

# Online doorpakken of doormodderen?

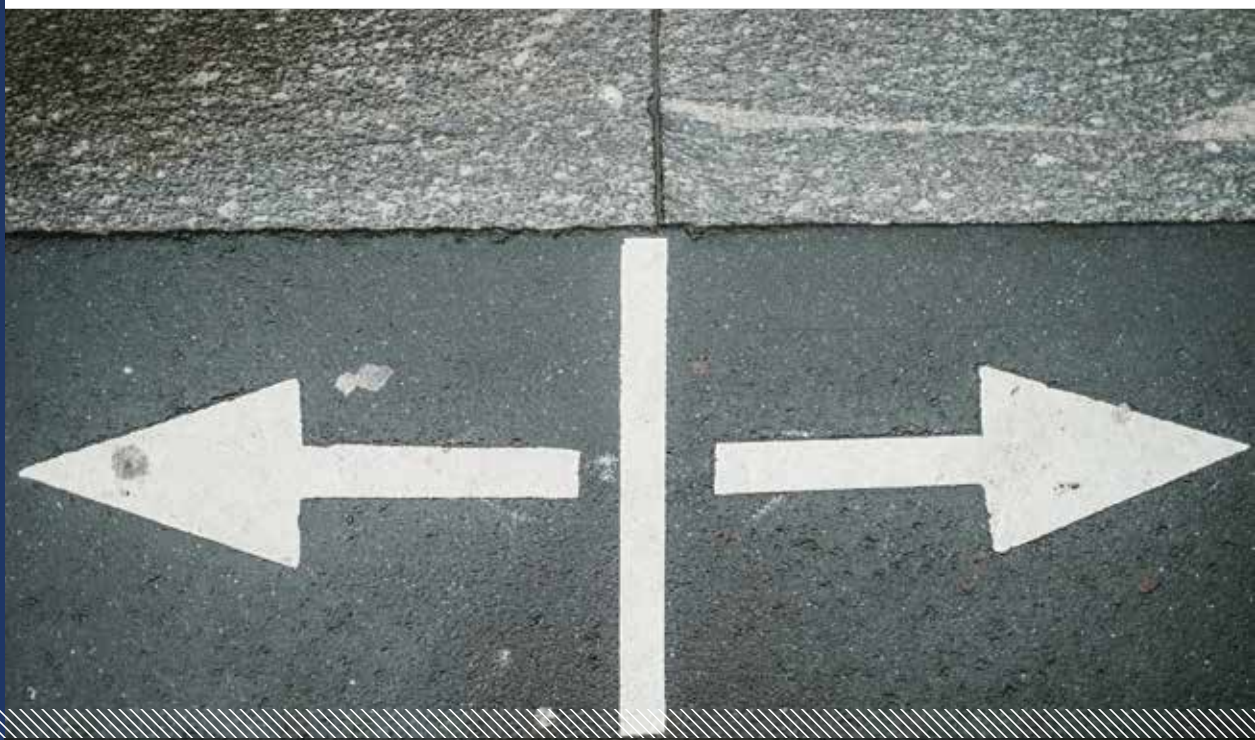
Saskia Westers

Nick van der Klok

Julia Klopman

Remco Spithoven

Jurjen Jansen



**Online doorpakken of doormodderen?**



# Online doorpakken of doormodderen?

Medewerkers van politiebasisteams over de lokale aanpak van online criminaliteit en de noodzaak tot sturing in de lokale, digitale transformatie

Saskia Westers MSc  
Nick van der Klok MSc  
Julia Klopman BA  
dr. Remco Spithoven  
dr. Jurjen Jansen

*juli 2026*

Lefebvre Sdu  
© 2026



Wetenschap



POLITIEACADEMIE



CYBER  
WEERBAAR  
NL

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:

Lefebvre Sdu Klantenservice

telefoon: 070 - 378 98 80

website: [www.sdu.nl/service](http://www.sdu.nl/service)

Omslagontwerp: Imago Mediabuilders

Afbeelding omslag: Claudio Schwarz via [Unsplash.com](https://unsplash.com)

ISBN: 9789012411615

NUR: 600, 680, 125

© 2026 Lefebvre Sdu, Den Haag; Politie & Wetenschap, Apeldoorn

Alle rechten voorbehouden. Behalve de door de Auteurswet gestelde uitzonderingen, mag niets uit deze uitgave worden vervoelvoudigd (waaronder begrepen het opslaan in een geautomatiseerd gegevensbestand) en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande schriftelijke toestemming van de uitgever.

De bij toepassing van art. 16h tot en met 16m Auteurswet wettelijk verschuldigde vergoedingen wegens kopiëren dienen te worden voldaan aan de Stichting Reprorecht ([www.reprorecht.nl](http://www.reprorecht.nl)). Voor het overnemen van een gedeelte van deze uitgave in bloemlezingen, readers en andere compilatiewerken op grond van art. 16 Auteurswet dient men zich te wenden tot de Stichting UvO ([www.stichting-uvo.nl](http://www.stichting-uvo.nl)). Voor het overnemen van een gedeelte van deze uitgave ten behoeve van commerciële doeleinden dient men zich te wenden tot de uitgever.

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, kan voor de afwezigheid van eventuele (druk)fouten en onvolledigheden niet worden ingestaan en aanvaarden auteur(s), redacteur(en) en uitgever deswege geen aansprakelijkheid voor de gevolgen van eventueel voorkomende fouten en onvolledigheden.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system of any nature, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

While every effort has been made to ensure the reliability of the information presented in this publication, Lefebvre Sdu neither guarantees the accuracy of the data contained herein nor accepts responsibility for errors or omissions or their consequences.

# Inhoudsopgave

**Samenvatting / 7**

**Afkortingenlijst / 11**

|          |                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b> | <b>Inleiding en theoretische verkenning / 13</b>                                                                                |
| 1.1      | Inleiding en aanleiding onderzoek / 13                                                                                          |
| 1.2      | Doelen en onderzoeksvragen / 15                                                                                                 |
| 1.3      | Theoretische verkenning lokale aanpak online criminaliteit / 16                                                                 |
| 1.4      | Leeswijzer / 26                                                                                                                 |
| <b>2</b> | <b>Onderzoeksdesign en -methoden / 29</b>                                                                                       |
| 2.1      | Literatuuronderzoek / 29                                                                                                        |
| 2.2      | Interviews basisteams / 30                                                                                                      |
| 2.3      | Vragenlijst / 31                                                                                                                |
| 2.4      | Ontwerponderzoek / 35                                                                                                           |
| 2.5      | Interviews intensivering / 36                                                                                                   |
| <b>3</b> | <b>Interviewresultaten basisteams / 39</b>                                                                                      |
| 3.1      | Achtergrondkenmerken van de geïnterviewde politiemensen / 39                                                                    |
| 3.2      | Perspectief op slachtofferschap, daderschap, prevalentie en de rol van het basisteam in de aanpak van online criminaliteit / 40 |
| 3.3      | Toewijzingskader / 43                                                                                                           |
| 3.4      | Huidige aanpak van online criminaliteit / 44                                                                                    |
| 3.5      | Teamontwikkeling / 46                                                                                                           |
| 3.6      | Behoeften in de lokale aanpak van online criminaliteit / 48                                                                     |
| <b>4</b> | <b>Vragenlijstresultaten basisteams / 55</b>                                                                                    |
| 4.1      | Werkzaamheden van respondenten / 55                                                                                             |
| 4.2      | Bekendheid met en de aanpak van online criminaliteitsvormen bij basisteams / 56                                                 |
| 4.3      | De lokale politietaak van online criminaliteit volgens respondenten / 64                                                        |
| 4.4      | Kennis en vaardigheden / 68                                                                                                     |
| 4.5      | Bevorderende en belemmerende factoren van interventies / 76                                                                     |

