdeel grofweg de meeste aanknopingspunten geeft voor de opsporing. Daarbij worden categorieën (aangifte)delicten buiten beschouwing gelaten die wel een digitaal element hebben maar waarbij deze digitale component geen onderdeel uitmaakt van de daadwerkelijke uitvoering van het delict. Denk bijvoorbeeld aan een fysiek delict, zoals mishandeling, waarbij voorafgaand contact is geweest tussen een dader en slachtoffer via WhatsApp.

In de uitvoering van delicten bestaat er ook differentiatie in de mate waarin er een digitaal element aanwezig is ten opzichte van fysieke elementen. In de analyse is de nadruk gelegd op delicten met een *'substantiële' digitale component* – dat wil zeggen: de digitale component is een wezenlijk onderdeel van de uitvoering van het delict, er zijn digitale sporen en het plegen van het delict was zonder digitale middelen niet of in veel geringere mate mogelijk geweest. Dit is geen strak afgebakende categorie. Daarom is ook bekeken in hoeverre delicten een 'beperkte' digitale component hebben in de uitvoering ervan. Daarbij gaat het onder meer om stalkingzaken waarin de incidenten (en ook de dreiging) vooral fysiek van aard zijn geweest, maar er een of een paar keer ook via social media contact is gezocht. Deze categorie is relatief klein ten opzichte van de

categorie met een substantiële digitale component en valt verder buiten de scope van het onderzoek. Tot slot vallen ook kinderporno en grooming buiten de scope van het onderzoek. Die zaken landen niet op lokaal niveau, maar bij gespecialiseerde afdelingen.

Aansluitend op het literatuuronderzoek (zie de vorige Bijlage) hebben voorgaande aannames geleid tot de volgende categorieën van digitale criminaliteit:

- *Fraude/oplichting:* financiële oplichting als bankhelpdeskfraude, BEC-fraude, hulpvraagfraude, betaalverzoekfraude, tech support scam, misbruik van accounts voor bestellingen, aan- en verkoopfraude, beleggingsfraude.
- *Persoonsgericht:* delicten die in de persoonsgerichte sfeer worden gepleegd, zoals stalking, bedreiging, smaad/laster/belediging, sexting.
- *Chantage/afpersing*: delicten als ransomware en sextortion.
- *Overig:* onder meer delicten op basis van politieke of ideologische motieven, maar bijvoorbeeld ook delicten die uit verveling of baldadigheid worden gepleegd.

De onderzoeksperiode voor de quickscan is: oktober 2022 tot en met september 2023. Dit was ten tijde van de uitvoering van het onderzoek de meest recente periode.

Query's

Voor de quickscan is eerst gebruikgemaakt van een binnen de politie ontwikkelde overkoepelende query om veelvoorkomende vormen van cybercrime en gedigitaliseerde criminaliteit vanuit politieregistraties inzichtelijk te maken. Een query is een zoekopdracht in een database aan de hand van vooraf opgestelde trefwoorden – ofwel: het is een geautomatiseerde selectieregel. We hebben deze query toegepast binnen de Basisvoorziening Handhaving (BVH), het politiesysteem waarin de aangiften en meldingen worden geregistreerd. In de oriëntatiefase van ons onderzoek bleek echter dat deze overkoepelende query aan de ene kant te veel uitkomsten ('false positives') genereerde, terwijl de query aan de andere kant bepaalde fenomenen – voornamelijk online smaad/laster/belediging en sexting/sextortion – onvoldoende in beeld bracht. Daarom is in tweede instantie gekozen voor een andere opbouw met verschillende query's/zoekslagen die in BVH de meest voorkomende categorieën van digitale criminaliteit inzichtelijk maken. Het betreft de volgende:[31]

1. Online fraude/oplichting;
2. Cybercrime;
3. Online bedreiging/stalking;

31 Om online fraude inzichtelijk te maken is de gelijknamige zoekslag gebruikt. Persoonsgerichte delicten zijn in kaart gebracht met de query's gericht op online bedreiging/stalking, online smaad/laster/belediging en sexting/sextortion (wat betreft sexting). Bij afpersing is ook gebruikgemaakt van de query sexting/sextortion (wat betreft sextortion) en de cybercrime query (wat betreft ransomware). De cybercrime query geeft in de volle breedte informatie over thema's – voor zover er een cybercrimecomponent is – die voor het overgrote deel fraude betreffen, maar het kan ook gaan om persoonsgerichte delicten, afpersing en overige delicten. Grotendeels zijn deze registraties al met de andere query's naar boven gekomen. Dus de cybercrimequery is vooral aanvullend gebruikt.

4. Online smaad/laster/belediging;
5. Sexting/sextortion (zie hieronder voor een nadere beschrijving van de query's).

Bij de totstandkoming van de query's gold als uitgangspunt dat het om delicten moest gaan met een substantieel digitaal element (en met invloed op de opvolging vanuit de politie). Dit uitgangspunt werkt door in de keuze die is gemaakt voor de query's om tot een inschatting te komen van de omvang van digitale criminaliteit. Er moest steeds een balans worden gezocht tussen het aandeel 'false positives' (registraties van criminaliteit die geen of een heel beperkt digitale component hebben en die buiten de scope van het onderzoek vallen) enerzijds en het aandeel 'false negatives' (registraties die digitale criminaliteit betreffen, maar die niet meekomen in de output) anderzijds.

Op basis van bovenstaande query's hebben we voor de onderzoeksperiode oktober 2022 tot en met september 2023 een bestand met potentiële digitale criminaliteit samengesteld. Hierbij ontstond er overlap tussen de uitkomsten van de verschillende query's. Daarom zijn bij het samenvoegen van de data zaken ontdubbeld op basis van registratienummers. Dit heeft een bestand opgeleverd van 198.476 unieke registraties van potentiële digitale criminaliteit. Het gaat zowel om aangiften als meldingen – dit laatste wil zeggen: registraties in BHV waarbij het slachtoffer (nog) geen aangifte heeft gedaan.

Daarna hebben we een aselecte steekproef getrokken en dossieronderzoek verricht om vast te stellen of er daadwerkelijk sprake is van digitale componenten in de uitvoering van het delict, hoe groot deze rol is (substantieel of beperkt), en onder welke hoofdcategorieën (waaronder fraude en persoonsgerichte delicten) en subcategorieën het delict valt. In totaal zijn er 600 registraties beoordeeld en geannoteerd.[32] Hiermee kan een betrouwbare afspiegeling van de gehele dataset van 198.476 registraties worden gegeven. De 600 geannoteerde registraties zijn random verdeeld over drie codeurs (zie hieronder meer informatie over het gebruikte codeboek). Voorafgaand hieraan hebben deze codeurs twintig dezelfde registraties afzonderlijk bekeken in het kader van kruisvalidatie. Er is op basis hiervan vastgesteld in welke mate de registraties hetzelfde werden geannoteerd. Waar er verschillen waren, zijn de annotatieafspraken nader besproken en aangescherpt.

Na het annoteren van alle 600 registraties is een vergelijking gemaakt tussen de uitkomsten van de verschillende codeurs. Waar er opvallende verschillen waren, hebben de codeurs ingezoomd op hoe die verschillen zijn ontstaan. In sommige gevallen heeft dit tot bijstellingen geleid. Discussies gingen vooral over de mate waarin delicten als 'digitaal' moeten worden beschouwd. Zie in Box 1 en 2 voorbeelden om een en ander

32 Met een betrouwbaarheid van 95%, een foutmarge van 5% en de verwachting dat 50% van de registraties digitale criminaliteit betreft, is de minimale steekproefomvang bij een populatie van ongeveer 200.000 een kleine 400 registraties. Er is gekozen voor een grotere steekproefomvang om de betrouwbaarheid te verhogen en om betere uitspraken te kunnen doen over de inhoud van delictscategorieën.

te verduidelijken omtrent het onderscheid tussen 'substantieel' en 'beperkt' wat betreft de digitale component van een delict. Uit de data komt naar voren dat het bij registraties met een beperkte digitale component relatief vaak gaat om persoonsgerichte delicten (46%). In dit geval heeft het delict een digitaal element, maar de fysieke bestandsdelen zijn groter/en of hebben meer gewicht ('false positives'). We hebben geprobeerd dit soort registraties zo veel mogelijk uit te filteren.

Tot slot zijn we in het dossieronderzoek nagegaan waar zaken zijn binnengekomen en afgehandeld door de politie, en in welke mate de basisteams hierin een rol spelen. Om inzichtelijk te krijgen welke vervolgstappen er zijn geweest vanuit de opsporing, hebben we aan de registraties binnen de steekproef informatie gekoppeld uit het systeem Betere Opsporing door Sturing op Zaken (BOSZ). Daarbij moet rekening worden gehouden met het feit dat een deel van de BVH-registraties niet in BOSZ komt. De registraties die zijn gebleven bij meldingen (en niet hebben geresulteerd in aangiften) worden voor een groot deel niet in BOSZ geregistreerd, omdat er sowieso geen strafrechtelijk onderzoek volgt.[33] We richten ons in de beschrijving van de afhandeling van digitale criminaliteit door de politie dus met name op wat er met aangiften van slachtoffers is gebeurd.

Box 1: Persoonsgericht delict (smaad/laster) met substantiële digitale component
'… X heeft een order bij meldster geplaatst, welke niet in een keer geleverd kon worden. Meldster heeft met haar een afspraak gemaakt voor een deel levering, waar X mee akkoord ging. Vervolgens zag meldster op 12 augustus 2023 dat er een bericht gepost was in een Facebook-groep genaamd [geanonimiseerd]. Dit bericht werd gepost door X, ook is zij de aanjager van de groep. In het bericht wordt het online bedrijf betiteld als Oplichter en zou het de leveringsvoorwaarden niet nakomen. Verder worden er berichten gedeeld van de privé adresgegevens van meldster en wordt er opgeroepen om zoveel als mogelijk berichten achter te laten in de Facebook-groep…'

Box 2: Persoonsgericht delict (bedreiging/stalking) met beperkte digitale component
'... Melder wil een afspraak om in een mutatie vast te laten leggen dat zij wordt lastiggevallen door een persoon die haar zwartmaakt, omdat haar ex-partner een aantal jaren geleden is veroordeeld voor doodslag. Melder legt uit dat dit niet openbaar gebeurt, maar direct naar haar: telefonisch en per sms... Meldster is afgelopen week twee keer via app benaderd door X. Soort "dreigementen": ... je moet oppassen...'

Toelichting: De melder wordt vooral telefonisch lastiggevallen. Een beperkt deel vindt online plaats (twee keer 'dreigementen' via WhatsApp).

33 Uitgezonderd de registraties die in BVH zijn opgemaakt in categorieën die betrekking hebben op misdrijven.

Codeboek dossieronderzoek

1. Betreft het digitale criminaliteit?

Antwoordcategorie	Toelichting
Ja	De digitale component is een wezenlijk onderdeel van de uitvoering van het delict. Zonder digitale middelen was het plegen van het delict niet of in veel geringere mate mogelijk geweest. Ook zijn er digitale sporen aanwezig.
Nee	Het betreft een vorm van traditionele criminaliteit die in de meeste gevallen in de fysieke ruimte plaatsvindt. In de registratie kan sprake zijn van digitale middelen, maar in de uitvoering van het delict zijn geen digitale bestanddelen aanwezig. Voorbeeld: online is een video gedeeld waarin gevaarlijk rijgedrag wordt getoond. Hoewel wel sprake is van een digitale component, maakt deze geen onderdeel uit van de uitvoering van het delict. Het gaat hier om een verkeersmisdrijf en niet om een vorm van digitale criminaliteit.
Beperkt	De digitale component is aanwezig maar deze is relatief beperkt ten opzichte van de fysieke bestanddelen. Voorbeeld: slachtoffer wordt lastiggevallen door een persoon die vooral fysiek bij haar aan de deur komt en haar opbelt. Echter wordt er ook twee keer een bericht via WhatsApp gestuurd met waarschuwingen niet zijnde strafbare bedreigingen.
Onbekend	De informatie in de registratie is te summier om deze te kunnen duiden.

2. Heeft de zaak een hybride karakter?

Antwoordcategorie	Toelichting
Ja	Het delict heeft een substantiële digitale component, maar vindt ook fysiek plaats. Voorbeeld: de verdachte valt het slachtoffer lastig op haar werk, maar zij ontvangt ook regelmatig vervelende WhatsApp-berichtjes. De stalking vindt dus zowel fysiek als digitaal plaats.
Nee	Het delict vindt alleen in de digitale of alleen in de fysieke ruimte plaats.

3. Gaat het om een melding of een aangifte?

Antwoordcategorie	Toelichting
Melding	
Aangifte	

4. Binnen welke hoofdcategorie valt het delict?

Antwoordcategorie	Toelichting
Fraude	Het motief van het delict betreft financiële oplichting.
Persoonsgericht	Het delict is erop gericht het slachtoffer te schaden.
Afpersing/Chantage	Het slachtoffer wordt onder bedreiging (van geweld) gedwongen iets te doen of te laten (bijvoorbeeld het betalen van een som geld of het afgeven van naaktfoto's).
Overig	Het delict valt niet te classificeren onder een van de voornoemde categorieën.

Query's en zoekslagen
Voor **online fraude/oplichting** is uitgegaan van maatschappelijke klassen (categorieën) in BVH. Alle registraties in BVH worden (door de verbalisanten) getypeerd/geclassificeerd aan de hand van een systeem van maatschappelijke klassen (MK's). Uit eerder onderzoek in de Eenheid Den Haag is gebleken dat de maatschappelijke klassen voor horizontale fraude in de BVH voor een groot deel online fraude betreffen (Schuppers et al., 2022). Dit geldt vooral voor de vier meest voorkomende maatschappelijke klassen horizontale fraude:

- F620 OVERIGE HORIZONTALE FRAUDE
- F636 FRAUDE MET ONLINE HANDEL
- F614 FRAUDE MET BETAALPRODUCTEN
- F617 IDENTITEITSFRAUDE

Deze maatschappelijke klassen hadden in 2020 een aandeel van 98% binnen de gehele categorie horizontale fraude. Uit ander onderzoek kwam al naar voren dat ruim 90% van de delicten kan worden getypeerd als 'online fraude', waarbij het voornamelijk gaat om 'aan- en verkoopfraude', 'hulpvraagfraude' en 'online fraude met bankgegevens/internetbankieren' (Hesseling et al., 2021).