---

|                          |                                                                          |
|--------------------------|--------------------------------------------------------------------------|
| <b>5</b>                 | <b>Ontwerponderzoek: lokale interventies</b> / 79                        |
| 5.1                      | Interventieaanpak Postenveld / 79                                        |
| 5.2                      | Interventieaanpak Lichtblauwveen / 89                                    |
| <b>6</b>                 | <b>Interviewresultaten intensivering</b> / 95                            |
| 6.1                      | Inleiding / 95                                                           |
| 6.2                      | Landelijk en lokaal voorbij de lokale vrijblijvendheid sturen / 95       |
| 6.3                      | Conclusies en principes voor landelijke opschaling / 98                  |
| <b>7</b>                 | <b>Conclusies, discussie, beperkingen en aanbevelingen</b> / 103         |
| 7.1                      | Conclusie en discussie / 103                                             |
| 7.2                      | Reflectie op de rol van de onderzoekers / 111                            |
| 7.3                      | Beperkingen / 112                                                        |
| 7.4                      | Aanbevelingen voor de praktijk / 113                                     |
| 7.5                      | Aanbevelingen voor vervolgonderzoek / 117                                |
| <b>8</b>                 | <b>Epiloog: online doorpakken is geen keuze maar een noodzaak!</b> / 119 |
| <b>Referenties</b> / 125 |                                                                          |

## **BIJLAGEN**

**Bijlage 1 Beschrijving basisteams** / 135

**Bijlage 2 Interviewprotocol basisteams** / 139

**Bijlage 3 Codering van de basisteamsinterviews** / 145

**Bijlage 4 Vragenlijst politiebasisteams** / 149

**Bijlage 5 Interviewprotocol landelijke opschaling** / 163

**Bijlage 6 Experts over de principes voor de landelijke opschaling** / 169

**Bijlage 7 Toestemmingsverklaring** / 177

**Bijlage 8 Tijdlijn interventie-ontwikkeling** / 179

**Uitgaven in de reeks Politiekunde** / 181

## Samenvatting

Het werk van de politie is de afgelopen jaren aanzienlijk veranderd door de toename van online criminaliteit. Op nationaal niveau zijn het afgelopen decennium al belangrijke stappen gezet in de aanpak van (grootschalige en complexe) online delicten. De ambitie van de politie is om deze aanpak ook door te voeren naar lokaal niveau, waarbij basisteams een groeiende rol krijgen in de aanpak van (eenvoudige vormen van) online criminaliteit. Dit onderzoek richt zich op de vraag: *hoe kunnen basisteams van de politie hun personeel effectief voorbereiden op een intensivering van de lokale aanpak van online criminaliteit?*

### Bevindingen

Medewerkers van de basisteams zien online criminaliteit in de samenleving toenemen, maar hebben beperkt zicht op de omvang en vormen van online criminaliteit in hun eigen werkgebied. Daarentegen is de impact op slachtoffers op financieel, emotioneel en psychisch vlak voor hen inmiddels duidelijk zichtbaar.

In een ideale situatie zou de lokale aanpak van online criminaliteit door de basisteams neerkomen op het correct opnemen van aangiften, het bieden van nazorg en preventie voor slachtoffers om herhaald slachtofferschap te voorkomen en het uitvoeren van opsporing van kleinere, minder complexe zaken. Veel respondenten vinden dat de aanpak van gedigitaliseerde criminaliteit – zoals online fraude – bij medewerkers van de basisteams hoort, maar de aanpak van cybercrime – zoals hacken – bij specialistische teams ligt, zoals de Cybercrimeteams. Er zijn volgens medewerkers van de basisteams verschillende uitdagingen, waaronder capaciteitsproblemen, een lage motivatie om online criminaliteit aan te pakken en tekorten in kennis- en vaardigheden. Ook zijn er grote verschillen tussen medewerkers: sommigen zijn geïnteresseerd en deskundig terwijl anderen niets met online criminaliteit te maken willen hebben. Daarnaast stromen medewerkers met kennis van de aanpak van online criminaliteit vaak door naar andere teams, waardoor opgebouwde expertise op dit terrein verloren gaat.

Op dit moment richten basisteams zich vooral op nazorg door slachtoffers te helpen met het doen van aangifte en hen te adviseren om herhaald slachtofferschap van online criminaliteit te voorkomen. Daarnaast worden door basisteamedewerkers alternatieve interventies uitgevoerd, zoals stopgesprekken met geldezels. Opsporing en preventie worden volgens de respondenten minder gedaan dan gewenst. Alleen de incidentafhandeling doet incidenteel iets aan verstoring en preventie van daderschap van online criminaliteit. De basisteamedewerkers vinden dat opsporing, nazorg, verstoring, alternatieve interventies en preventie van online criminaliteit binnen de basis-

teams allemaal prioriteit moeten krijgen. Er is echter een groot verschil tussen wat medewerkers belangrijk vinden en wat in de praktijk daadwerkelijk wordt gedaan.

Medewerkers van de basisteams willen beter leren herkennen welke vormen van online criminaliteit er zijn en hoe zij digitale sporen kunnen veiligstellen. Daarbij ontbreekt het regelmatig aan juridische kennis, zoals bevoegdheden voor digitale opsporing. Daarnaast willen basisteammedewerkers meer ondersteuning van specialisten, zoals Cybercrimeteams, en betere afstemming met andere afdelingen binnen de nationale politie en politie-eenheden. Leerstrategieën die als effectief worden ervaren, zijn *learning by doing*, waarbij praktijkgerichte oefeningen met echte casuïstiek uit het eigen verzorgingsgebied worden uitgevoerd. Ook fysieke bijeenkomsten, waarbij in groepsverband wordt geleerd met ondersteuning van experts, werken volgens de medewerkers het best.

**Conclusie.** Medewerkers van de basisteams van de politie zien het belang van de lokale aanpak van online criminaliteit, maar ontberen kennis, vaardigheden en capaciteit om deze effectief uit te voeren. Verbetering vraagt daarom om helder landelijk beleid, duidelijke taakverdeling, heldere sturing, structurele opleiding en praktijkgerichte leerstrategieën. De verandering op lokaal niveau geleid door het lokaal management – moet geleidelijk zijn en worden afgestemd op de behoeften en capaciteiten van medewerkers.

### Aanbevelingen voor de praktijk

Deze resultaten leiden tot de volgende aanbevelingen voor de praktijk:

- Maak de aanpak van eenvoudige online criminaliteit verplicht voor basisteams, net als bij andere algemene politietaken, zoals de aanpak van georganiseerde misdaad. Vertaal landelijke doelstellingen naar lokale prioriteiten, ondanks bezuinigingen en capaciteitstekorten. Communiceer de urgentie duidelijk naar basisteams, bijvoorbeeld door lokale casuïstiek en slachtofferverhalen te delen. Ga daarbij het maken van moeilijke keuzes over welke werkzaamheden minder of niet meer worden gedaan niet uit de weg, en wees hierbij duidelijk en realistisch.
- Creëer bewustzijn van de aard en omvang van online criminaliteit in het eigen verzorgingsgebied, het herkennen van strafbare, online feiten en digitale sporen, het handelen op een plaats delict met digitale sporen en het veiligstellen daarvan. Daarnaast moeten medewerkers opsporingsonderzoeken voor eenvoudige zaken kunnen opstarten.
- Medewerkers van Intake & Service (I&S) moeten zich richten op het te woord staan en opnemen van kwalitatief goede aangiftes van slachtoffers. De incidentafhandeling fungeert intussen op basis van landelijk beleid (in potentie) als *first responder* voor slachtoffers door hen op te vangen, te adviseren, door te verwijzen en aangiften op te nemen. De recherche van de basisteams richt zich op opsporing van lokale daders van eenvoudige zaken van online criminaliteit en het ondersteunen van andere teams.
- Investeer in structurele opleidingen om operationele vaardigheden te versterken, zoals het veiligstellen van digitale sporen, het toepassen van juridische bevoegdheden

- 
- den en het bieden van hulp aan slachtoffers van online criminaliteit. Ondersteuning door digi-specialisten en Cybercrimeteams kan basisteams helpen met gerichte feedback en het begeleid opdoen van praktijkervaring. Leidinggevendenden moeten prioriteit geven aan deze lokale verandering, weerstand in hun team adresseren en ruimte voor medewerkers creëren voor leren tijdens werktijd. Daarvoor moeten echter eerst de kennis en betrokkenheid onder de leidinggevendenden van de basisteams bij de lokale aanpak van online criminaliteit worden vergroot.
- Zet in op de leerstrategie *learning by doing*. Verplichte, offline bijeenkomsten met lokale casuïstiek zijn naar inschatting van de respondenten en de wetenschappelijke literatuur het effectiefst. Hierbij moet rekening worden gehouden met functie-specifieke behoeften, zoals die van I&S, recherche, incidentafhandeling en leiding van de basisteams. *Early adopters*, gemotiveerde medewerkers voor de lokale aanpak van online criminaliteit, kunnen hun collega's meenemen in de verandering. Succesverhalen delen helpt daarbij om motivatie om online criminaliteit te verhogen en vertrouwen in de lokale aanpak van online criminaliteit te vergroten.
  - Versterk de samenwerking tussen basisteams, specialisten en externe partijen, zoals gemeenten en Regionale Informatie- en Expertisecentra (RIEC's). Vermijd een radicale omslag en bouw de nieuwe taken rondom de aanpak van online criminaliteit stapsgewijs op. Hiervoor is het cruciaal om voldoende tijd en ruimte vrij te maken om daadwerkelijk te kunnen samenwerken, aangezien het opbouwen van onderling vertrouwen tijd kost en essentieel is voor een effectieve samenwerking.

### **Vervolgonderzoek**

Er zijn verschillende mogelijkheden voor toekomstig onderzoek. Ten eerste kan onderzoek worden uitgevoerd naar de rol van leidinggevendenden en experts in de transitie van basisteams naar de aanpak van online criminaliteit, en wat hierin werkt en belemmert. Ten tweede kan longitudinaal onderzoek worden gedaan naar de vraag hoe basisteams zich over tijd ontwikkelen in de lokale aanpak van online criminaliteit. Ten derde kan ontwerponderzoek worden uitgevoerd waarbij een zelftest voor basisteams wordt ontwikkeld om aandachtspunten in kaart te brengen in de verandering naar de lokale aanpak van online criminaliteit. Ten slotte kan internationaal vergelijkend onderzoek worden gedaan naar de vraag hoe politiekorpsen in andere landen online criminaliteit lokaal aanpakken. Dit met als doel om inzichten te verkrijgen die kunnen bijdragen aan het verder verbeteren van de lokale aanpak.

### **Terugblik en positionering**

Na ruim dertig jaar onderzoek naar digitalisering en politiewerk blijkt dat veel politie-medewerkers in basisteams wel het belang inzien van het aanpakken van online criminaliteit, maar liever niet zelf actie ondernemen. Slechts een kleine groep zet zich hiervoor in, vaak ondanks weerstand van collega's en leidinggevendenden, terwijl online criminaliteit inmiddels een enorme omvang heeft bereikt: jaarlijks worden 2 tot 2,5 miljoen Nederlanders van vijftien jaar en ouder slachtoffer, met een impact die net zo groot of zelfs groter is dan die van traditionele criminaliteit. Ondanks communicatie

vanuit van de korps- en eenheidsleiding, beleid, doelstellingen en initiatieven om online criminaliteit prioriteit te geven, blijft de transformatie in de lokale praktijk steken. Redenen hiervoor zijn (ervaren) capaciteitsgebrek, weinig affiniteit met digitaal werk, onzekerheid in de uitvoering en een cultuur waarin 'echt politiewerk' nog steeds wordt geassocieerd met actie en straatwerk. Bovendien worden medewerkers met relatief sterke digitale vaardigheden afgeremd door collega's of leidinggevenden die vasthouden aan traditioneel politiewerk.

Een belangrijke oplossingsrichting is het stellen van duidelijke prioriteiten, een herverdeling van middelen en taken en het aannemen van professionals met specifieke expertise in data en complexe opsporing. In de basisteams moet er meer aandacht komen voor hulpverlening aan slachtoffers van online criminaliteit. De politie kan niet langer wachten: de samenleving en de criminaliteit zijn in hoge mate gedigitaliseerd en de politie moet meebewegen om haar legitimiteit en taakstelling – handhaven van de rechtsorde en hulp bieden – te waarborgen. Het is hoog tijd voor online doorpakken, zonder verder uitstel. Zo niet, dan blijft men doormodderen en blijft een effectieve aanpak van online criminaliteit uit.