Als iets breder wordt gekeken, kunnen ook de maatklassen F638 TELECOMFRAUDE, F639 BELEGGINGSFRAUDE, F633 VASTGOEDFRAUDE, F637 VOORSCHOTFRAUDE en F94 WITWASSEN worden meegenomen, omdat er bij deze – veel minder voorkomende MK's – ook weleens sprake wil zijn van een online fraudecomponent. Tevens zijn de nieuwe (in mei 2023) ingevoerde maatschappelijke klassen inzake online fraude meegenomen: F651 TELEFONISCHE HELPDESKFRAUDE, F652 ONLINE IDENTITEITSFRAUDE en F650 HULPVRAAGFRAUDE.

Er is ook nog een deel van online fraude dat weg wordt geschreven onder F90 CYBERCRIME indien een delict een cybercrime-element heeft (denk bijvoorbeeld aan bankhelpdeskfraude waarbij er sprake is van computervredebreuk). Deze registraties komen terug in onze zoekslag gericht op cybercrime in enge zin (zie hieronder). Uit eerdere analyses is naar voren gekomen dat online fraude vrijwel altijd onder de fraudemaatklassen of F90 CYBERCRIME wordt weggeschreven. Als deze bronnen worden samengenomen, ontstaat er een bijna volledig beeld met betrekking tot online fraude. Soms is het ook mogelijk dat het blijft bij een melding/mutatie in algemene categorieën, zoals E40 AFHANDELING OVERIGE MELDINGEN, J30 ALGEMENE MUTATIE en J12 VERDACHTE SITUATIE. De inschatting is dat dit aandeel niet hoger is dan 5% (gebaseerd op bevindingen aan de hand van de landelijke cybercrime query; zie hieronder).

Cybercrime kan in beeld worden gebracht op basis van de Landelijke Cybercrimequery (LCQ). In deze query zijn zoektermen opgenomen die voornamelijk verband houden met cybercrime (in enge zin), waarbij het onder meer gaat om bestanddelen die

betrekking hebben op hacken/computervredebreuk, phishing, DDOS en ransomware. Daarbij zijn de zoektermen zodanig opgesteld dat er ook gedigitaliseerde criminaliteit meekomt, omdat de scheidslijn tussen cybercrime en gedigitaliseerde criminaliteit in registraties vaak dun is. Binnen de meeste politie-eenheden zijn cybercrime-registraties – door medewerkers cyberintelligence – veredeld in BlueIntel.[34] Hierbij beoordelen medewerkers of er sprake is van cybercrime, gedigitaliseerde criminaliteit of geen digitale criminaliteit. Het algemene beeld is dat een kleine 20% helemaal geen digitale criminaliteit betreft ('false positives' vanuit ons perspectief). In de uitkomsten van de LCQ is een grote overlap zichtbaar met het aantal registraties met betrekking tot fraudemaatklassen. Op basis van de gescoorde registraties voortvloeiend uit de LCQ blijkt dat 85% van alle registraties cybercrime en gedigitaliseerde criminaliteit fraude en oplichting betreft. Verder gaan deze registraties over persoonsgerichte delicten (bedreiging/stalking/smaad/laster) en over delicten in het kader van afpersing (voornamelijk sextortion). Aangiften/meldingen van ransomware en DDOS zijn er maar in beperkte mate.

Online bedreiging/stalking. Vanuit de query die door het WODC is gebruikt, is een aantal zoektermen gericht op enerzijds bedreiging/stalking en anderzijds de online-elementen. Deze zoektermen zijn geactualiseerd/opgeschoond. Een eerste test leverde zoveel uitkomsten met 'false positives' op dat ervoor is gekozen om een woordafstand te gebruiken tussen termen omtrent 'bedreiging/stalking' enerzijds en termen omtrent 'online-elementen' anderzijds. Hierbij is geaccepteerd dat er ook een beperkt deel 'false negatives' is: registraties die wel als online bedreiging/stalking kunnen worden beschouwd, maar die niet worden opgehaald door de query. Daarbij weegt mee dat er een differentiatie bestaat in de mate waarin het online-element een rol heeft gespeeld in de uitvoering van het delict. Bij de registraties die worden 'gemist' gaat het meestal om gevallen waarin een delict ook een fysieke component heeft. Verder is er een aanscherping van de query geweest met betrekking tot in welke formulieren er is gezocht. De verdachtenverhoren zijn buiten beschouwing gelaten, omdat er – ongeacht of het een online dan wel fysiek delict betreft – regelmatig aan verdachten wordt gevraagd of ze gebruikmaken van sociale media – en zo ja welke. Dat leverde vooral 'false positives' op.

Online smaad/laster/belediging. Er waren nog geen zoektermen opgenomen ten aanzien van dit fenomeen. Daarom hebben we gezocht naar smaad, laster en belediging, gecombineerd met online-elementen. Ook hier zijn de verklaringen uit verdachtenverhoren buiten beschouwing gelaten. Deze zoekslag leverde veel bruikbare uitkomsten op over zaken waarin aangifte is gedaan (dan wordt letterlijk gesproken over smaad/laster en belediging). In gevallen waarin het bleef bij een (vagere) melding is dat niet

34 BlueIntel is een applicatie waarmee aan geselecteerde BVH-registraties gestructureerde informatie kan worden toegevoegd. Dit betreft onder andere informatie over soort delict, leeftijd slachtoffer, bedrijf, gemelde schade en opsporingsindicaties (zoals telefoonnummers en bankrekeningnummers en social media-accounts).

altijd het geval. Daarom is ook breder gezocht op termen die verwijzen naar cyberpesten, vernederingvideo's, enzovoort.

Sexting/Sextortion. Hierbij is gebruikgemaakt van een query die door de Eenheid Amsterdam is ontwikkeld ten behoeve van een werkgroep waarbij verschillende politiedisciplines alsook externe partijen, zoals hulporganisaties (Helpwanted/Qpido) en KPN, aansloten. Wederom zijn verklaringen uit verhoren van verdachten buiten beschouwing gelaten.

Uitkomsten per query
In onderstaande Tabellen 1 tot en met 4 staan de uitkomsten per query weergegeven.

Tabel 1 Mate waarin registraties digitale criminaliteit betreffen per query (N=600)

Digitaal	Ja		Beperkt		Nee		Onbekend		Buiten scope		Eindtotaal	
Query	aantal	%	aantal	%	aantal	%	aantal	%	aantal	%	aantal	%
Fraude	263	83%	34	11%	18	6%	3	1%	0	0%	318	100%
Cybercrime (LCQ)	92	84%	7	6%	11	10%	0	0%	0	0%	110	100%
Bedreiging/stalking	62	42%	29	20%	50	34%	5	3%	0	0%	146	100%
Cyberpesten	29	37%	7	9%	37	47%	2	3%	4	5%	79	100%
Sextortion/sexting	25	36%	3	4%	37	53%	0	0%	5	7%	70	100%
Smaad/laster	20	53%	5	13%	10	26%	1	3%	2	5%	38	100%
Noot: er zit overlap tussen de query's, waardoor de optelling van de eindtotalen per query hoger uitkomt dan 600. De overlap zit tussen query's gericht op persoonsgerichte delicten (bedreiging/stalking, cyberpesten, smaad/laster en sextortion/sexting) enerzijds en tussen Fraude en Cybercrime (LCQ) anderzijds.												

Tabel 2 Mate waarin registraties digitale criminaliteit betreffen per categorie query's (N=600)

Digitaal	Ja		Beperkt		Nee		Onbekend		Buiten scope		Eindtotaal	
Query	aantal	%	aantal	%	aantal	%	aantal	%	aantal	%	aantal	%
Persoonsgericht inclusief sextortion/sexting	96	35%	33	12%	125	46%	6	2%	11	4%	271	100%
Fraude/Cybercrime (LCQ)	281	81%	35	10%	29	8%	3	1%	0	0%	348	100%
Noot: in lijn met bovenstaande zijn de query's geclusterd. Er bestaat tussen de categorieën 'persoonsgericht inclusief sextortion/sexting' en 'fraude/Cybercrime (LCQ)' een kleine overlap, waardoor de optelling van de eindtotalen ook hier hoger uitkomt dan 600. De overlap is hier wel een stuk kleiner dan in Tabel 1.												

Tabel 3: Mate waarin registraties digitale criminaliteit betreffen bij persoonsgerichte query's (en sextortion/sexting), inclusief ophoging (N=371)

Digitaal	Ja		Beperkt		Nee		Onbekend		Buiten scope		Eindtotaal	
Query	aantal	%	aantal	%	aantal	%	aantal	%	aantal	%	aantal	%
Bedreiging/stalking	93	46%	36	18%	68	34%	5	2%	0	0%	202	100%
Cyberpesten	35	34%	9	9%	54	52%	2	2%	4	4%	104	100%
Sextortion/stalking	33	35%	5	5%	50	53%	0	0%	6	6%	94	100%
Smaad/laster	24	51%	5	11%	14	30%	2	4%	2	4%	47	100%
Noot: er zijn honderd registraties toegevoegd aan de steekproef vanuit de persoonsgerichte query's (inclusief sextortion/sexting). De N is daarmee gestegen van 271 naar 371.												

Tabel 4: Mate waarin registraties digitale criminaliteit betreffen bij categorie persoonsgerichte query's (plus sextortion/sexting), inclusief ophoging (N=371)

Digitaal	Ja		Beperkt		Nee		Onbekend		Buiten scope		Eindtotaal	
Query	aantal	%	aantal	%	aantal	%	aantal	%	aantal	%	aantal	%
Persoonsgericht inclusief sextortion/sexting	136	37%	43	12%	173	47%	7	2%	12	3%	371	100%

Bijlage 4 Methode en aanpak locatieonderzoek

Om vast te stellen hoe basisteams in de praktijk omgaan met de instroom van meldingen en aangiften van digitale criminaliteit, hebben we locatieonderzoek uitgevoerd. Dit locatieonderzoek bestaat uit zes schetsen van basisteams en 77 zaakreconstructies (zie ook Bijlage 5). De cases zijn geselecteerd via ons eigen netwerk van programmamanagers, projectadviseurs en proceseigenaren en andere medewerkers die zich binnen de politie bezighouden met de digitale transformatie en de aanpak van digitale criminaliteit. Hierbij is gelet op enige spreiding door het land en op de grootte van gemeenten waarbinnen de basisteams functioneren. Naast drie grote steden binnen de Randstad, heeft het locatieonderzoek ook in een stad buiten de Randstad en in twee kleinere gemeenten plaatsgevonden.

De zes schetsen geven geen volledig representatief beeld van hoe basisteams met digitale criminaliteit omgaan, maar bevatten beschrijvingen die een goede indruk van verschillende praktijken geven. Het gaat om zes geanonimiseerde locaties: het Team Noord, Team Oost, Team Midden, Team Stad, Team Strand en Team Zee. Om een indruk van deze teams te krijgen hebben we steeds een dag meegelopen en politiefunctionarissen (op verschillende andere dagen) persoonlijk of telefonisch gesproken. In totaal hebben we interviews gehouden met 54 respondenten. Deze interviews duurden tussen een halfuur en een uur. Soms waren er twee respondenten bij een interview aanwezig. Hieronder staan de geïnterviewde respondenten per basisteam toegelicht.

Respondenten
Op het Team Noord ging het om acht respondenten: de teamchef, een leidinggevende belast met de Digitale Transformatie, vier I&S-medewerkers (leidinggevenden en uitvoerenden), een VVC-medewerker en een digitaal wijkagent.

Op het Team Oost hebben we elf respondenten geïnterviewd: twee vertegenwoordigers van de teamleiding, twee leidinggevenden verantwoordelijk voor Dienstverlening, een kwaliteits-HOvJ, twee I&S-medewerkers, een wijkagent/casescreener, een portefeuillehouder en een aanjager Digitale Transformatie en een coördinator van de basisteamrecherche.

Op het Team Midden hebben we met negen respondenten gesproken: de plaatsvervangend teamchef, de portefeuillehouder Gedigitaliseerde criminaliteit en cybercrime, een leidinggevende en een medewerker van I&S, een kwaliteits-HovJ, een wijkagent, en

drie medewerkers van de recherche (twee van de VVC/basisteamrecherche en een van de DR).

Op het Team Stad zijn er gesprekken met tien respondenten gevoerd: de teamchef, twee leidinggevenden belast met de Digitale Transformatie, twee medewerkers van de VVC, waaronder een specialist cybercrime/gedigitaliseerde criminaliteit, de coördinator van I&S, een digitaal wijkagent, een analist/intelligence-medewerker en twee taakaccenthouders Digitale criminaliteit.

Op het Team Strand ging het om tien respondenten: de teamchef, een leidinggevende GGP en een leidinggevende I&S, een jeugdagent, een medewerker wijkzorg, een senior verantwoordelijk voor de VVC en vier medewerkers van de DR.

Tot slot hebben we op het Team Zee vijf respondenten geïnterviewd: de teamchef, een leidinggevende en een medewerker van I&S, twee VVC-medewerkers, waaronder een casescreener/coördinator en een wijkagent.

Format interviews
Tijdens de interviews met respondenten zijn we op de volgende onderwerpen ingegaan:

Aard en omvang van het digitale werkaanbod op het basisteam
1. Cybercrime versus gedigitaliseerde criminaliteit (link met kwantitatieve analyse leggen!)
2. Zicht op digitaal slachtoffer- en daderschap in de wijk
3. Impact van digitale criminaliteit op politiewerk en op maatschappij/ burgers (is het HIC?)
4. Wat voor zaken komen er (voornamelijk) voorbij?
5. Hybride/combi fysiek-digitaal: wanneer is het 'digitaal' (substantieel digitaal/ dat het specifieke digitale kennis en inzet nodig heeft)?

Werkstromen aanvoerroutes digitale criminaliteit
1. Aangiften/meldingen (fysiek, telefoon, internet, LMIO (via BOSZ), buitenland, partner/ externe instanties, van buiten de regio)
2. Project Centurion
3. RSC
4. Signalen van de werkvloer, wat zien en horen BT-medewerkers buiten meldingen en aangiften?
5. Andere…

Wie doet wat aan zaken/ politiewerk met een digitale component?
1. Welke functies/rollen/afdelingen/teams?
2. Specifieke taakaccenten/collega's met specifieke expertise
3. Wat doet noodhulp/opsporing/wijkagenten/intelligence?
4. Welke rol speelt preventie?

Sturing op online werk/zaken
1. Vanuit de teamleiding/teamchef
2. Beleidsplannen, streefcijfers, prioriteitstelling
3. Rol van digitale transformatie/transitie

Kennis en kunde bij medewerkers m.b.t. digitale zaken
1. Kennisniveau: goed/gemiddeld/slecht (en waarom)?
2. Welke hulplijnen zijn er? (personen/specialisten, protocollen, digitale fora/websites)
3. Wat mist er, wat is er nodig?