## Afkortingenlijst

|         |                                                  |
|---------|--------------------------------------------------|
| BR      | Basisteamrecherche                               |
| BPZ     | Basis Politie Zorg                               |
| CCT     | Cybercrimeteam                                   |
| DCT     | Digicrime team                                   |
| DR      | Districtsrecherche                               |
| DRIO    | Dienst Regionale Intelligence Organisatie        |
| ECDO    | Expertisecentrum Cybercrime en Digitaal Opsporen |
| FO      | Forensische Opsporing                            |
| GGP     | Gebiedsgebonden Politie                          |
| HIC     | High Impact Crime                                |
| HOvJ    | Hulpofficier van Justitie                        |
| I&S     | Intake en Service                                |
| LOCO    | Landelijk Operationeel Cybercrime Overleg        |
| LMIO    | Landelijk Meldpunt Internet Oplichting           |
| LS      | Leiding en Sturing                               |
| NTCS    | Netwerktafel Crimineel Speelveld                 |
| OE      | Operationeel Expert                              |
| OCP     | Operationeel Coördinatie Politie                 |
| OpCo    | Operationeel Coördinator                         |
| OS      | Operationeel Specialist                          |
| OSINT   | Open Source INTelligence                         |
| OvD-P   | Officier van Dienst Politie                      |
| PIAC    | Programma Intensivering Aanpak Cybercrime        |
| RTIC    | Real Time Intelligence Centre                    |
| STO     | Senior Tactische Opsporing                       |
| Summ-IT | Politieregistratiesysteem in Nederland           |
| TDO     | Team Digitale Opsporing                          |

|      |                               |
|------|-------------------------------|
| THTC | Team High Tech Crime          |
| VAT  | Verdachte Afhandel Team       |
| VVC  | Veelvoorkomende Criminaliteit |
| WPG  | Wet Politie Gegevens          |

# 1 Inleiding en theoretische verkenning

In dit hoofdstuk starten we met de inleiding en aanleiding van het onderzoek (paragraaf 1.1). Daarna presenteren we de doelen en onderzoeksvragen (paragraaf 1.2). Vervolgens staan we stil bij de theoretische verkenning (paragraaf 1.3). Het hoofdstuk sluit af met een leeswijzer (paragraaf 1.4).

## 1.1 Inleiding en aanleiding onderzoek

Het werkaanbod van de Nederlandse politie is de afgelopen jaren ingrijpend veranderd. Naast het voortbestaan van de traditionele, offline criminaliteit, is daar een grote hoeveelheid online criminaliteit bijgekomen: in 2023 was 20% van de Nederlanders van vijftien jaar of ouder slachtoffer van traditionele criminaliteit en 16% van online criminaliteit (Akkermans et al., 2024). Criminelen kunnen met relatief weinig moeite en een lage pakkans online een enorme groep slachtoffers bereiken. Daar plegen zij naast relatief nieuwe vormen van criminaliteit (i.e., cybercrime, zoals *hacking* en DDoS-aanvallen) ook traditionele vormen van criminaliteit in een digitale vorm (i.e., gedigitaliseerde criminaliteit, zoals online bedrog en diefstal).

Hoewel doorgaans het beeld heerst dat online criminaliteit voornamelijk financiële schade veroorzaakt, is het probleem omvattender. Hoewel uit een eerder onderzoek (Leukfeldt, Notte & Malsch, 2018) bleek dat slachtoffers van online criminaliteit minder praktische behoeften hadden dan slachtoffers van traditionele criminaliteit, bleek uit een later onderzoek dat slachtoffers van online criminaliteit dezelfde behoefte aan praktische, financiële en emotionele ondersteuning hebben als slachtoffers van traditionele criminaliteit (Leukfeldt et al., 2020). Sterker nog, de impact van online delicten kan zelfs hoger zijn door het online karakter. Denk bijvoorbeeld aan intieme foto's die telkens weer opduiken, maar ook aan sporen van oplichters die duidelijk nog actief en zichtbaar zijn voor het slachtoffer. Online criminaliteit is dan ook allesbehalve slachtofferloos (Borwell et al., 2021a, b; Jansen & Leukfeldt, 2018; Leukfeldt et al., 2020).

Slachtoffers van online criminaliteit kunnen ook emotionele of psychische problemen ervaren, vooral in gevallen van cyberpesten, *stalking*, *phishing*, *shame sexting* en identiteitsfraude (Akkermans et al., 2024). Slachtoffers van online criminaliteit melden respectievelijk dat zij minder vertrouwen in andere mensen hebben, zich minder veilig voelen, het voorval steeds opnieuw beleven, slaapproblemen ervaren en daarnaast melden zij angst- en depressieve klachten (Arends et al., 2025). De effecten van slachtofferschap van online criminaliteit op de psychische en emotionele staat wordt ook gerapporteerd in het onderzoek van Borwell (2025).

Gezien de omvang en impact is het essentieel dat de politie, in samenwerking met partners, actie onderneemt om deze groeiende trend van online criminaliteit effectief aan te pakken. De Nederlandse politie heeft de afgelopen jaren dan ook forse stappen gezet om deze ontwikkelingen bij te benen. Naast het Team High Tech Crime (THTC), het Landelijk Meldpunt Internetoplichting (LMIO) en de komst van cybercrimeteams bij elke politie-eenheid zien we dat sinds een tijdje ook de basisteams in beweging komen. Zo bestaan er intussen digitale districten, digitaal wijkagenten, digitaal vrijwilligers en digitale taakaccenthouders door het hele land. Ook is vanuit De Digitale Meldkamer in Oost-Nederland intussen een landelijke werkwijze geïntroduceerd waarbij basisteams vanuit de noodhulp slachtoffers van online criminaliteit die daarvoor kiezen voorzien van emotionele steun, praktische hulp in het beperken van de impact. Ook geven ze advies hoe herhaald slachtofferschap kan worden voorkomen en worden aangiften bij slachtoffers thuis opgenomen (Spithoven et al., 2026; Van Amersfoort et al., 2025;).

De lokale, digitale politietaken lijkt vooralsnog echter een taak voor de ‘hobbyist’ of ‘liefhebber’ (Spithoven & Leukfeldt, 2023; Terpstra et al., 2021), terwijl de omvang van online criminaliteit zou legitimeren om deze vorm van criminaliteit ook op lokaal niveau intussen als gemeengoed te bestempelen (Jansen, 2025; Kort & Spithoven, 2022; 2021; Leukfeldt et al., 2020; Spithoven et al., 2022). Dat is de volgende stap binnen de aanpassing van de politieorganisatie aan de steeds verder digitaliserende omgeving en het digitale werkaanbod: ‘lokaal digitaal’.

Onderzoekers zien als lokale politietaken aangaande online criminaliteit op lokaal niveau vooral om het bewustzijn van de aard en omvang van online criminaliteit onder doelgroepen te vergroten en het kennen, weten te herkennen en benoemen van de strafbaarstelling van specifieke delicten. Daarnaast moet men weten hoe op te treden op een plaats delict, moet men met aangedragen informatie om kunnen gaan en een opsporingsonderzoek op basis van de daarvoor geldende eisen kunnen uitvoeren voor online criminaliteit (Boekhoorn, 2020; Huisman et al., 2016; Jansen et al., 2020; Kort & Spithoven, 2021; Leukfeldt et al., 2012; POR, 2020; Schiks et al., 2022). In sommige eenheden wordt ‘blauw’ ook belast met het opnemen van meldingen en aangiften op het bureau (Jansen et al., 2020).

Er lijkt een belangrijke hindernis te zitten op lokaal niveau als het gaat over de motivatie van personeel rondom de digitalisering en de aanpak van online criminaliteit. Deze bottleneck wordt vaak aangeduid met de term ‘koudwatervrees’ (Ruiter et al., 2023; Spithoven & Leukfeldt, 2023). Dit is een belangrijke uitdaging die moet worden overwonnen, aangezien het onoverkomelijk is dat digitale zaken bij de basisteams terechtkomen. Naast het vergroten van bewustzijn over online criminaliteit, is het daarom cruciaal om hier in de uitvoering van het lokale politiewerk daadwerkelijk prioriteit aan te geven en actie te ondernemen.

Conform het Toewijzingskader Cybercrime van de toenmalige Portefeuille Digitalisering & Cybercrime (2023), richt dit onderzoek zich op taken van politiebasteams met betrekking tot lokale problematiek. Daarbij gaat het om het aanpakken van eenvoudige zaken met een lage complexiteit. Deze zaken bevatten voldoende opsporingsindi-

caties en een lage politieke gevoeligheid. Het gaat dan bijvoorbeeld om het aanpakken van geldezels, *sextortion* (zonder letsel of dood) en cyberpesten. Maar ook om eenvoudige vormen van online criminaliteit, zoals *hacking* in de relationele sfeer of op een lokale school, DDoS-aanvallen met bekende dader(s) en diefstal van gegevens in dienstbetrekking (Politie, 2023).

De hiervoor genoemde, noodzakelijke verandering binnen de basisteams van de politie-eenheden zal niet zonder slag of stoot gaan. In huidige, lokale initiatieven rondom online criminaliteit lopen de betrokken politiemensen namelijk tegen stevige grenzen aan. Naast de ervaren werkdruk, ervaren zij die grenzen vooral op het gebied van kennis en vaardigheden. Bovendien is het lastig voor politiemensen om constante ontwikkelingen en de snelheid van deze ontwikkelingen bij te benen (Hadlington et al., 2021). Ook is het nog maar de vraag in hoeverre medewerkers van basisteams zich deze nieuwe taken eigen *willen* maken (Spithoven et al., 2026). Dit onderzoek helpt om die uitdagingen aan te gaan.

In dit praktijkgerichte ontwerponderzoek slaan twee samenwerkende hogescholen de handen ineen met twee basisteams van de eenheden Oost- en Noord-Nederland, het Cybercrimeteam van de eenheid Oost-Nederland, een Digitaal Platform uit Noord-Nederland, de Portefeuille Digitalisering & Cybercrime (2023) en de Portefeuille Gebiedsgebonden Politie. Er is immers zowel behoefte aan kennis als aan verbetering van de praktijk (Van den Berg & Kouwenhoven, 2008; Van Turnhout, Andriessen & Cremers, 2023). De samenwerkende organisaties geven samen vorm aan een intensivering van de lokale, digitale politietaak. De onderzoekers en professionals van de twee politie-eenheden gaan met dit onderzoek gezamenlijk op expeditie: lokaal digitaal.

## 1.2 Doelen en onderzoeksvragen

Het doel van dit ontwerponderzoek is om inzicht te bieden in hoe basisteams hun personeel effectief kunnen voorbereiden op de intensivering van de lokale aanpak van online criminaliteit en handvatten te ontwikkelen voor toepassing in de politiepraktijk. De hoofdvraag bij dit onderzoek luidt dan ook: *Hoe kunnen basisteams van de politie hun personeel effectief voorbereiden op een intensivering van de lokale aanpak van online criminaliteit?*

Om deze hoofdvraag te beantwoorden, zijn de volgende deelvragen geformuleerd:

1. Hoe percipiëren politiemensen van de basisteams de lokale taak, waar liggen wat hen betreft de zwaartepunten in de aanpak van online criminaliteit en wat hebben zij aan kennis en vaardigheden nodig om invulling aan deze taak te geven?
2. Hoe pakken basisteammedewerkers online criminaliteit momenteel in de praktijk aan?
3. Wat kan er middels interventies worden gedaan om de lokale aanpak van online criminaliteit te intensiveren (of hierop voor te bereiden) en op welke wijze kan dat effectief?

4. Hoe wordt de ontwikkelde interventie door deelnemers ervaren en wat zijn de effecten ervan in de praktijk?
5. Hoe kan de aanpak van online criminaliteit door medewerkers van de basisteams worden geïntensiveerd?

### 1.3 Theoretische verkenning lokale aanpak online criminaliteit

In deze paragraaf gaan we achtereenvolgens in op digitalisering en online criminaliteit, de rol van basisteams in een digitaliserende samenleving, de lokale aanpak van online criminaliteit door basisteams en kennis en vaardigheden omtrent lokaal politiewerk en de aanpak van online criminaliteit. Ten slotte staan we stil bij de inzichten uit de internationale literatuur.

#### Digitalisering en online criminaliteit

De toename van online criminaliteit is goed te begrijpen wanneer we kijken naar veranderingen in gelegenheidsstructuren voor criminaliteit. In de fysieke wereld heeft met name verbeterde beveiliging geleid tot een afname van criminaliteit. In de online wereld nam de gelegenheid daarentegen enorm toe, omdat vrijwel elke burger en organisatie online actief is, zich onvoldoende bewust is van de risico's die zij daar lopen en overheden nog grotendeels zoekende zijn naar hun rol in het tegengaan van online criminaliteit (Jansen, 2025; Leukfeldt, 2016; Spithoven, 2020; Yar, 2005).

Daarmee is het niet verrassend dat daders op zoek gaan naar online kansen om hun oude vormen van criminaliteit in de vorm van onder andere oplichting en geweld uit te voeren. Maar er zijn ook nieuwe vormen van criminaliteit ontstaan, zoals *malware*, DDoS-aanvallen en *hacking*. In de Nederlandstalige literatuur wordt daarbij onderscheid gemaakt tussen gedigitaliseerde criminaliteit en cybercriminaliteit. Deze worden in de internationale literatuur respectievelijk aangeduid als *cyber-enabled crime* en *cyber-dependent crime*. Gedigitaliseerde criminaliteit is een vorm van criminaliteit dat met digitale middelen wordt gefaciliteerd, zoals online fraude of bedreiging via sociale media. Cybercriminaliteit zijn misdrijven die zowel met een digitaal middel worden uitgevoerd én een digitaal doelwit hebben, zoals *hacking* en DDoS-aanvallen. Deze twee vormen tezamen noemen wij online criminaliteit. Spithoven vat dit geheel al eerder samen in een illustratieve taxonomie (zie figuur 1.1).



Figuur 1.1 Taxonomie van online criminaliteit (Spithoven, 2020, p. 49)

### Rol van basisteams in een digitale samenleving

Hoewel online criminaliteit veelal wordt gezien als een grensoverschrijdend probleem dat vraagt om nationale of zelfs internationale samenwerking, is een sterke lokale aanpak voor met name gedigitaliseerde criminaliteit en eenvoudigere vormen van hacking en DDoS-aanvallen essentieel voor een effectief veiligheidsbeleid. Naast het Team High Tech Crime (THTC), dat zich intussen ongeveer twintig jaar richt op nationale en internationale cybercrime, werd na het Programma Aanpak Cybercrime (PAC) dat startte in 2008, het Programma Intensivering Aanpak Cybercrime (PIAC) in 2016 gelanceerd om regionale achterstanden in de bestrijding van online criminaliteit aan te pakken. Dit politieprogramma richt zich op het opzetten van regionale cybercrime-teams en flexibele eenheden die zich specifiek bezighouden met het bestrijden van online criminaliteit binnen hun eigen regio's (Boekhoorn, 2020).