Partners: met wie wordt samengewerkt? Bijvoorbeeld:
1. Ondernemers
2. Banken
3. Verzekeraars
4. Hulpverleners

Initiatieven en innovatie: wat is er in ontwikkeling? Bijvoorbeeld:
1. Digitale Meldkamer
2. Digihub
3. Andere initiatieven/projecten

Tot slot, wat vindt men van:
1. Prioriteit voor digitale criminaliteit op het team?
2. Wat gaat goed?
3. Wat kan beter?
4. Welke problemen en barrières komt men in de afhandeling tegen?

Bijlage 5 Methode en aanpak zaakreconstructies

Om te laten zien hoe digitale zaken die op een basisteam spelen in de praktijk verlopen, hebben we zaakreconstructies gemaakt. De selectie van zaken is gemaakt door van ieder deelnemend basisteam (N=6) zaken te selecteren. De selectie van zaken vond als volgt plaats. Eerst hebben we de teams gevraagd om drie zaken aan te leveren die speelden in het aan ons onderzoek voorafgaande jaar, te weten: een zaak waar men 'trots' op is wat betreft aanpak en verloop, een zaak die 'leerpunten' bevat en een via LMIO gerouteerde zaak die afgehandeld werd op het team. In totaal leverde deze exercitie drie zaken op per basisteam, met een totaal van achttien.

Vervolgens hebben we zelf per deelnemend basisteam een steekproef van tien zaken getrokken uit de landelijke dataset die aan de basis ligt van de quickscan. Deze quicscan bevat digitale zaken uit het jaar 2022-2023. Het gaat hier om politiedata uit het registratiesysteem BVH dat de beperking kent dat uitsluitend datgene wat is gemuteerd is kan worden meegenomen in de analyse. Daarbij komt dat sommige zaken dermate omvangrijk waren (bijvoorbeeld zaken met negentig incidenten en diverse teams met eigen registraties hiervan) dat die zaken in BVH op hoofdlijnen zijn gerapporteerd. Dit soort zaken hebben we niet meegenomen. Ook 'summit registraties' (artikel 9) zijn niet meegenomen in de analyse, evenmin als OM-data over strafrechtelijke afdoeningen. Ervaring leert echter: van de meeste zaken is wel relevante info in BVH te vinden. Daarna verliep de selectie in vier stappen:

1. Vanuit het databestand zijn per deelnemend basisteam at random vijftig zaken getrokken (aselecte steekproef).
2. Deze vijftig zaken heeft een onderzoeker gelezen en gescoord op 'digitaal ja/nee'. Daarna hebben we een interbeoordelaars-check uitgevoerd. In lijn met de bevindingen uit de quickscan bleek dat rond de 56% zaken in de steekproef een 'digitale zaak' betrof.
3. Per basisteam hebben we er tien zaken (zestig in totaal) geselecteerd die representatief worden geacht voor het werkaanbod, waarbij is gelet op de verdeling naar delict en op de verdeling over typen delicten.
4. Iedere zaak is voorzien van een code en een voor zover mogelijk passende titel die verwijst naar de aard van het delict.

Een zaak viel tijdens het reconstructieproces af, omdat deze dubbel bleek te zijn. In totaal komen we dus op 77 zaken verspreid over de zes basisteams.

Overzicht van zaken

Alle 77 zaken zijn voorzien van unieke en geanonimiseerde zaakcodes, die hieronder staan vermeld. In hoofdstuk 7 wordt naar deze codes verwezen.

Zaakcode	Naam	Hoofddelict	Subdelict
MIDDEN12	Financiële sextortion	Chantage/afpersing	Sextortion
MIDDEN15	Vuurwapen in whatsapp	Persoonsgericht	Bedreiging/stalking
MIDDEN16	Discriminatie tijdens feest Sint	Persoonsgericht	Smaad/laster/belediging
MIDDEN20	Facebook-account gehackt: makkelijk geld verdienen	Fraude/oplichting	Overige fraude
MIDDEN23	ID-fraude bestelling	Fraude/oplichting	Misbruik accounts voor bestellingen
MIDDEN24	Bedreiging na marktplaats-verkoop	Persoonsgericht	Bedreiging
MIDDEN27	Aankoopfraude	Fraude/oplichting	Aan-en verkoopfraude
MIDDEN5	Boilerroomfraude	Fraude/oplichting	Beleggingsfraude
MIDDEN6	Bankhelpdeskfraude na mail creditcard	Fraude/oplichting	Overige fraude
MIDDEN7	Bankhelpdeskfraude aankopen elektronica	Fraude/oplichting	Bankhelpdeskfraude
MIDDENlmio1	Sextortion na scheiding	Chantage/afpersing	Sextortion
MIDDENlmio2	LMIO-zaak minderjarige verdachte	Fraude/oplichting	Aan-en verkoopfraude
MIDDENtrots/lmio	Webwinkel: verdachte of money mule	Fraude/oplichting	Aan-en verkoopfraude
OOST14	Frauduleuze beleggingsad-vertentie	Fraude/oplichting	Beleggingsfraude
OOST16	Datingfraude	Fraude/oplichting	Overige fraude
OOST22	Poging vriend in nood fraude	Fraude/oplichting	Hulpvraagfraude
OOST36	Onterechte aanmaningen	Fraude/oplichting	Misbruik accounts voor bestellingen
OOST38	Langdurige stalking	Persoonsgericht	Bedreiging/stalking
OOST42	Phishingmail creditcardfir-ma	Fraude/oplichting	Creditcardfraude
OOST48	Beledigend TikTok-filmpje	Persoonsgericht	Smaad/laster/belediging
OOST5	Beschuldigingen op Facebook	Persoonsgericht	Smaad/laster/belediging
OOST6	Afpersing door ex	Persoonsgericht	Overige afpersing
OOST8	Pakketjesfraude	Fraude/oplichting	Aan-en verkoopfraude
OOSTleerpunt	Sextortion van minderjari-gen	Chantage/afpersing	Sextortion
OOSTlmio	Overlastgevend adres, ook voor online fraude	Fraude/oplichting	Aan-en verkoopfraude

OOSTtrots	Bankhelpdeskfraude: meer dan de pinpas	Fraude/oplichting	Bankhelpdeskfraude
STAD13	Beleggen in crypto na Tindercontact gaat fout	Fraude/oplichting	Beleggingsfraude
STAD15	Digitale bedreigingen uit buitenland	Persoonsgericht	Bedreiging/stalking
STAD17	Je baas vraagt je geld over te maken	Fraude/oplichting	CEO-fraude
STAD2	Opgelicht door mijn 'zoon'	Fraude/oplichting	Vriend in Nood-fraude
STAD20	Bedreigd met de dood via TikTok	Persoonsgericht	Bedreiging
STAD24	Bankhelpdeskfraude wordt cybercrime	Fraude/oplichting	Bankhelpdeskfraude
STAD27	Identiteitsfraude advocatenkantoor	Fraude/oplichting	Misbruik accounts voor bestellingen
STAD31	Stalking via Facebook	Persoonsgericht	Bedreiging/stalking
STAD40	Hacken wallet en crypto stelen	Fraude/oplichting	Overige fraude
STAD6	Aanmaningen en vage whatsapps n.a.v. ID-fraude	Fraude/oplichting	Misbruik accounts voor bestellingen
STADleerpunt	De testosteronhandelaar	Fraude/oplichting	Aan-en verkoopfraude
STADlmio	Stapelen LMIO-zaken	Fraude/oplichting	Aan-en verkoopfraude
STADtrots	Heterdaadje bankhelpdesk-fraude	Fraude/oplichting	Aan-en verkoopfraude
NOORD19	Leeghalen bouwdepot	Fraude/oplichting	Overige fraude
NOORD20	Victim blaming sextortion	Chantage/afpersing	Sextortion
NOORD21	Drie keer aan-en verkoop	Fraude/oplichting	Aan-en verkoopfraude
NOORD29	Bankhelpdeskfraude met anydesk bij ouderen	Fraude/oplichting	Bankhelpdeskfraude
NOORD31	Slachtoffer wordt dader	Chantage/afpersing	Sextortion
NOORD38	Geld van bankrekeningen: geen idee	Fraude/oplichting	Overige fraude
NOORD40	Misbruik ID voor bestellingen	Fraude/oplichting	Misbruik accounts voor bestellingen
NOORD42	Poging CEO-fraude stichting	Fraude/oplichting	CEO-fraude
NOORD44	Sexting bij begeleid wonen	Persoonsgericht	Sexting
NOORD7	Hybride stalking	Persoonsgericht	Stalking
NOORDfleerpunt	Bankhelpdeskfraude heterdaad	Fraude/oplichting	Bankhelpdeskfraude
NOORDlmio	Meerdere geldezels, één verdachte	Fraude/oplichting	Aan-en verkoopfraude
NOORDtrots	Gestapelde aangiften	Fraude/oplichting	Bankhelpdeskfraude
STRAND10	Phishing via werkmail	Overige	Overige: cybercrime
STRAND12	Beleggingsfaude met bitcoins is civiele zaak?	Fraude/oplichting	Beleggingsfraude

STRAND2	Aanmaningen voor dingen die je niet besteld hebt	Fraude/oplichting	Misbruik accounts voor bestellingen
STRAND31	ID-fraude bestellingen retour	Fraude/oplichting	Misbruik accounts voor bestellingen
STRAND34	Vissen naar creditcard gegevens	Fraude/oplichting	Bankphishing
STRAND39	Sextortion op herhaling	Chantage/afpersing	Sextortion
STRAND4	Poging helpdeskfraude	Fraude/oplichting	Helpdeskfraude
STRAND45	VIN-fraude oudere dame	Fraude/oplichting	Hulpvraagfraude
STRAND47	Geskimd in het buitenland	Fraude/oplichting	Creditcardfraude
STRAND48	Internationale laster	Persoonsgericht	Smaad/laster/belediging
STRANDleerpunt	Nassau	Fraude/oplichting	Bankhelpdeskfraude
STRANDtrots	Bankhelpdeskfraude oude dame 8 verdachten	Fraude/oplichting	Bankhelpdeskfraude
ZEE15	Stalking door ex	Persoonsgericht	Bedreiging/stalking
ZEE18	Beleggingen in Bitcoins	Fraude/oplichting	Beleggingsfraude
ZEE20	Poging hulpvraagfraude	Fraude/oplichting	Hulpvraagfraude
ZEE23	Bedreigingen via Snapchat	Persoonsgericht	Bedreiging/stalking
ZEE27	Douchevideo	Persoonsgericht	Sexting
ZEE41	AH-app gehackt	Fraude/oplichting	Overige fraude
ZEE43	Boilerroomfraude	Fraude/oplichting	Beleggingsfraude
ZEE46	Nepproduct	Fraude/oplichting	Aan-en verkoopfraude
ZEE48	ID-fraude bij webshopaankopen	Fraude/oplichting	Misbruik accounts voor bestellingen
ZEE8	Bedreigend YouTube-filmpje	Persoonsgericht	Bedreiging/stalking
ZEElmio	Cluster van hulpvraagfraudezaken	Fraude/oplichting	Hulpvraagfraude
ZEElmio/trots	LMIO-cluster van verkoopfraude	Fraude/oplichting	Aan-en verkoopfraude
ZEEmoeizaam	Jongeren lenen elkaars bankrekening	Fraude/oplichting	Aan-en verkoopfraude

Kenschets van de digitale zaken

Zoals uit bovenstaand overzicht blijkt, zijn de 77 onderzochte digitale zaken onder te verdelen naar drie typen: fraude/oplichting, persoonsgerichte delicten en chantage/afpersing (Tabel 1). De fraude/oplichtingszaken betreffen vooral aan-en verkoopfraude (N=13). Daarnaast gaat het over misbruik van accounts voor bestellingen (N=8), bankhelpdeskfraude (N=8), beleggingsfraude (N=6) en hulpvraagfraude (of hulpvraagfraude) (N=5). Ook betreft dit soort zaken CEO- en creditcardfraude, diefstal van cryptomunten, bankphishing en helpdeskfraude. Naast smaad/laster/belediging gaan persoonsgerichte zaken vooral over bedreiging/stalking (N=10). Onder de categorie 'afpersing' gaan alle zes zaken over sextortion. De categorie 'overig' (N=1) gaat om een cybercrimezaak waarbij een e-mailaccount gehackt werd. Van de gereconstrueerde zaken kwamen 49 (63%) binnen via een basisteam, 16 (20%) via een Regionaal

Servicecentrum en 7 (9%) via het OIV-LE: de Operationele Informatieverwerking van de Landelijke Eenheid (LMIO). Rond 45% van de meldingen/aangiften werd aan het bureau opgenomen, 27% via een internetaangifte en 19% telefonisch.

Tabel 1 Zaakreconstructies naar type delict

Fraude/oplichting	(53) 69%
Persoonsgericht	(17) 22%
Afpersing/chantage	(6) 8%
Overig	(1) 1%
Eindtotaal	**(77) 100%**

Van de geanalyseerde online fraude-/oplichtingszaken is bijna in alle gevallen aangifte gedaan (96%). Bij de persoonsgerichte delicten is dit veel minder het geval (35%). Bij zaken die om chantage/afpersing gaan werd in de helft van de gevallen aangifte gedaan. De digitale middelen die gebruikt werden in de zaken betreffen vooral e-mail en sociale media (WhatsApp, Marktplaats, Snapchat, TikTok, Instagram, Facebook, Telegram). Andere digitale middelen zijn al dan niet valse internetpagina's van datingsites en webshops.

Delicten hebben regelmatig een hybride karakter: behalve een 'online' component bestaat er een 'offline' component in de zin dat er (ook) sprake is van fysieke interactie tussen slachtoffer en pleger. Dit is bij ongeveer een kwart van de fraudezaken en bij bijna 60% van de persoonsgerichte delicten het geval. Bij een groot deel van de fraude-/oplichtingzaken is geen verdachte in beeld (69%). Bij de persoonsgerichte delicten is juist in 82% van de zaken wel een verdachte bekend. Bij chantage/afpersing is dit voor de helft van de zaken het geval.

Het valt op dat de doorlooptijden van digitale zaken op basisteams verschillen. Ze hebben ofwel een relatief korte looptijd – 45% van alle zaken kent een doorlooptijd tussen de één en 21 dagen. Sommige zaken werden direct – nog op dezelfde dag van melding/aangifte – afgehandeld (14 van de 77). De rest van de zaken liep langer dan drie weken. Het gaat dan om enkele maanden of zelfs langer. Rond eenderde van de zaken (26 van de 77) kende een looptijd van langer dan honderd dagen. Zo komt het voor dat een zaak na vijf weken zonder inzet van opsporingsmiddelen (administratief) wordt afgerond (NOORD38) of dat er twee maanden na aangifte werd besloten een zaak af te ronden (NOORD40).

Ook komt het voor dat er met tussenpozen activiteiten plaatsvinden en een zaak (ogenschijnlijk) een tijd stilligt. Zo was er een andere zaak waarbij er een maand overheen ging voordat deze in behandeling werd genomen, waarna het weer drie weken duurde voordat de verdachte aan het dossier werd toegevoegd en vervolgens nog eens vijf we-

ken voordat er een stopgesprek werd gevoerd (ZEE46). Als uitschieter kwam een zaak voorbij met wel negentig aangiften van fraude/oplichting en een doorlooptijd van in totaal 13 maanden (MIDDENtrots/lmio). In veel geanalyseerde digitale zaken zijn er bepaalde periodes dat ze lijken stil te liggen in die zin dat er geen (geregistreerde) activiteit plaatsvindt. Het kan lang duren voordat een zaak in behandeling wordt genomen en er vorderingen worden gedaan, en er, na vordering, gegevens binnenkomen.

Uitsplitsing van zaken
Hieronder zijn de gereconstrueerde en geanalyseerde 77 zaken uitgesplist naar 'delicttypen' (Tabel 2), 'wel of geen aangifte gedaan' (Tabel 3), 'wel of geen hybride zaak' (Tabel 4) en 'wel of geen bekende verdachte' (Tabel 5).

Tabel 2 Zaakreconstructies (N=77) naar hoofd- en subdelict

	Fraude/ oplichting	**Persoonsgericht**	**Afpersing/ chantage**	**Overig**	**Eindtotaal**
Aan- en verkoopfraude	13				13
Misbruik accounts voor bestellingen	8				8
Bankhelpdeskfraude	8				8
Beleggingsfraude	6				6
Overige fraude	6				6
Hulpvraagfraude	3				3
Vriend in Nood-fraude	2				2
CEO-fraude	2				2
Creditcardfraude	2				2
Diefstal cryptomunten	1				1
Bankphishing	1				1
Helpdeskfraude	1				1
Sextortion			6		6
Overige afpersing		1			1
Smaad/laster/belediging		4			4
Bedreiging/ stalking		10			10
Overige cybercrime				1	1
Sexting		2			2
Eindtotaal	**53**	**17**	**6**	**1**	**77**

Tabel 3 Zaakreconstructies (N=77): aangifte ja/nee

	Ja	Nee	Eindtotaal
Fraude/oplichting	96%	4%	100%
Persoonsgericht	35%	65%	100%
Chantage/afpersing	50%	50%	100%
Overig	100%	0%	100%
Eindtotaal	**79%**	**21%**	**100%**

Tabel 4 Zaakreconstructies (N=77) hybride ja/nee

	Ja	Nee	Eindtotaal
Fraude/oplichting	26%	74%	100%
Persoonsgericht	59%	41%	100%
Chantage/afpersing	17%	83%	100%
Overig	0%	100%	100%
Eindtotaal	**32%**	**68%**	**100%**

Tabel 5 Zaakreconstructies (N=77) Bekende verdachte ja/nee

	Ja	Nee	Eindtotaal
Fraude/oplichting	31%	69%	100%
Persoonsgericht	82%	18%	100%
Chantage/afpersing	50%	50%	100%
Overig	0%	100%	100%
Eindtotaal	**44%**	**56%**	**100%**

Zaakreconstructies

Voor de reconstructie van de 77 zaken hebben we een tijdlijn en reflectie gemaakt (zie format hieronder). Er hebben vier onderzoekers aan de zaakreconstructies gewerkt, waarbij we wederom een interbeoordelaars-check hebben uitgevoerd door onderling zaken met elkaar te bekijken, te bespreken en te vergelijken. Hierdoor is een persoonlijke bias bij de reconstructie van zaken zo veel mogelijk tegengegaan.

Zaakinfo	
Zaakcode	BT/nr.
Zaaknaam	Naam
Aangeleverd door	*Steekproef/BT*
Analyse door	Naam

Vragen vooraf		
1a	Maatschappelijke klasse – code	
1b	Maatschappelijke klasse – omschrijving	
2a	Type delict – hoofddelict	
2b	Type delict – subdelict	
3	Aangifte j/n	
4	Bekende verdachte j/n	
5	BOSZ-status	
6	Digitaal middel	
7	Hybride j/n	
8	SLO en VD bekenden? j/n	
9	Kanaal van melding/aangifte	
10	Organisatieonderdeel instroom	
11	Organisatieonderdeel(en) afhandeling	
12	Contactpersoon/ team	

Tijdlijn		
Datum	**Gebeurtenis/incident/activiteit**	**Vragen & opvallendheden**

Kenschets (kort)

Wie deed wat?
- Acties politie
- Acties partners

Keuzes: welke keuzes zijn gemaakt op basis waarvan/waarom?

Reflectievragen
- Terugkijken: hoe liep het proces van aangifte tot afhandeling?
- Wat is onduidelijk/niet bekend?
- Heeft de politie gedaan wat ze kon?
- Wat ging goed?
- Wat kon beter?
- Wat en wie maakte het verschil?
- Overige

Analyse en reflectie
De analyse van de 77 tijdlijnen betrof een kwalitatieve analyse van de zaken om gedeelde kenmerken en rode lijnen te identificeren. Daaruit kwamen de volgende thema's naar voren: het herkennen van digitale criminaliteit, keuzes in zaken, samenwerken (intern en extern), schaalbare criminaliteit, afloop/resultaten, omgaan met slachtoffers, omgaan met verdachten en verschil maken. Het beeld dat uit deze rode lijnen naar voren kwam, is tijdens aparte reflectiesessies voorgelegd aan en besproken met een vertegenwoordiging van ieder van de zes basisteams. Vragen die we hebben gesteld zijn: herkennen jullie dit beeld? Waarop wel of niet? En hoe zijn bevindingen te duiden of verklaren? Dit gebeurde tijdens terugkoppelsessies van ongeveer twee uur op elk van de zes basisteams.

Bijlage 6 Methode en aanpak slachtofferenquête

Enquêtegegevens
In de periode 2022-2023 heeft de politie een grootschalig enquêteonderzoek uitgevoerd onder aangevers van criminaliteit, genaamd 'Politiemonitor'. Alle personen die in de periode augustus 2022 tot eind december 2022 aangifte hadden gedaan in Nederland hebben een vragenlijst toegestuurd gekregen teneinde hen te bevragen over hun ervaring met het aangifteproces. In totaal hadden 162.399 personen aangifte gedaan, waarvan er 25.760 de vragenlijst volledig invulden (16% respons). Van deze groep deden 1.483 (6%) aangifte van digitale criminaliteit, zoals hacken, helpdeskfraude, marktplaatsfraude en fraude via apps. De overige 24.277 slachtoffers (94%) hadden aangifte gedaan van traditionele criminaliteit, waaronder vermogensdelicten, geweld, fraude, vandalisme, incidenten in het verkeer en discriminatie.

Representativiteit
Om na te gaan in hoeverre de respondenten representatief waren voor alle aangevers van criminaliteit, hebben we een logistische regressieanalyse uitgevoerd om respondenten met niet-respondenten te vergelijken op geslacht, nationaliteit, leeftijd en het type criminaliteit waarvan ze aangifte hadden gedaan. De representativiteitsanalyse toont aan dat vrouwen iets meer geneigd waren dan mannen om de vragenlijst in te vullen en dat de kans op respons hoger was onder aangevers van criminaliteit met een hogere leeftijd. Nationaliteit (Nederlands versus niet-Nederlands) hing sterk samen met de kans om de vragenlijst in te vullen, waarbij personen met een Nederlandse nationaliteit aanzienlijk meer geneigd waren de vragenlijst in te vullen dan personen met een niet-Nederlandse nationaliteit. Het feit dat de vragenlijst alleen in het Nederlands beschikbaar was zal een belangrijke rol hebben gespeeld. Tot slot zagen we verschillen in respons tussen aangevers van verschillende typen delicten; slachtoffers van vermogensdelicten, incidenten in het verkeer en vandalisme bleken minder geneigd te zijn de vragenlijst in te vullen dan slachtoffers van digitale criminaliteit. Voor slachtoffers van discriminatie, fraude en geweld zagen we geen verschillen in respons met de slachtoffers van digitale criminaliteit.

Aangezien uit de representativiteitsanalyse bleek dat de respons op de Politiemonitor niet volledig representatief was voor de aangevers van criminaliteit in Nederland, hebben we weegfactoren berekend en toegepast in alle verdere analyses. Respondenten met een lagere kans om te reageren, kregen een hoger gewicht en telden zodoende zwaarder mee, terwijl respondenten met een relatief hoge kans om te reageren een la-

ger gewicht kregen. Door in de analyses gebruik te maken van de weegfactoren kunnen de resultaten uit de kwantitatieve analyse beter gegeneraliseerd worden naar de gehele populatie slachtoffers die aangifte doen in Nederland dan wanneer ongewogen resultaten zouden worden gepresenteerd. Op deze wijze kunnen de verschillen tussen slachtoffers van digitale criminaliteit en slachtoffers van andere vormen van criminaliteit in Nederland worden onderzocht op de volgende punten: (a) de impact van een incident op het slachtoffer, (b) de behoeftes van slachtoffers die zij hadden na een incident en (c) de tevredenheid met de politie na het aangifteproces. Zie de afsluitende paragraaf van deze bijlage voor meer details over de respondenten en niet-respondenten van de Politiemonitor en de representativiteitstest.

Uitkomstmaten
We beschrijven achtereenvolgens de drie uitkomstmaten die zijn geanalyseerd. Bij het bespreken van de variabelen wordt soms gebruikgemaakt van verkorte labels. De volledige beschrijvingen van deze labels zijn in de laatste paragraaf van deze bijlage te vinden. Tabel 1 presenteert de beschrijvende statistieken van de uitkomstmaten voor alle respondenten van het onderzoek.

Impact van het incident op slachtoffers. De impact die slachtoffers ervaarden na het incident werd op twee manieren uitgevraagd: er werd gevraagd naar a) de directe impact van het incident en b) de latere impact van het incident.

Om de ***directe impact*** te meten werd respondenten de volgende vraag gesteld: *Wat ging er door u heen op het moment dat het strafbare feit plaatsvond of toen u ontdekte dat het had plaatsgevonden?* Respondenten konden kiezen uit één of meerdere antwoorden, te weten: *shock, ontkenning, wanhoop, hulpeloosheid, lichamelijke klachten,* en *anders, namelijk...* Alle losse antwoordcategorieën zijn als dichotome uitkomstmaten (ja/nee) geanalyseerd. Gemiddeld gaven de respondenten aan 1,14 directe gevolgen te ervaren (*SD*=0,92). Respondenten blijken direct na het incident de meeste gevoelens van hulpeloosheid te ervaren (26% van de respondenten gaf dit aan) en/of andere gevolgen dan degene waaruit gekozen kon worden in de vragenlijst (38% van de respondenten gaf dit aan).

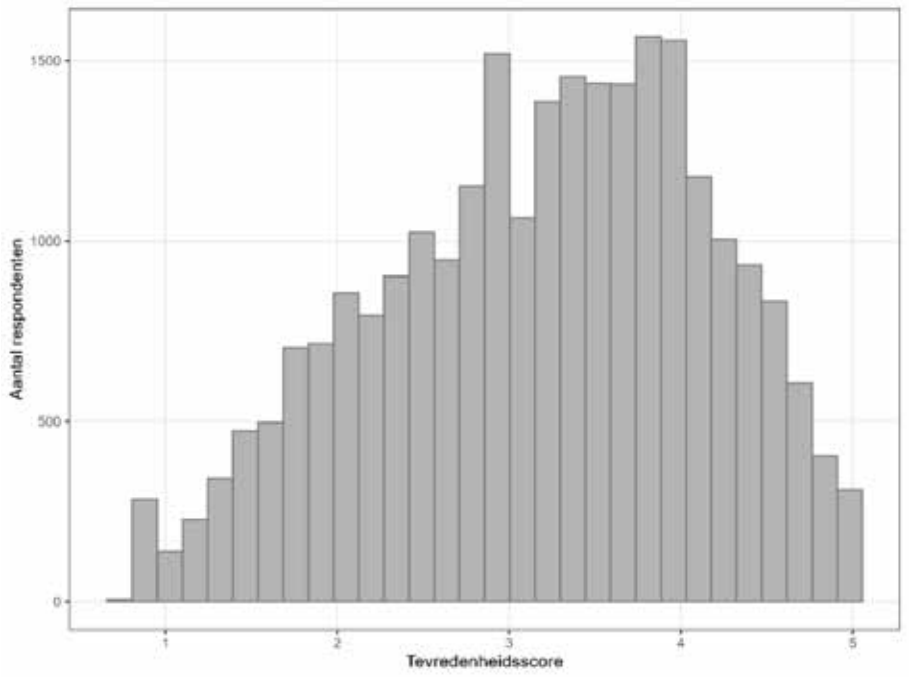
Om de ***latere impact*** te meten werd de volgende vraag gesteld: *Heeft het strafbare feit op dit moment nog emotionele gevolgen voor u?* De vraagstelling refereert naar de impact ten tijde van het invullen van de Politiemonitor. Respondenten konden kiezen uit één of meerdere antwoorden, te weten: *stress, angst, boosheid, schuldgevoelens, voorzichtigheid, herbeleving, herhalingsangst, onveiligheidsgevoel op het internet*. Gemiddeld gaven de respondenten aan 1,22 latere gevolgen te ervaren (*SD*=1,35). De meest genoemde langetermijngevolgen betreffen boosheid (36% van de respondenten gaf dit aan) en voorzichtigheid (35% van de respondenten gaf dit aan).