De politie worstelt al sinds de jaren negentig met de vraag hoe zij online criminaliteit tegen moet gaan. Een constante factor blijft een gebrek aan kennis en vaardigheden op de algemene politiemedewerker. Daarbij wordt van tijd tot tijd gewisseld van strategie tussen een benadering waarin dit vooral aan de specialisten is en een breedtebenadering waarin dit een taak van elke politiemedewerker betreft. Deze laatste wint de afgelopen jaren weer aan terrein. Deze aanpak waarin ook reguliere politiemensen opgeleid worden in digitale vaardigheden zou ervoor zorgen dat kennis over online criminaliteit zich verspreidt door de hele organisatie. Dit zou leiden tot een meer alom-

vattende aanpak waarbij basisteams voldoende uitgerust zouden zijn om online criminaliteit te bestrijden en minder afhankelijk worden van gespecialiseerde afdelingen. Gedurende de start van dit onderzoeksproject (in 2024) zijn de taken van de basisteams van lokale of familiale problematiek met een bekende dader beleidsmatig in concept vastgelegd in het Toewijzingskader Cybercrime van de (toenmalige) Portefeuille Digitalisering & Cybercrime van de politie (2023).

Ook in het buitenland wordt het belang van een lokale aanpak van online criminaliteit steeds vaker als potentieel waardevol erkend (Brunner, 2020; Hadlington et al., 2021; Holt & Bossler, 2012; Hull et al., 2018). Collier en collega's (2020) benadrukken dat lokale politieteams met haar partners, dankzij hun sterke banden met de gemeenschap en diepgaande kennis van lokale problematiek, de regie moeten voeren in de preventie van potentiële slachtoffers en daders. In deze publiek-private samenwerking moet duidelijk zijn waar de politie en haar partners verantwoordelijk voor zijn en wie welk onderdeel van de lokale aanpak aanjaagt (Spithoven et al., 2022).

Het belang van deze samenwerking tussen veiligheidspartners komt ook terug in het Nederlandse raamwerk voor de lokale aanpak van cybercriminaliteit (Leukfeldt et al., 2020). Dit raamwerk bestaat uit slachtofferpreventie, het stimuleren van het doen van aangifte, versterking van de informatiepositie, monitoring van lokale trends en het opsporen en het frustreren van dader(groepen) en daderpreventie. In deze samenwerking vormt de politie en samen met het Openbaar Ministerie de kern voor de opsporing. Kort en Spithoven (2022) hebben de taken voor de lokale aanpak van online criminaliteit verdeeld voor verschillende rollen (tabel 1.1). Ook hierin komen voorheen benoemde taken zoals signaleren, preventie, samenwerking met partners, opsporing en frustreren van dadergroepen naar voren.

Tabel 1.1 Contouren van de lokale, digitale politietaak (Kort & Spithoven, 2022, p. 115)

| Intake en service                                 | Wijkwerk                                                                                                                                | Interventie                                                                                                                          | Veelvoorkomende criminaliteit                                                | Ondersteunen opsporing                                                                                                                                                                  |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Signaleren van lokaal slachtoffer- en daderschap. | Signaleren van lokaal actieve daders, dadergroepen en criminele netwerken. Lokaal agenderen en tot integrale, preventieve aanpak komen. | Samenwerken met partnerorganisaties bij preventieve activiteiten. Gezamenlijk voeren van stopgesprekken met <i>first offenders</i> . | Opsporen van lokaal actieve daders en eenvoudig te onderkennen dadergroepen. | Andere organisatieonderdelen ondersteunen met advies en lokale kennis ten aanzien van lokale daders, dadergroepen of criminele netwerken en ondersteunen bij het aanhouden en verhoren. |

Tegelijkertijd kent de lokale aanpak van online criminaliteit diverse uitdagingen. Veel eenheden kampen met capaciteitsproblemen, waardoor zij onvoldoende middelen en personeel hebben om deze criminaliteit effectief aan te pakken (Boekhoorn, 2020). Dit vergroot de afhankelijkheid van nationale en internationale teams en ondermijnt de effectiviteit van de aanpak. Lokale teams moeten met beperkte middelen opereren binnen structuren die hierop niet zijn afgestemd. Het blijft een uitdaging om op zowel

lokaal als nationaal niveau voldoende capaciteit vrij te maken voor een effectieve aanpak.

### **Lokale aanpak van online criminaliteit door basisteams**

Een basisteam heeft als functie om aangiften en meldingen op te nemen, signalen op te vangen in het werkgebied en (digitale) sporen veilig te stellen (Leukfeldt et al., 2012; 2013; Toutenhoofd-Visser et al., 2009). De aanpak van online criminaliteit op lokaal niveau heeft diverse uitdagingen, die met name zichtbaar worden in het opsporingsproces bij basisteams. Dit proces kan in vijf fasen worden ingedeeld waarbij naast de I) intake, II) casescreeening (beoordelen input) en III) voorbereiding, ook de IV) uitvoering van het opsporingsonderzoek en V) afronding plaatsvinden (Jansen et al., 2020). Elk van deze fasen kent specifieke knelpunten wanneer het gaat om de aanpak van online criminaliteit.

De wijze waarop de intake, het opnemen van meldingen of aangiften, is georganiseerd verschilt per eenheid (Jansen et al., 2020). Het overgrote deel van de intakewerkzaamheden wordt uitgevoerd door speciaal aangestelde medewerkers Intake en Service (I&S). De politiemensen in uniformdienst (blauw) doen de intake op locatie, bijvoorbeeld naar aanleiding van een melding op straat of bijvoorbeeld per telefoon via het OC. In sommige eenheden worden ook politiemensen in blauw belast met het op bureau opnemen van meldingen en aangiften. Als de aard en complexiteit van de aangifte daarom vragen, dan kunnen specialisten worden betrokken om te ondersteunen bij het opnemen van aangiften.

De intake vormt het startpunt van het opsporingsproces, maar in de praktijk blijkt dat aangiften van online criminaliteit niet altijd worden opgenomen, wanneer slachtoffers zich bij de politie melden (Ruiter et al., 2023). Dit lijkt deels te wijten aan onvoldoende kennis van online criminaliteit onder intake medewerkers (Boekhoorn, 2020; Van Steden et al., 2025). Aangezien een kwalitatief hoogwaardige aangifte van cruciaal belang is voor de verdere strafrechtelijke behandeling, wordt in de literatuur benadrukt dat intake medewerkers van de politie beter moeten worden toegerust (Ruiter et al., 2023). Het geautomatiseerde aangifteproces, zoals beschikbaar via de website van de politie, biedt ook kansen voor verbetering, omdat het een gerichter doorvragen mogelijk maakt (Ruiter et al., 2023).