Tabel 1 Beschrijvende statistieken impact en behoeftes (N=25.760)

Directe impact	Min	Max	Proportie
anders	0	1	0,38
hulpeloosheid	0	1	0,26
wanhoop	0	1	0,18
ontkenning	0	1	0,12
lichamelijke klachten	0	1	0,10
shock	0	1	0,09
Langdurige impact			
boosheid	0	1	0,36
voorzichtigheid	0	1	0,35
herhalingsangst	0	1	0,20
stress	0	1	0,12
schuldgevoelens	0	1	0,07
angst	0	1	0,05
herbeleving	0	1	0,04
onveiligheidsgevoel op het internet	0	1	0,04
Behoeftes van slachtoffers			
opsporing	0	1	0,58
serieus	0	1	0,35
erkenning	0	1	0,33
compensatie	0	1	0,28
assistentie	0	1	0,26
support	0	1	0,22
informatie	0	1	0,20
anders	0	1	0,17
advies	0	1	0,15
praten	0	1	0,09
bescherming	0	1	0,08
therapie	0	1	0,02

Behoeftes van slachtoffers. Respondenten werd de volgende vraag gesteld: *Waaraan had u vooral behoefte direct nadat het strafbare feit u was overkomen?* Respondenten kregen twaalf opties voorgelegd, te weten: *support, assistentie, therapie, bescherming, praten, opsporing, compensatie, erkenning, serieus, advies*, *informatie* en *anders, namelijk...* Alle losse antwoordcategorieën zijn als dichotome uitkomstmaten (ja/nee) geanalyseerd. Gemiddeld gaven de respondenten aan 2,73 behoeftes te hebben voor het doen van de aangifte (*SD*=1,81). Respondenten blijken het meest behoefte te hebben aan opsporing, aanhouding en vervolging van de dader (58% van de respondenten gaf dat aan).

Tevredenheid met de politie. De tevredenheid van slachtoffers werd gemeten met behulp van negen verschillende vragen en stellingen. De meeste variabelen varieerden van 1 (sterk mee oneens) tot 5 (sterk mee eens). Drie variabelen moesten worden aangepast om op deze schaal te passen: voor twee negatief geformuleerde vragen werden de antwoordcategorieën omgedraaid en één variabele met een 10-puntsschaal werd naar dezelfde range omgezet door de waarden door twee te delen. Tabel 2 geeft een overzicht van de afzonderlijke tevredenheidsitems en hun beschrijvende statistieken. We voerden een factoranalyse uit op deze negen variabelen om te zien of de afzonderlijke items zijn samen te voegen tot een enkele tevredenheidsschaal. Dit bleek inderdaad mogelijk en de negen afzonderlijke items vertonen een hoge interne consistentie (Cronbach's alpha=0,87). Voor elke respondent construeerden we daarom een algemene tevredenheidsscore door het gemiddelde over de geldige waarden op de negen items te berekenen. Figuur 1 geeft de verdeling van de tevredenheid over alle respondenten weer. Het gemiddelde van de tevredenheidscore is 3,19 (*SD*=0,96). De meerderheid van de respondenten was niet echt tevreden of echt ontevreden over de politie, maar er zijn uitschieters naar zowel boven als beneden. Sommige respondenten waren (zeer) tevreden, maar anderen juist (zeer) ontevreden.



Figuur 1 Verdeling tevredenheid (N=25.760)

Slachtofferschap van digitale of traditionele criminaliteit
De belangrijkste predictor in deze studie betreft de dichotome variabele digitale criminaliteit. Deze scoort 1 voor de 1.483 (6%) respondenten die aangifte hadden gedaan van digitale criminaliteit en 0 voor de overige 24.277 respondenten (94%) die aangifte hadden gedaan van traditionele criminaliteit.

Tabel 2 Beschrijvende statistieken tevredenheidsitems

Tevredenheidsvariabelen	Minimum	Maximum	Gemiddelde	SD
Ik werd serieus genomen	1	5	3,50	1,29
De politie onderschatte de gevolgen die het strafbare feit voor mij had	1*	5	2,76	1,27
Voor mijn gevoel gaf de politie mij de schuld van het strafbare feit	1*	5	1,64	0.96
De politie had genoeg kennis om mij goed te kunnen helpen	1	5	3,67	1,06
Ik kreeg voldoende informatie van de politie over wat ze gedaan hebben of nog gaan doen met mijn aangifte	1	5	2,73	1,36
De verwachtingen die ik had toen ik aangifte deed zijn waargemaakt	1	5	2,86	1,35
Ik ben tevreden over de wijze waarop de politie mijn aangifte heeft behandeld	1	5	3,27	1,27
Na het doen van mijn aangifte heb ik door de manier waarop de politie hiermee is omgegaan meer vertrouwen gekregen in de politie	1	5	3,15	0,78
Als u terugkijkt naar de manier waarop de politie u heeft geïnformeerd over de afhandeling van uw aangifte welk rapportcijfer geeft u daar dan voor?	1*	10	5,79	2,69

Noot: Variabelen gemarkeerd met een * zijn aangepast voordat de tevredenheidsschaal werd geconstrueerd.

Controlevariabelen
Voor een nauwkeurige beantwoording van de onderzoeksvragen is het essentieel om in de analyse rekening te houden met variabelen die de verschillen tussen slachtoffers van digitale en traditionele criminaliteit op de verschillende uitkomstmaten kunnen beïnvloeden. De groep slachtoffers van digitale criminaliteit kan immers op allerlei kenmerken verschillen van de groep slachtoffers van traditionele criminaliteit en deze kenmerken kunnen ook samenhangen met impact, behoeftes, en de tevredenheid van slachtoffers. Hieronder worden alle controlevariabelen besproken. Tabel 3 presenteert de beschrijvende statistieken van deze variabelen.

Sociaal-demografische kenmerken. Slachtoffers verschillen van elkaar op sociaal-demografische kenmerken. Deze kenmerken brengen uiteenlopende ervaringen met zich mee en leiden tot verschillende percepties van incidenten en/of interacties met de politie (o.a. Bolger et al., 2021; Reisig & Parks, 2000; CBS, 2022; Weiss, 2010; Wu, 2014).

In de analyses houden we om die reden rekening met *leeftijd*, *geslacht*, *nationaliteit* en *opleidingsniveau*. Leeftijd is gemeten in jaren en geslacht betreft een dichotome variabele (man/vrouw) gebaseerd op de wijze waarop aangevers in het systeem van de politie waren geregistreerd. Nationaliteit is tevens gebaseerd op de wijze waarop aangevers in het systeem van de politie waren geregistreerd. De verschillende nationaliteiten van de aangevers in het politiesysteem hebben we gedichotomiseerd in een groep met een Nederlandse nationaliteit en een groep met een niet-Nederlandse nationaliteit. Voor opleidingsniveau is aan de respondenten gevraagd wat hun hoogst voltooide opleidingsniveau is. De antwoorden zijn omgecodeerd naar het totale aantal jaren genoten onderwijs dat er gewoonlijk voor staat om een dergelijk niveau af te ronden.

Tabel 3 Beschrijvende statistieken controlevariabelen

Variabelen	Proportie	Gemiddelde	SD	Min	Max
Leeftijd		53,01	16,62	16	98
Opleidingsniveau		15,12	3,32	6	20
Verstreken tijd sinds incident		140,98	52,90	44	258
Vrouw	0,44			0	1
Nederlands	0,95			0	1
Eerder slachtofferschap	0,24			0	1
Aangiftekanaal:					
Op het politiebureau	0,21			0	1
Thuis	0,06			0	1
Een andere fysieke locatie	0,01			0	1
Via de telefoon	0,06			0	1
Via internet	0,62			0	1
Video conference call	0,01			0	1
Anders	0,03			0	1
Communicatie	0,46			0	1
Politieactie	0,16			0	1

Eerder slachtofferschap. Eerder slachtofferschap kan psychologische en fysieke sporen nalaten (Hanson et al., 2010; Semenza et al., 2021). Dit zou het beeld wat slachtoffers hebben over de politie kunnen beïnvloeden. Respondenten werden twee vragen gesteld: *Was u de afgelopen 2 jaar al een slachtoffer van hetzelfde strafbare feit?* en *Heeft u in de afgelopen 2 jaar zelf een ander strafbaar feit meegemaakt?* Beide vragen konden beantwoord worden met *Ja*, *Nee,* en *Zeg ik liever niet.* We hebben de antwoorden op beide vragen gecombineerd tot een dichotome variabele *eerder slachtofferschap* (ja/nee). Als op één of op beide oorspronkelijke vragen *ja* werd geantwoord, werd de score voor *eerder slachtofferschap* als *ja* geregisterd. In andere gevallen werd de score voor *eerder slachtofferschap* als *nee* geregistreerd.

Aangiftekanaal. Respondenten kunnen aangifte doen middels verschillende aangiftekanalen. Eerder onderzoek liet zien dat de tevredenheid van slachtoffers lager is wanneer zij online aangifte doen vergeleken met slachtoffers die aangifte doen in persoon of via de telefoon (MOPAC, 2020, 2021). Respondenten werd de vraag gesteld: *Hoe heeft u aangifte gedaan?* De vraag kon beantwoord worden door een van de volgende opties te kiezen: *op een politiebureau, thuis, op een andere plaats – niet op een politiebureau of thuis, via internet, via beeldbellen, via de telefoon* en *anders, namelijk...*

Communicatie na aangifte. Respondenten kunnen na hun aangifte contact hebben gehad met de politie. Vervolgcontact blijkt een positieve invloed te hebben op slachtoffers (Clark et al., 2022). Respondenten werd de vraag gesteld: *Heeft u na uw aangifte iets gehoord van de politie?* De vraag kon beantwoord worden met *ja* of *nee*.

Politieactie naar aanleiding van de aangifte. De politie kan naar aanleiding van de aangifte actie ondernemen. Politieoptreden kan de tevredenheid van burgers beïnvloeden (o.a. Brandl & Horvath, 1991) Respondenten werd de vraag gesteld: *Is de politie in actie gekomen naar aanleiding van uw aangifte?* De vraag kon beantwoord worden met *Ja, Nee* of *Dat weet ik niet.* De antwoorden zijn gecombineerd tot één dichotome variabele voor *politieactie* (ja/nee). Als op de oorspronkelijke vraag *ja* werd geantwoord, werd de score voor *politieactie* als *ja* geregistreerd. In de andere gevallen werd de score voor *politieactie* als *nee* geregistreerd.

Verstreken tijd sinds het incident. Gevoelens en meningen over een incident kunnen veranderen over de tijd (Janssen et al., 2021). Uit het politiesysteem kon worden achterhaald wanneer een incident voor het eerst was gemeld. Bij het invullen van de vragenlijst is opgeslagen wanneer respondenten de vragenlijst afrondden. Het verschil in dagen tussen het invullen van de vragenlijst en het registreren van het incident is de *verstreken tijd sinds het incident*.

Analysemethode

Voor de analyse van de dichotome uitkomstmaten (de afzonderlijke items voor *directe impact*, *latere impact* en *behoeftes*) is gebruikgemaakt van logistische regressieanalyse. Voor de analyse van de continue uitkomstmaat tevredenheid is gebruikgemaakt van een lineair OLS-regressiemodel. Telkens zijn we met name geïnteresseerd in de parameter voor digitale criminaliteit. Die drukt immers de mate van verschil uit in de uitkomstmaat tussen slachtoffers van digitale criminaliteit en slachtoffers van traditionele criminaliteit. Om die parameter zo zuiver mogelijk te schatten zijn per uitkomstmaat telkens modellen geschat waarin rekening werd gehouden met controlevariabelen die (in ieder geval theoretisch) voorafgaand aan de desbetreffende uitkomstmaat een rol kunnen hebben gespeeld. Daarmee houden we bij de analyse van directe impact en behoeftes rekening met de sociaal-demografische variabelen *leeftijd*, *geslacht*, *nationaliteit, opleidingsniveau*, *eerder slachtofferschap en verstreken tijd sinds het incident* terwijl we bij de analyse van latere impact (ten tijde van het invullen van de survey) daar-

naast ook rekening houden met *communicatie na de aangifte* en of de *politie na de aangifte actie heeft ondernomen*. Bij de analyse van tevredenheid nemen we alle controlevariabelen mee en houden we daarnaast ook rekening met de *impact* die het op het slachtoffer heeft gehad en welke *behoeftes* het slachtoffer heeft gehad. Tabel 4 geeft een overzicht van de verschillende controlevariabelen die in de afzonderlijke analyses een rol hebben gespeeld.

Om de lezer niet te belasten met ellenlange tabellen beperken we de presentatie van de resultaten tot een grafische weergave van enkel de parameter voor digitale criminaliteit. Dit betreft telkens de parameter zoals deze in de afzonderlijke logistische of continue regressiemodellen werd geschat, dus na rekening te hebben gehouden met de controlevariabelen. De lezer die wel geïnteresseerd is in de details van de modellen verwijzen we graag door naar de laatste paragraaf van deze bijlage.

De resultaten van de logistische regressieanalyses presenteren we als odds ratio's (OR) met hun bijbehorende 95%-betrouwbaarheidsinterval. De odds ratio is een statistische maat die de verhouding aangeeft van de odds van een bepaalde gebeurtenis in een groep ten opzichte van de odds van dezelfde gebeurtenis in een andere groep. De odds betreffen de kans (P) dat de gebeurtenis plaatsvindt gedeeld door de kans dat deze niet plaatsvindt ($= P_{ja} / (1 - P_{ja})$). Voor onze dichotome uitkomstmaten betreft de gebeurtenis telkens dat de respondent een bepaald antwoord heeft aangevinkt (*ja* op de uitkomstmaat). Een odds ratio van 1 geeft aan dat de kans voor slachtoffers van digitale criminaliteit exact gelijk is aan de kans voor slachtoffers van traditionele criminaliteit. Odds ratio's boven 1 wijzen op een grotere kans onder slachtoffers van digitale criminaliteit, terwijl odds ratio's tussen 0 en 1 juist wijzen op een grotere kans onder slachtoffers van traditionele criminaliteit. Een odds ratio van 2 wijst er bijvoorbeeld op dat de odds tweemaal zo groot is onder slachtoffers van digitale criminaliteit als onder slachtoffers van traditionele criminaliteit, terwijl een odds ratio van bijvoorbeeld 0,33 er juist op zou wijzen dat de odds een derde zo groot (dus driemaal zo klein) is onder slachtoffers van digitale criminaliteit als onder slachtoffers van traditionele criminaliteit.

De resultaten van het continue OLS-regressiemodel geven we weer als ongestandaardiseerde regressiecoëfficiënt met het bijbehorende 95%-betrouwbaarheidsinterval. Een positieve regressiecoëfficiënt wijst op een hogere tevredenheid onder slachtoffers van digitale criminaliteit dan onder slachtoffers van traditionele criminaliteit, een negatieve op een lagere tevredenheid.

Tabel 4 Controlevariabelen per uitkomstmaat

	Impact direct	**Behoeftes**	**Impact later**	**Tevredenheid**
Digitale slachtoffer	x	x	x	x
Sociaal-demografisch	x	x	x	x
Eerder slachtofferschap	x	x	x	x
Aangiftekanaal			x	x
Communicatie na aangifte			x	x
Politieactie naar aanleiding van de aangifte			x	x
Verstreken tijd sinds het incident	x	x	x	x
Impact direct				x
Behoeftes				x
Impact later				x

Additionele informatie over respondenten, representativiteit, labels en modellen
Hieronder staat additionele informatie over de representativiteit van respondenten (Figuur 5) van de Politiemonitor en de representativiteitstest die is uitgevoerd (Figuur 6). Ook bevat deze afsluitende paragraaf informatie over labels en over het gebruikte lineaire regressiemodel (Figuur 7 en 8).

Tabel 5 Demografisch gegevens van (niet-)respondenten van de Politiemonitor

	Niet-respondenten (N=136.639)	Respondenten (N=25.760)
	Gemiddelde (SD)	*Gemiddelde (SD)*
Vrouwen	0,44 (0,50)	0,44 (0,50)
Nederlanders	0,88 (0,33)	0,95 (0,22)
Leeftijd	41,6 (16,1)	53,0 (16,6)
Digitale criminaliteit	0,03 (0,16)	0,06 (0,23)

Tabel 6 Representativiteitstest

	Estimate	SE	Z-Value	Pr (>|z|)
Vrouw	0,046**	0,014	3,194	0,001
Leeftijd (leeftijd-min(leeftijd))	0,039***	0,000	90,292	0,000
Nederlands	0,608***	0,030	20,125	0,000
Type criminaliteit (ref = digitale criminaliteit)				
Discriminatie	0,035	0,077	0,456	0,649
Fraude	-0,032	0,050	-0,647	0,518
Vermogensdelicten	-0,412***	0,033	-12,288	0,000
Verkeersincidenten	-0,522***	0,038	-13,646	0,000
Vandalisme	-0,236***	0,038	-6,238	0,000
Geweldsdelicten	0,018	0,043	0,410	0,682
Intercept	-3,125***	0,046	-67,565	0,000

Ter toelichting op Tabel 6: de p-waarden helpen bepalen of de effecten van leeftijd, geslacht, nationaliteit en type criminaliteit significant zijn bij het voorspellen van de kans op reageren op de Politiemonitor. Uit onderstaande gegevens blijkt dat de groep respondenten die heeft gereageerd verschilt van alle Nederlandse aangevers van criminaliteit. De representativiteitsanalyse toonde aan dat vrouwen, slachtoffers met een Nederlandse nationaliteit en met een hogere leeftijd meer geneigd om de Politiemonitor in te vullen. Daarnaast was ook het type criminaliteit niet representatief; slachtoffers van vermogensdelicten, incidenten in het verkeer en vandalisme bleken minder geneigd te zijn de vragenlijst in te vullen.

Tabel 7 Uitgeschreven labels van de variabelen behoeftes en impact

Behoeftes van slachtoffers	Labels
Weten waar ik terecht kon voor hulp en ondersteuning na het strafbaar feit	support
Praktische hulp bij de door het strafbare feit ontstane problemen, zoals bijvoorbeeld bij herstel of bij het regelen van zaken	assistentie
Professionele therapie of begeleiding om de gevolgen van het strafbaar feit te verwerken	therapie
Ik wilde door de politie beschermd worden	bescherming
Iemand bij de politie om mee te praten/met wie ik mijn gevoelens kon delen	praten
Opsporing, aanhouding en vervolging van de dader	opsporing
Financiële compensatie voor de schade die ik heb geleden	compensatie
Erkenning dat het strafbare feit mij is overkomen	erkenning
Serieus genomen worden als slachtoffer	serieus
Advies om te voorkomen dat ik nog eens zo'n strafbaar feit meemaak	advies
Informatie over het strafbare feit en hoe dit heeft kunnen plaatsvinden	informatie
Anders, namelijk…	anders
Directe impact	
Ik was hierdoor in psychische shock	shock
Ik ontkende wat er was gebeurd of kon het moeilijk geloven	ontkenning
Ik voelde mij hierdoor wanhopig	wanhoop
Ik voelde mij hierdoor hulpeloos	hulpeloosheid
Ik had hierdoor lichamelijke klachten zoals hartkloppingen, duizeligheid, trillen of hoofdpijn	lichamelijke klachten
Andere gevolgen, namelijk…	anders
Langdurige impact	
Ik ervaar nog stress of spanning	stress
Ik heb angst – of paniekklachten	angst
Ik maak mij er boos over	boosheid
Ik geef mijzelf de schuld van wat er is gebeurd	schuldgevoelens
Ik ben voorzichtiger geworden	voorzichtigheid
Ik beleef de gebeurtenis steeds opnieuw	herbeleving
Ik ben bang om nog een keer zoiets mee te maken	herhalingsangst
Ik voel mij op het internet minder veilig	onveiligheidsgevoel op het internet

Tabel 8 Lineair regressiemodel van tevredenheid (N=25.760)

	B	SE	Beta
Digitaal slachtoffer	0,011	0,025	0,002
Leeftijd (per 10 jaar)	0,087***	0,004	0,151
Vrouw	0,009	0,012	0,005
Nederlands	0,010	0,026	0,003
Jaren onderwijs	-0,006***	0,002	-0,021
Eerder slachtofferschap			
Aangiftekanaal (referentie: Op het politiebureau)			
Anders	-0,425***	0,036	-0,080
Thuis	0,137***	0,028	0,030
Andere locatie	-0,021	0,062	-0,002
Via internet	-0,429***	0,017	-0,211
Via videobellen	-0,058	0,061	-0,006
Via de telefoon	-0,083***	0,027	-0,019
Communicatie achteraf	0,611***	0,017	0,217
Politieactie achteraf	0,412***	0,013	0,208
Verstreken tijd sinds het incident (per maand)	-0,020***	0,003	-0,036
Behoefte			
Support	0,100***	0,016	0,042
Assistentie	0,047***	0,014	0,021
Therapie	-0,039	0,047	-0,006
Bescherming	-0,052**	0,025	-0,015
Praten	0,064***	0,024	0,018
Opsporing	-0,246***	0,013	-0,123
Compensatie	-0,049***	0,013	-0,023
Erkenning	0,045***	0,013	0,022
Serieus	-0,183***	0,014	-0,090
Advies	0,126***	0,019	0,045
Informatie	-0,015	0,016	-0,006
Anders	-0,238***	0,016	-0,087
Impact direct			
Shock	-0,064**	0,025	-0,021
Ontkenning	0,055***	0,019	0,019
Wanhopig	-0,047***	0,017	-0,019
Hulpeloos	-0,148***	0,015	-0,069
Lichamelijke klachten	-0,029	0,023	-0,009
Andere gevolgen	-0,014	0,013	-0,007

Impact later			
Stress	-0,285***	0,024	-0,101
Angst	-0,073**	0,036	-0,018
Boos	-0,358***	0,013	-0,178
Schuldgevoelens	0,019	0,024	0,005
Voorzichtiger	0,069***	0,013	0,034
Herbeleving	-0,078**	0,038	-0,016
Herhalingsangst	-0,080***	0,017	-0,035
Onveiligheidsgevoel op internet	-0,016	0,035	-0,003
Intercept	3,378***	0,042	
Adj. R2			

Opmerking: Gewogen met het omgekeerde van de waarschijnlijkheid van respons, genormaliseerd naar de steekproefomvang. 'Leeftijd', 'opleidingsniveau' en 'verstreken tijd sinds het incident' werden in het model opgenomen na aftrek van hun minimumwaarde; * p<0,05; ** p<0,01; *** p<0,001

Bijlage 7 Methode en aanpak interviews met slachtoffers

Ter illustratie bij de slachtofferenquête hebben we getracht ook met slachtoffers van digitale criminaliteit – en over hun ervaringen met de politie – te spreken. Het selectiecriterium hierbij was dat de slachtoffers aangifte of melding van het delict hadden gedaan.

Respondenten
Het bleek niet eenvoudig om respondenten onder slachtoffers van digitale criminaliteit te werven. Vanuit de onderzochte basisteams lukt het om vier respondenten aan te leveren. Om dit aantal uit te breiden hebben we in september 2023 1.100 studenten van de Hogeschool Utrecht, 75 docenten van de opleiding Integrale Veiligheidskunde aan de Hogeschool Utrecht en 498 masterstudenten Bestuurskunde aan de Vrije Universiteit Amsterdam benaderd. In september 2024 hebben we nog eens een uitvraag gedaan onder 300 studenten van de Hogeschool Utrecht en 659 masterstudenten Bestuurskunde aan de Vrije Universiteit Amsterdam. Deze twee pogingen leverden in totaal zes extra respondenten op. Daarnaast meldden zich vier respondenten uit het netwerk van de onderzoekers zelf. Via één van deze respondenten kwamen we op het spoor van nog eens twee respondenten.

De in totaal zestien interviews vonden plaats met zeven mannen en negen vrouwen. De oudste werd geboren in 1956, de jongste in 2005. Het merendeel van de respondenten heeft een hoger opleidingsniveau. Dertien respondenten deden aangifte, één een melding en twee hebben geen aangifte gedaan, maar waren wel in contact met de politie. Bij de een raadde een rechercheur informeel af om aangifte te doen, omdat het duidelijk was dat sporen naar het buitenland liepen en dit en te complexe zaak voor het basisteam werd. De ander deed geen aangifte, maar kwam uit politieonderzoek naar boven als geldezel en werd daarom ontboden. Uiteindelijk bleek deze respondent slachtoffer te zijn, waarna diegene werd heengezonden. Negen aangiften vonden plaats per internet of telefonisch (of een combinatie). Zes aangiften zijn op een basisteam opgenomen en bij een respondent heeft de politie ter plaatse een aangifte opgemaakt.

Format interviews
Tijdens de interviews met respondenten zijn we op de volgende onderwerpen ingegaan:

De gebeurtenis

1. Kunt u een beschrijving geven van het delict?
2. Waarvan bent u slachtoffer geworden?
   a. Fraude/oplichting: financiële oplichting zoals bankhelpdeskfraude, BEC-fraude, hulpvraagfraude, betaalverzoekfraude, tech support scam, misbruik van accounts voor bestellingen, aan- en verkoopfraude, beleggingsfraude.
   b. Persoonsgericht: delicten die in de persoonsgerichte sfeer worden gepleegd zoals stalking, bedreiging, smaad/laster/belediging, sexting.
   c. Chantage/afpersing: delicten als ransomware en sextortion.
   d. Overig: delicten die uit politieke of ideologische motieven of uit verveling of baldadigheid worden gepleegd zoals DDoS-aanvallen.
3. Wat is uw relatie tot de pleger(s)?
4. Heeft u aangifte of een melding gedaan?
5. Via welk kanaal heeft u een melding/aangifte gedaan?
   a. Persoonlijk op het politiebureau
   b. Telefonisch
   c. Via internet
   d. Via een 3D-verbinding (beeldbellen)
   e. Op het plaats delict
   f. Anders: …
   g. Wat is er gebeurd?
6. Heeft u zich vooraf aan de aangifte/melding voorbereidt op welke (bewijs)informatie relevant is om mee te nemen naar de politie ten behoeve van de aangifte/melding?

Behoeften en verwachtingen

1. Welke behoeften had u toen u een melding/aangifte deed bij de politie? Kunt u meer vertellen over:
   a. Strafrechtelijk: dat de dader wordt gepakt (straf, vergelding)
   b. Financieel: dat de schade wordt vergoed (probleem oplossen)
   c. Emotioneel: erkenning als slachtoffer
   d. Informatief: uitleg over het aangifteproces, de verdachte, het rechtssysteem
   e. Praktische behoeften: invullen van schadeformulieren bij bank of verzekeraar
   f. Anders: …
2. Waar had u het meest behoefte aan bij het doen van de melding/aangifte (belangrijkst)?
   a. Praktische hulp
   b. Actie
   c. Erkenning/serieus genomen worden
   d. Informatie over het delict en hoe dit heeft kunnen gebeuren
   e. Advies over hoe herhaling te voorkomen
   f. Ondersteuning en begeleiding of doorverwijzing naar bijvoorbeeld slachtofferhulp
   g. Anders: …

3. Was uw verwachting bij de melding/aangifte dat de politie aan uw belangrijke behoefte(n) kon voldoen? Bijvoorbeeld:
   a. Dat de politie veel actiebereidheid zou tonen/de dader zou pakken
   b. Dat de politie goed zou luisteren
   c. Dat de politie advies/tips/informatie zou geven
   d. Dat de politie zou doorverwijzen naar andere instanties
   e. Anders: …
4. Heeft de politie na melding/aangifte aan deze behoefte(n) voldaan? – en waarom wel of niet
   a. Ja
   b. Nee
   c. Anders: …
5. Hoe tevreden bent u over de politie:
   a. Intakegesprek of melding/aangifte over internet
   b. De uitkomsten van eventuele vervolgacties

Impact of gevolgen van het delict
1. In financiële zin
2. In psychische/emotionele zin
3. Wat zijn andere gevolgen voor u?

Over het slachtoffer
1. Geslacht
2. Leeftijd/geboortejaar
3. Woonplaats

De gespreksverslagen van de interviews zijn met behulp van een datamatrix in Excel gecodeerd en geanalyseerd.