Na de intake volgt de casescreeening, een fase waarin politiezaken worden beoordeeld op hun prioriteit en opsporingsindicatie. Onderzoek naar de screening van online criminaliteitszaken is schaars, maar de beschikbare data suggereren dat deze zaken in de praktijk minder snel worden opgepakt dan traditionele misdrijven (Ruiter et al., 2023). Ook blijkt een inadequate opvolging van aangiften te leiden tot onterechte afwijzingen tijdens de casescreeening (Boekhoorn, 2020).

Mogelijke oorzaken hiervan zijn de vermeende complexiteit van online zaken, het internationale karakter ervan, een gebrek aan capaciteit binnen de politieorganisatie en gebrekkige kwaliteit van de opgenomen aangiften (Ruiter et al., 2023). Boekhoorn (2020) voegt daar een beperkte informatiepositie met betrekking tot online delicten aan toe. Bovendien geven interviews met politiepersoneel in het onderzoek van Ruiter

en collega's (2023) aan dat er vaak geen duidelijke opsporingsindicatie in de aangifte is en dat het ontbreken van een directe verdachte de opsporing belemmert. Om een verdachte in beeld te brengen moeten namelijk – meer dan bij traditionele criminaliteit –, OC worden gecombineerd en aanvullende data worden opgevraagd om tot een verdachte te kunnen komen. Ook kan de eerdergenoemde 'digitale koudwatervrees' – een lage motivatie om deze zaken aan te pakken – een oorzaak zijn van de tegenvallende aantallen zaken rond online criminaliteit. Het uitvoerende personeel mist naar eigen gevoel de benodigde kennis en vaardigheden om de eerste stap te zetten om online criminaliteitszaken op te pakken (Spithoven & Leukfeldt, 2023).

Op basisteamniveau richt de opsporing zich voornamelijk op kleinschalige en minder complexe zaken van online criminaliteit (Jansen et al., 2020). De basisteamrecherche (BR) houdt zich bezig met zowel traditionele misdrijven (met of zonder digitale component) als met online criminaliteitsonderzoeken. Digitale kennis is echter niet alleen van belang bij online criminaliteit; ook bij traditionele misdrijven speelt de aanwezigheid van digitale sporen een steeds grotere rol, aangezien ieder delict digitale sporen kan bevatten (Zuurveen & Stol, 2020).

De opsporing van online criminaliteit wordt bemoeilijkt door vier belangrijke knelpunten (Ruiter et al., 2023). Er is ten eerste een gebrek aan prioriteit. Binnen politieorganisaties krijgt online criminaliteit vaak minder aandacht. Dit komt deels doordat de complexiteit van dergelijke zaken niet altijd goed wordt ingeschat en de gevolgen voor het slachtoffer van online criminaliteit onvoldoende worden erkend. Het tweede knelpunt in de opsporing van online criminaliteit is de complexiteit. Het internationale karakter en de vluchtigheid van digitale gegevens maken het opsporingsproces ingewikkeld. Verdachten bevinden zich mogelijk buiten de landsgrenzen en digitale sporen kunnen snel verdwijnen, waardoor het verzamelen van bewijs een race tegen de klok is. Het laatste knelpunt, dat tevens de focus van dit onderzoek vormt, betreft een tekort aan kennis en vaardigheden binnen de politieorganisatie (Jansen et al., 2020; Jansen, 2025; Ruiter et al., 2023; POR, 2020). Dit gebrek aan kennis en vaardigheden belemmert de effectieve uitvoering van opsporingsonderzoeken met een digitaal component. Vooral cybercrimezaken vragen digitale kennis waardoor deze zaken zelden op basisteamniveau worden afgehandeld (Jansen et al., 2020).

Een gebrek aan kennis en capaciteit is ook een belemmering in het gebruiken van digitale sporen door politiemensen (Zuurveen & Stol, 2020). Hoewel binnen de politieorganisatie gespecialiseerde teams bestaan die hun collega's kunnen ondersteunen bij het veiligstellen en analyseren van digitale sporen, worden deze teams vanwege een gebrek aan kennis en bewustzijn weinig benaderd (Zuurveen & Stol, 2020). De kloof tussen de basisteams en meer specialistische afdelingen lijkt groot te zijn (Terpstra et al., 2021). De politiemensen in basisteams ervaren dat door specialisten verzamelde informatie slechts in beperkte mate relevant is voor de lokale aanpak van criminaliteit en dat gedegen analyses ontbreken. Dat leidt ertoe dat men vanuit basisteams zelf probeert aan deze informatie te komen, waar dan vaak deskundigheid en middelen voor ontbreken. In de huidige situatie is een basisteam afhankelijk van intrinsiek gemotiveerde aanjagers op het gebied van online criminaliteit (Terpstra et al., 2021; Van Steden et al.,

2025). Zoals Terpstra en zijn collega's beschrijven (2021, p. 57): *'De deskundigheid van het basisteam op het gebied van digitalisering hangt echter nog in grote mate af van "hobbyisme" van een aantal teamleden.'* Het basisteam wordt kwetsbaar wanneer de aanpak van online criminaliteit afhangt van individuele hobbyisten omdat hun vertrek kan leiden tot het verlies van cruciale kennis en vaardigheden (Terpstra et al., 2021). Terpstra en collega's stellen dat er binnen basisteams minder vrijblijvendheid moet zijn over wie de digitalisering oppakt. De focus zou moeten liggen op een gezamenlijke ontwikkeling – een 'gemeenschappelijke voorraad van kennis, ervaringen en modellen' – die als structurele basis dient voor het basisteam.

Ook Van Steden en collega's (2025) benadrukken dat meer en eenduidige sturing op de aanpak van online criminaliteit dringend nodig is, met specifieke aandacht voor de ondersteuning van basisteams. Zij pleiten voor een stevigere en consistentere inbedding van gebiedsgebonden politiezorg binnen deze aanpak. Dit vraagt niet alleen om een duidelijke visie en beleid rond 'online blauw werk', maar ook om passende organisatie, middelen, ondersteuning, hulplijnen, opleidingen en capaciteit. Het is voor basisteams ondoenlijk om deze aanpak enkel zelfstandig te organiseren.

### **Kennis en vaardigheden op het gebied van online criminaliteit**

Politiewerk in een gedigitaliseerde samenleving vereist voortdurende aanpassing, met name op het gebied van digitale kennis en vaardigheden. Dit betekent dat politiemensen in de digitale samenleving een breed scala aan kennis en vaardigheden moeten beheersen. Tot op heden hebben twee onderzoeken specifiek bijgedragen aan het vaststellen van kennisnormen voor politiemensen, die in de volgende paragrafen worden toegelicht.

In het onderzoek *Level-Up!* (Jansen et al., 2020) zijn kennisnormen voor digitale aspecten van politiewerk vastgesteld voor verschillende groepen politiemensen, waarbij specifieke eisen zijn opgesteld per functie binnen het basisteam. In deze kennisnormen kunnen klassiek en digitaal politiewerk niet los van elkaar worden gezien; digitale aspecten zijn (grotendeels) geïntegreerd in het reguliere politieproces. In dat onderzoek is op het niveau van basisteams onderscheid gemaakt tussen drie groepen: I) I&S, II) politiemensen in uniform (blauw/incidentafhandeling) en de III) basisteamrecherche. Voor elk van deze groepen zijn specifieke kennisnormen vastgelegd.