Uitgaven in de reeks Politiekunde

1. ***Criminaliteit in de virtuele ruimte***
   P. van Amersfoort, L. Smit & M. Rietveld, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002
2. ***Cameratoezicht. Goed bekeken?***
   I. van Leiden & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2002
3. ***De 10 stappen van Publiek-Private Samenwerking (PPS)***
   J.C. Wever, A.A. van Pel & L. Smit, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002
4. ***De opbrengst van projecten. Een verkennend onderzoek naar de bijdrage van projecten aan diefstalbestrijding***
   C.J.E. In 't Velt, e.a., NPA-Onderzoeksgroep, LSOP, Apeldoorn, 2003
5. ***Cameratoezicht. De menselijke factor***
   A. Weitenberg, E. Jansen, I. van Leiden, J. Kerstholt & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem/TNO, Soesterberg, 2003
6. ***Jeugdgroepen in beeld. Stappenplan en randvoorwaarden voor de shortlist-methodiek***
   H.B. Ferwerda & A. Kloosterman, Advies- en Onderzoeksgroep Beke & Politieregio Gelderland-Midden, Arnhem, 2004 (vierde druk 2006)
7. ***Hooligans in beeld.Van informatie naar aanpak***
   H.B. Ferwerda & O. Adang, Advies- en Onderzoeksgroep Beke, Arnhem/ Onderzoeksgroep Politieacademie Apeldoorn, 2005
8. ***Richtlijnen auditieve confrontatie***
   J.H. Kerstholt, A.G. van Amelsvoort, E.J.M. Jansen & A.P.A. Broeders, TNO Defensie en Veiligheid, Soesterberg/Politieacademie, Apeldoorn/NFI, Den Haag, 2005
9. ***Niet verschenen***
10. ***De opsporingsfunctie binnen de gebiedsgebonden politiezorg***
    O. Zoomer, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2006
11. ***Inzoomen en uitzoomen op Zaandam***
    I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006

12. ***Aansprakelijkheidsmanagement politie. Beschrijving, analyse en handreiking***
E.R. Muller, J.E.M. Polak, C.J.J.M. Stoker m.m.v. M.L. Diepenhorst & S.H.E. Janssen, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag/ Faculteit der Rechtsgeleerdheid Universiteit Leiden, 2006

13. ***Cold cases – een hot issue***
I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem, 2006

14. ***Adrenaline en reflectie. Hoe leren politiemensen op de werkplek?***
A. Beerepoot & G. Walraven e.a., DSP-groep BV, Amsterdam/Walraven onderzoek en advies, 2007

15. ***Tussen aangifte en zaak. Een referentiekader voor het aangifteproces***
W. Landman, L.A.J. Schoenmakers & F. van der Laan, Twynstra Gudde, adviseurs en managers, Amersfoort, 2007

16. ***Baat bij de politie. Een onderzoek naar de opbrengsten voor burgers van het optreden van de politie***
M. Goderie & B. Tierolf, m.m.v. H. Boutellier & F. Dekker, Verwey-Jonker Instituut, Utrecht, 2008

17. ***Hoeveel wordt het vandaag? Een studie naar de kans op voetbalgeweld en het veiligheidsbeleid bij voetbalwedstrijden***
E.J. van der Torre, R.F.J. Spaaij & E.D. Cachet, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2008

18. ***Overbelast? De administratieve belasting van politiemensen bij de afhandeling van jeugdzaken***
G. Brummelkamp & M. Linssen, EIM, Zoetermeer, 2008

19. ***Geografische daderprofilering. Een inventarisatie van randvoorwaarden en succesfactoren***
G. te Brake & A. Eikelboom, TNO Defensie en Veiligheid, Soesterberg, 2008

20. ***Solosurveillance. Kosten en baten***
S.H. Esselink, J. Broekhuizen & F.M.H.M. Driessen, Bureau Driessen, 2009

21. ***Onderzoek naar de mogelijke meerwaarde van AWARE voor de politie. Ervaringen met een nieuwe aanpak van belaging door ex-partners***
M.Y. Bruinsma, J. van Haaf, R. Römkens & L. Balogh, IVA Beleidsonderzoek en Advies, i.s.m. INTERVICT/Universiteit van Tilburg, 2008

22. ***Gebiedsscan criminaliteit en overlast. Een methodiekbeschrijving***
B. Beke, E. Klein Hofmeijer & P. Versteegh, Bureau Beke, Arnhem, 2008

23. ***Informatiemanagement binnen de politie. Van praktijk tot normatief kader***
V. Bekkers, M. Thaens, G. van Straten & P. Siep; m.m.v. A. Dijkshoorn, Center for Public Innovation, Erasmus Universiteit Rotterdam, 2009

24. ***Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept***
H.B Ferwerda, E.J van der Torre & V. van Bolhuis, Bureau Beke, Arnhem/ COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

25. ***Rellen om te rellen. Een studie naar grootschalige openbare-ordeverstoringen en notoire ordeverstoorders***
I. van Leiden, N. Arts & H.B. Ferwerda, Bureau Beke, Arnhem, 2009

26a. ***Verbinden van politie- en veiligheidszorg. Politie en partners over signaleren & adviseren***
W. Landman, P. van Beers & F. van der Laan, Twynstra Gudde, Amersfoort, 2009

26b. ***Politiepolitiek. Een empirisch onderzoek naar politiële signalering & advisering***
E.J.A. Bervoets, E.J. van der Torre & J. Dobbelaar m.m.v. N. Koeman, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

27. ***De politie aan zet: de aanpak van veelplegers in Deventer***
I. Bakker & M. Krommendijk, IPIT, Enschede, 2009

28. ***Boven de pet? Een onderzoek naar grootschalige ordehandhaving in Nederland***
O.M.J. Adang (redactie), S.E. Bierman, K. Jagernath-Vermeulen, A. Melsen, M.C.J. Nogarede & W.A.J. van Oorschot, Politieacademie, Apeldoorn, 2009

29. ***Rellen in Ondiep. Ontstaan en afhandeling van grootschalige ordeverstoring in een Utrechtse achterstandswijk***
G.J.M. van den Brink, M.Y. Bruinsma (redactie), L.J. de Graaf, M.J. van Hulst, M.P.C.M. Jochoms, M. van de Klomp, S.R.F. Mali, H. Quint, M. Siesling, G.H. Vogel, Politieacademie, Apeldoorn, 2010

30. ***Burgerparticipatie in de opsporing. Een onderzoek naar aard, werkwijzen en opbrengsten***
A. Cornelissens & H. Ferwerda (redactie), met medewerking van I. van Leiden, N. Arts & T. van Ham, Bureau Beke, Arnhem, 2010

31. ***Poortwachters van de politie. Meldkamers in dagelijks perspectief***
J. Kuppens, E.J.A. Bervoets & H. Ferwerda, Bureau Beke, Arnhem & COT, Den Haag, 2010

32. ***Het integriteitsbeleid van de Nederlandse politie: wat er is en wat ertoe doet***
M.H.M. van Tankeren, Onderzoeksgroep Integriteit van Bestuur, Vrije Universiteit Amsterdam, 2010

33. ***Civiele politie op vredesmissie. Uitzendervaringen van Nederlandse politiefunctionarissen***
H. Sollie, Universiteit Twente, Enschede, 2010

34. ***Ten strijde tegen overlast. Jongerenoverlast op straat: is de Engelse aanpak geschikt voor Nederland?***
M.L. Koemans, Universteit Leiden, 2010

35. ***Het districtelijk opsporingsproces; de black box geopend***
R.M. Kouwenhoven, R.J. Morée &. P. van Beers, Twynstra Gudde, Amersfoort, 2010

36. ***Balanceren tussen alert maken en onrust voorkomen. Publiekscommunicatie over seriële schokkende incidenten (casestudy Lelystad)***
A.J.E. van Hoek, m.m.v. P.F. van Soomeren, M.D. Abraham & J. de Kleuver, DSP-groep, Amsterdam, 2011

37. ***Sturing van blauw. Een onderzoek naar operationele sturing in de basispolitiezorg***
W. Landman, m.m.v. M. Malipaard, Twynstra Gudde, Amersfoort, 2011

38. ***Onder het oppervlak. Een onderzoek naar ontwikkelingen en (a)select optreden rond preventief fouilleren***
J. Kuppens, B. Bremmers, E. van den Brink, K. Ammerlaan & H.B. Ferwerda, m.m.v. E.J. van der Torre, Bureau Beke, Arnhem/COT, Den Haag, 2011

39. ***Naar eigen inzicht? Een onderzoek naar beoordelingsruimte van en grenzen aan de identiteitscontrole***
J. Kuppens, B. Bremmers, K. Ammerlaan & E. van den Brink, Bureau Beke, Arnhem/COT, Den Haag, 2011

40. ***Toezicht op zedendelinquenten door de politie in samenwerking met de reclassering***
H.G. van de Bunt, N.L. Holvast & J. Plaisier, Erasmus Universiteit, Rotterdam/ Impact R&D, Amsterdam, 2012

41. ***Daders over cameratoezicht***
H.G.A. van Schijndel, A. Schreijenberg, G.H.J. Homburg & S. Dekkers, Regioplan Beleidsonderzoek, Amsterdam, 2012

42. ***Aanspreken op straat. Het werk van de straatcoach in al zijn verschijningsvormen***
L. Loef, K. Schaafsma & N. Hilhorst, DSP-groep, Amsterdam, 2012

43. ***De organisatie van de opsporing van cybercrime door de Nederlandse politie***
N. Struiksma, C.N.J. de Vey Mestdagh & H.B. Winter, Pro Facto, Groningen/ Kees de Vey Mestdagh, Groningen, 2012

44. ***Politie in de netwerksamenleving. De opbrengst van de politiële netwerkfunctie voor de kerntaken opsporing en handhaving openbare orde en de sturing hierop in de gebiedsgebonden politiezorg***
I. Helsloot, J. Groenendaal & E.C. Warners, Crisislab, Renswoude, 2012

45. ***Tegenspraak in de opsporing. Verslag van een onderzoek***
R. Salet & J.B. Terpstra, Radboud Universiteit Nijmegen, 2012

46. ***Tunnelvisie op tunnelvisie? Een verkennend en experimenteel onderzoek naar de besluitvorming door VKL-teams met betrekking tot het onderkennen van tunnelvisie en andere procesaspecten***
I. Helsloot, J. Groenendaal & B. van 't Padje, Crisislab, Renswoude, 2012

47. ***M.-waarde. Een onderzoek naar de bijdrage van Meld Misdaad Anoniem aan de politionele opsporing***
M.C. van Kuik, S. Boes, N. Kop, M. den Hengst-Bruggeling, T. van Ham & H. Ferwerda, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2012

48. ***Seriebrandstichters. Een verkennend onderzoek naar daderkenmerken en delictpatronen***
Y. Schoenmakers, A. van Wijk & T. van Ham, Bureau Beke, Arnhem, 2012

49. ***Van wie is de straat? Methodiek en lessen voor de politie om ongrijpbare veiligheidsfenomenen grijpbaar te maken – op basis van vijf praktijkcasus***
H. Ferwerda, T. van Ham & B. Bremmers, Bureau Beke, Arnhem, 2013

50. ***Recherchesamenwerking in de Euregio Maas-Rijn. Knooppunten, knelpunten en kansen***
H. Nelen, M. Peters & M. Vanderhallen, Politieacademie, Apeldoorn/ Universiteit Maastricht, 2013

51. ***De operationele politiebriefing onderzocht. Een onderzoek naar de effectiviteit van de operationele politiebriefing***
A. Scholtens, J. Groenendaal & I. Helsloot, Crisislab, Renswoude 2013

51a. ***De operationele politiebriefing onderzocht (2). Een actie(vervolg)onderzoek om tot een effectievere politiebriefing te komen***
A. Scholtens, Crisislab, Renswoude 2015

52. ***Sociale media: factor van invloed op onrustsituaties?***
R.H. Johannink, I. Gorissen & N.K. van As, Politieacademie Apeldoorn/ VDMMP, Houten, 2013

53. ***De terugkeer van zedendelinquenten in de wijk***
C.E. Huls & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen/Centrum voor Openbare Orde en Veiligheid, Groningen, 2013

54. ***Van meld- naar aantoonplicht. Een onderzoek naar een systeem van digitale surveillance***
C. Veen & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen, 2013

55. ***Heterdaadkracht in twee Haagse pilotgebieden***
B. van Dijk, J.B. Terpstra & P. Hulshof, Politieacademie, Apeldoorn/DSPgroep, Amsterdam, 2013

56. ***Inzet op Maat. Onderzoek naar kenmerken en mogelijkheden van duurzame inzetbaarheid van oudere medewerkers***
H. de Blouw, I.R. Kolkhuis Tanke & C.C. Sprenger, Politieacademie, Apeldoorn, 2013

57. ***Interventies in de opsporing. Impulsen in kwaliteit en effectiviteit van het opsporingsproces***
R.M. Kouwenhoven, R.J. Morée & P. van Beers, Twynstra Gudde, Amersfoort, 2013

58. ***De plaats delict in beeld. Fotografie in de dagelijkse en gesimuleerde praktijk***
G. Vanderveen & J. Roosma, Instituut voor Strafrecht & Criminologie, Universiteit Leiden, 2013

59. ***Jeugdgroepen van toen. Een casusonderzoek naar de leden van drie criminele jeugdgroepen uit het einde van de vorige eeuw***
H. Ferwerda, B. Beke & E. Bervoets, Bureau Beke, Arnhem/Beke Advies, Arnhem/LokaleZaken, Rotterdam, 2013

60. ***Tussen hei en hoofdbureau. Leiderschapsontwikkeling bij de politie***
W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort, 2013

61. ***Gemeentelijk blauw. Het dagelijks werk van gemeentelijke handhavers in beeld***
E. Bervoets, J. Bik & M. de Groot, LokaleZaken, Rotterdam, 2013

62. ***Excessief geweld op en om de voetbalvelden. Praktijkonderzoek naar omvang, ernst en aanpak van 'voetbalgeweld'***
P. Duijvestijn, B. van Dijk, P. van Egmond, M. de Groot, D. van Sommeren & A. Verwest, DSP-groep, Amsterdam, 2013

63. ***Beeld van gezag bij de politie. Maatschappelijke verbeelding en de impact van gezagsbeelden op burgers***
H. de Mare, B. Mali, M. Bleecke & G. van den Brink, m.m.v. Motivaction, Tilburg University, Stichting IVMV, Leiden, 2014

64. ***Informatiegestuurde dienders. Informatiesturing tussen theorie en praktijk***
A. van Sluis, P. Siep, V. Bekkers, m.m.v. M. Thaens & G. Straten, Center for Public Innovation, Erasmus Universiteit, Rotterdam, 2014

65. ***Hard op weg. Onderzoek aanpak verkeersveelplegers***
B. Bieleman, M. Boendermaker, R. Mennes & J. Snippe, Intraval, Groningen/ Rotterdam, 2014

66. ***Tussen hulp en hype. De inzet van opsporingsberichtgeving in ontvoeringszaken***
Y.M.M. Schoenmakers, J.V.O.R. Doekhie & J.C. Knotter, Yvette Schoenmakers Onderzoek en advies, Weesp, 2014

67. ***Nachtdienst bij de politie en verkeersveiligheid. Onderzoek naar ervaringen van politieagenten met verkeersonveiligheid in woon-werkverkeer na de nachtdienst***
P. Boekhoorn, BBSO, Nijmegen, 2014

68. ***Buit van woninginbraak. Onderzoek onder inbrekers en helers***
J. Snippe, M. Sijtstra, R. Mennes & B. Bieleman, Intraval, Groningen/ Rotterdam, 2014

69. ***Privaat blauw. Portiers, evenementbeveiligers en voetbalstewards op risicovolle locaties en tijdens risicovolle momenten***
E. Bervoets & S. Eijgenraam, LokaleZaken, Rotterdam, 2014

70. ***Met grof geschut. Reconstructie van een moordonderzoek binnen de criminele woonwagenwereld***
I. van Leiden, B. Bremmers & H. Ferwerda, Bureau Beke, Arnhem, 2014

71. ***Met fluwelen handschoenen? Politie en de omgang met verwarde personen in Amsterdam***
J. Kuppens, T. Appelman, T. van Ham & A. van Wijk, Bureau Beke, Arnhem, 2015

72a. ***Vermisten op de kaart. Aard en omvang van langdurige vermissingen***
I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2015

73. ***Van intel tot operatie. De impact van veiligheidsanalisten bij de aanpak van misdaad***
M. den Hengst, M. Bruinsma, Y. Schoenmakers, W. Niepce, Bureau Bruinsma, Tilburg, 2015

74. ***De bestuurlijke rapportage. Gezamenlijke inspanning in de aanpak van (georganiseerde) criminaliteit en overlast***
I. Gorissen, m.m.v. R.H. Johannink, PBLQ, Den Haag, 2015

75. ***De aangifte van delicten bij de multichannelstrategie van de politie***
P. Boekhoorn & J. Tolsma, Bureau Boekhoorn/Radboud Universiteit, Nijmegen, 2016

76. ***Die pakken we toch niet op? Afstemming tussen politie en Openbaar Ministerie in zaken van veelvoorkomende aangiftecriminaliteit***
R. Kouwenhoven & L. Kleijer-Kool, Twynstra Gudde, Amersfoort, 2016

77. ***Het real-time informeren van noodhulpeenheden. Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie***
A. Scholtens, M. den Hengst & R. Waterreus, Crisislab, Renswoude/ Politieacademie, Apeldoorn, 2016

78. ***Hoe lang kun je 'schijt hebben'? Dertien desisters uit criminele jeugdgroepen aan het woord***
C.E. Hoogeveen, A.E. van Burik & B.J. de Jong, m.m.v. E.M. Klooster, Bureau Alpha, 's-Hertogenbosch/VanMontfoort, Woerden, 2016

79. ***Onbenutte kansen. Een onderzoek naar het gebruik van restinformatie in de opsporing***
A. van Wijk & L. Scholten, m.m.v. B. Bremmers, Bureau Beke, Arnhem, 2016

80. ***Verbale leugendetectie-wizards***
G. Bogaard & E.H. Meijer, Maastricht University, Maastricht, 2016

81. ***Mensenhandel in de prostitutie opsporen zonder aangifte? Een vervolgonderzoek om de doorzettingsmacht van de politie te verduidelijken***
M. Goderie, m.m.v. R. Kool, Goderie Onderzoek, Klarenbeek, 2016

82. ***De onvindbaren. Op zoek naar voortvluchtige veroordeelden in Nederland***
Y. Schoenmakers, I. de Groot, J. van Zanten, A. van Rooyen & J. Baars, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2017

83. ***Elke dump is een plaats delict. Dumping en lozing van synthetisch drugsafval: verschijningsvormen en politieaanpak***
Y. Schoenmakers, S. Mehlbaum, M. Everartz & C. Poelarends, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2016

83A. ***De Intelligence Paradox. Lessen uit de integrale pilot Analyse Synthetische Drugs in Oost-Nederland***
Y. Schoenmakers, S. Mehlbaum, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2019

84. ***Naar handhaafbare noodbevelen en noodverordeningen. Een analyse van het gemeentelijke noodrecht***
A.J. Wierenga, C. Post & J. Koornstra, Rijksuniversiteit Groningen, Centrum voor Openbare Orde en Veiligheid, 2016

85. ***Vermisten op het spoor. Rechercheren naar langdurige vermissingen***
I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2017

86. ***De aard van het beestje. Kenmerken en achtergronden van dierenmishandelaars***
A. van Wijk & M. Hardeman, Bureau Beke, Arnhem, 2017

87. ***Modus operandi van de recherche. De rechercheprakijk in moord- en verkrachtingszaken***
A. van Wijk, I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2017

88. ***Over grenzen in de sport. De rol van de politie in de aanpak van seksueel grensoverschrijdend gedrag in de sport in samenwerking met relevante partners***
A. van Wijk, M. Hardeman, L. Scholten & M. Olfers, Vrije Universiteit Amsterdam, Bureau Beke, Arnhem, 2017

89. ***Defensiehulp. Legergroene bijstand aan de politie bij handhaving van de rechtsorde***
E. Bervoets, m.m.v. S. Eijgenraam, T. Dijkhuizen & J. van de Werken, Bureau Bervoets, Amersfoort, 2017

90. ***Tussen onder en boven. Productie en distributie van softdrugs in Noord- Nederland***
J. Snippe, R. Mennes, M. Sijtstra & B. Bieleman, Intraval, Groningen/Rotterdam, 2017

91. ***Vechten op afspraak. Inzicht in het fenomeen en input voor de ontwikkeling van een politiestrategie***
T. van Ham, L. Scholten, A. Lenders & H. Ferwerda, Bureau Beke, Arnhem, 2018

92. ***Notoire straten. Over de lokale inbedding van georganiseerde criminaliteit***
S. Mehlbaum, Y. Schoenmakers & J. van Zanten, Mehlbaum Onderzoek, Amsterdam, 2018

92A. ***De wortel en de stok. Praktijklessen uit een gebiedsgerichte probleemaanpak van ondermijning***
S. Mehlbaum, Y. Schoenmakers, Mehlbaum Onderzoek, Amsterdam, 2019

93. ***Ondermijning door criminele 'weldoeners'***
M. Bruinsma, R. Ceulen & T. Spapens, m.m.v. C. Deij, Tilburg University, Tilburg/Bureau Bruinsma, Tilburg, 2018

94. ***Kiezen voor politie. Een onderzoek onder mbo-studenten met een migratie – achtergrond in het veiligheidsdomein***
S. de Winter-Koçak, E. Klooster & M. Day, m.m.v. S. Mehlbaum, M. van Vugt & K. Leschonski, Verwey-Jonker Instituut, Utrecht, 2018

95. ***Doe-het-zelf-surveillance. Een onderzoek naar de werking en effecten van WhatsApp-buurtgroepen***
S. Mehlbaum & R. van Steden, m.m.v. M. van Dijk, Vrije Universiteit Amsterdam, Mehlbaum Onderzoek, Amsterdam, 2018

96. ***Een klacht is een gratis advies***
G. Jacobs, T. Hak, G. Vanderveen, M. Flory, T. Thuis, S. Valkeman & M. Franken, Erasmus Universiteit, Rotterdam, 2018

97. ***Voortgezet crimineel handelen tijdens detentie: je gaat het pas zien als je het doorhebt***
A. Verwest, W. Buysse, P. van Egmond, D. Hofstra, DSP-groep, Amsterdam, 2019

98. ***Zorg voor kinderen bij aanhouding van ouders; Best practices uit binnen- en buitenland***
J. Reef, N. Ormskerk, Universiteit Leiden, 2019

99. ***Aankoopfraude uit het buitenland***
J. Jansen, S. Westers, S. Twickler, W. Stol, NHL Stenden Hogeschool / Politieacademie

100. ***Grijs vakmanschap? Taakgerelateerd ongeoorloofd handelen binnen de politie***
R. Chr. van Halderen (diss. Avans Hogeschool), 2019

101. ***Niet meer doen! Een onderzoek naar de INDIGO-afdoening***
A. van Wijk, S. Dickie, J. van Esseveldt, Bureau Beke, Arnhem, 2019

102. ***De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging***
P. Boekhoorn, BBSO, Nijmegen, 2020

103. ***In- en doorstroom van nieuwkomers in beeld. Opgetekende lessen uit acht casussen rond de opvang van asielzoekers in Nederland.***
J. Kuppens, Bureau Beke, Arnhem 2020

104. ***De lading van vuurwapens. Een onderzoek naar de impact van illegale vuurwapens in Nederland.***
H. Ferwerda, J. Wolsink en I. van Leiden, Bureau Beke, Arnhem 2020

105. ***Q-teams. De politie onderweg naar toekomstbestendige opsporing en vervolging?***
P. van Egmond, A. Swami-Persaud, A. Verwest, DSP-groep, Amsterdam 2020

106. ***Onderwereld boven water? Zoektocht naar georganiseerde criminaliteit in de Noordelijke zeehavens***
N. Struiksma, C. Boxum, S.J. Hollenberg, N.O.M. Woestenburg, Pro Facto, Groningen 2020

107. ***Benutten van digitale sporen***
R. Zuurveen, W. Ph. Stol, Onderzoeksgroep Cybersafety. NHL Stenden en CyberScienceCenter 2020

108. ***Kansen en knelpunten binnen de financiële opsporing***
L.N. de Swart, G.P.J.M op 't Hoog, B.M.J Slot, A. Winkel. Ecorys 2021

109. ***Black box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk***
W. Bantema, S. Westers, M. Hoekstra, R. Herregodts, S. Munneke. NHL Stenden Hogeschool / Rijksuniversiteit Groningen, 2021

110. ***Ondermijning langs zijpaden. Een verkennend onderzoek naar de aard, omvang en aanpak van ondermijnende criminaliteit in relatie tot kleine havens en luchthavens, railtransport en binnenvaart in Noord-Brabant en Zeeland.***
S. van Nimwegen, T. Spapens, R. Ceulen, Tilburg University/Nationale Politie, 2021

111. ***Meer dan een ruzie. Politie in de netwerkaanpak huiselijk geweld.***
K.D. Lünnemann, S. ter Woerds, Verwey-Jonker Instituut 2021

112. ***Van verhalen naar verbalen. Een verkennende studie naar de aanpak van ondermijnende drugscriminaliteit in het Noordzeekanaalgebied en de haven van Amsterdam***
Y. Eski, M. Boelens, A. Mesic, H. Boutellier, Vrije Universiteit Amsterdam/Verwey-Jonker Instituut 2021

113. ***Weten, doen en leren. Een proeftuinonderzoek naar gebiedsgerichte opsporing***
E. Bervoets, J. Broekhuizen, K. van den Akker, J. Landsman, Bureau Bervoets, Amersfoort 2021

114. ***Zuiver op de graat? Over de betrokkenheid van de visserij bij maritieme drugssmokkel***
S. Mehlbaum, K. van den Akker, A. Verweij, A. Wester m.m.v. R. van der Borden en M. Dekker, Mehlbaum Onderzoek, Halfweg 2021

115. ***Kinderen als slachtoffer, getuige of dader van huiselijk geweld. Aard en afhandeling van door de politie bij ZSM aangebrachte zaken van huiselijk geweld waarbij minderjarigen zijn betrokken.***
V. van Koppen, M. Bruggeman, R. Houston, J. Harte, VU Amsterdam 2022

116. ***Wachters aan het woord. Dilemma's van accountants, advocaten, belastingadviseurs en notarissen in hun rol als poortwachter.***
K. van Wingerde, C. Hofman, Erasmus Universiteit Rotterdam, Erasmus school of law, 2022.

117. ***Ooggetuigenidentificaties: het verband tussen subjectieve zekerheid en accuraatheid. Een experimentele studie en her-analyse van bestaand onderzoek volgens Nederlandse confrontatieprotocollen***
M. Sauerland, N. Tupper, A.G. van Amelsvoort, Maastricht University 2022

118. ***Het fenomeen vechtafspraken: vier jaar later. Onderzoek naar de profielen van de deelnemers, kenmerken van de vechtgroepen en – nieuwe ontwikkelingen ten aanzien van – het fenomeen vechtafspraken***
J. Wolsink, H. Ferwerda, Bureau Beke, Arnhem 2022

119. ***Strip- en omkatfabrieken. Een fenomeenstudie als basis voor inzicht, awareness en aanpak***
H. Ferwerda, J. Wolsink, Bureau Beke, Arnhem 2022

120. ***Bestuurlijke rapportage bij sluitingen van drugspanden. Onderzoek naar het succesvol opstellen, aanbieden en opvolgen van bestuurlijke rapportages in artikel 13b Opiumwet-zaken***
L.M. Bruijn, R. Mennes, J.A. de Muijnck, M. Vols voor Breuer&Intraval en Rijksuniversiteit Groningen 2022

121. ***Mismatch. Een verkennend fenomeenonderzoek naar het plegen van zedendelicten na contact via een datingsite of datingapp***
J. Wolsink, J. Kuppens, N. Brouwer, H. Ferwerda, Bureau Beke, Arnhem 2023

122. ***Over een andere boeg. Lessen en uitdagingen in de integrale samenwerking tegen maritieme smokkel***
M. Boelens, D. de Rijk, Y. Eski, Boelens Onderzoek & Advies/Vrije Universiteit Amsterdam, 2023

123. ***Nieuwe tijden. Bijdrage van het bedrijfsleven aan de publieke opsporing***
E. Bervoets, J. Broekhuizen, K. van den Akker, m.m.v. Storm van Merkesteijn, Bureau Bervoets, 2024

124. ***De politieaanpak van sociale conflicten***
I. van Duijneveldt, S. Nafie, M. van Tooren, A. Visser, Andersson Elffers Felix, 2024

125. ***Bloemen op de begraafplaats. De aanpak van een complottheorie in Bodegraven. En wat we daarvan kunnen leren***
M. Eysink Smeets, H. Moors, L. de Veen, M. Koelink. Onderzoeksbureau EMMA en Onderzoeksbureau LEV, m.m.v. Hogeschool Inholland, gefinancierd door Onderzoeksprogramma Politie & Wetenschap, Politieacademie, 2025

126. ***Geklapt, gefilmd en gedeeld. Onderzoek naar hybride straatgeweld onder jongeren***
S. Mehlbaum, K. van den Akker, J. Broekhuizen, A. Verweij, m.m.v. Marloes van Lochem, 2025

127. ***Onderhandelen, betalen en melden na slachtofferschap van ransomware. Een mixed methods onderzoek naar de factoren die bijdragen aan beslissingsgedrag van burgers en ondernemers***
S. Matthijsse, S. van 't Hoff-de Goede, R. Leukfeldt. Halfweg, 2025

128. ***Bewegende beelden. Een onderzoek naar de meerwaarde van live video voor politiewerk***
S. Flight. Amsterdam, mei 2025

129. ***Conflictmanagement door collectieve inspanning. Een video-observatiestudie naar de samenwerking tussen stewards en politie tijdens het de-escaleren van conflicten op straat***
M. van Dalen, P. Ejbye-Ernst J. Thomas, M. van Bruchem, L. Suonperä Liebst, M. Rosenkrantz Lindegaard. Politie en Wetenschap, Amsterdam, mei 2025