Voor medewerkers I&S zijn de belangrijkste competenties als volgt. Zij moeten de standaardprocedure voor het opnemen van aangiften kennen en in staat zijn om verschillende vormen van online criminaliteit te herkennen op basis van signalen uit de praktijk. Daarnaast moeten zij de strafbaarstelling van cyberdelicten, zoals hacken en online fraude, kunnen identificeren. Zij moeten ook weten hoe zij verbanden tussen verschillende cyberdelicten kunnen herkennen en toetsen tijdens het aangifteproces. Verder dienen deze medewerkers inzicht te hebben in het verzamelen van digitale sporen die relevant zijn voor opsporing en moeten zij advies kunnen geven over hoe deze sporen veiliggesteld kunnen worden. Ook is het van belang dat zij op de hoogte zijn van richtlijnen die specifiek ontwikkeld zijn voor de intake van cybergerelateerde zaken. Op basis hiervan moeten zij de aangever of melder kunnen adviseren over preven-

tieve maatregelen om eventueel herhaald slachtofferschap te voorkomen of vervolgstappen naar aanleiding van het slachtofferschap te zetten om eventuele schade te beperken.

Voor politiemensen in uniformdienst zijn ook verschillende digitale competenties vereist. Zij moeten de verschillende fasen van het optreden op de plaats delict (PD) kennen, evenals het bijbehorende juridische kader. Daarnaast moeten zij de eerste maatregelen bij een incident begrijpen en kunnen uitvoeren en weten hoe zij een onderzoek op de PD moeten starten. Bij situaties waarin digitale sporen mogelijk aanwezig zijn, is het belangrijk dat deze medewerkers de basisstappen voor het omgaan met digitale sporen kennen. Zij moeten in staat zijn om relevante digitale gegevensdragers te herkennen en op een forensisch verantwoorde manier veilig te stellen. Ook het onderzoek in de directe omgeving van de PD moet volgens protocollen uitgevoerd kunnen worden. Ten slotte is kennis van communicatie met burgers via het internet voor deze groep politiemensen van belang.

Voor medewerkers van de BR zijn de competenties meer gericht op opsporing en onderzoek. Deze politiemensen moeten diverse vormen van digitale criminaliteit kunnen herkennen aan de hand van signalen uit de praktijk en weten hoe zij moeten optreden op en rondom de plaats delict. Bij het ontvangen van informatie, bijvoorbeeld via een aangifte of intelligence, moeten zij in staat zijn de waarde ervan voor het opsporingsonderzoek te beoordelen. Daarnaast is het belangrijk dat zij systematisch en planmatig te werk kunnen gaan in opsporingsonderzoeken. Ook zijn specifieke opsporingsvaardigheden van belang, zoals het gebruik van digitale sporen van gegevensdragers en het vorderen van digitale gegevens. Hoewel interceptiemogelijkheden voorbehouden zijn aan de recherche op districtsniveau of hoger, is kennis van deze opsporingsmethoden wel essentieel. Verder moeten rechercheurs onderzoeksbevindingen kunnen analyseren en interpreteren, de waarde van bewijs kunnen beoordelen, en hun eigen onderzoekshandelingen nauwkeurig vastleggen.

Voor alle politiemensen, ongeacht hun functie, zijn er enkele algemene competenties op het gebied van informatievergaring op het internet. Dit omvat kennis van digitale sporen, relevante juridische kaders, monitoring en identificatie, het gebruik van tools zoals zoekmachines, en inzicht in verschillende bronnen en het jargon of de thema's die hierbij een rol spelen.

Deze kennisnormen zijn door Jansen en collega's (2020) getest onder 402 politiemensen, waarbij onderscheid werd gemaakt tussen hoge en lage scores ten opzichte van het gemiddelde. Uit dit onderzoek bleek dat de kennis en het vermogen om strafbare gedragingen op het gebied van digitale criminaliteit te herkennen onvoldoende zijn. Daarnaast werd een tekort aan kennis vastgesteld met betrekking tot de risico's van het verliezen, vernietigen of besmetten van digitale sporen en de basisprocedures voor het veiligstellen van digitale gegevensdragers. Ook het prioriteren van gegevensdragers die als eerste veiliggesteld moeten worden, scoorde ondermaats. Daarentegen was de kennis over algemene handelingen op een plaats delict (PD) en de bewijsvoering relatief hoog. Bij onbekende gegevensdragers wordt vaak een specialist geraadpleegd om deze te identificeren.

Verder werden algemene digitale termen goed herkend, maar was de kennis over specifieke termen zoals het *clear web* en *deep web* beperkt. Hoewel de kennis over interpretatie hoog bleek, was het gebruik van beschikbare digitale hulpmiddelen laag. Binnen het subthema ‘vorderen van gegevens’ bleek er beperkte bekendheid te zijn met OSINT (Open Source INtelligence),<sup>1</sup> Intel en de verantwoordelijkheden rondom informatievergaring op het internet. De geïnterviewden scoorden laag op kennis over geavanceerde zoektermen, zoekoperatoren en geschikte internetbronnen, maar redelijk hoog wat betreft het gebruik van tools voor informatiezoekopdrachten. Ten slotte bleek dat er beperkte kennis was over welke internettoepassingen burgers gebruiken en welke toepassingen geschikt zijn voor communicatie met burgers. Hoewel de kennis over aangiften van online criminaliteit in het algemeen hoog was, ontbrak het politiemensen aan voldoende inzicht in welke sporen bij deze aangiften kunnen worden geïnventariseerd. En vorenstaande was de situatie voordat Artificiële Intelligentie (AI) haar algemene intrede deed in de samenleving.

In het onderzoek van de Politieonderwijsraad (2020) zijn algemene richtlijnen vastgesteld voor de kennis, vaardigheden en attitudes die gelden voor politiemensen in een basisteam. Allereerst is een goed begrip van het internet en de verschillende online communicatiemiddelen, platforms en sociale media gevraagd. Daarnaast moeten zij goed thuis zijn in het gebruik van digitale tools en smartphones, aangezien deze apparaten een grote rol spelen in politiewerk en de samenleving.

Naast deze kennis over digitale mogelijkheden is het belangrijk dat politiemensen in een basisteam zich bewust zijn van de juridische en ethische kaders rondom digitalisering. Hun handelingen in de digitale wereld worden nauwlettend gevolgd, vergelijkbaar met het werken in een ‘glazen kooi’. Dit vraagt om een zorgvuldige en verantwoorde omgang met digitale gegevens en situaties. Ook leergierigheid en het vermogen om zich voortdurend te blijven ontwikkelen zijn cruciaal, juist omdat de digitale wereld zo snel verandert. Politiemensen moeten bereid zijn om fouten te maken en daarvan te leren, maar ook om hulp of uitleg te vragen wanneer dat nodig is. Deze open houding maakt het mogelijk om zowel online als offline aspecten effectief te combineren in hun werk.

Daarnaast moeten politiemensen in een basisteam in staat zijn om de betrouwbaarheid van bronnen en informatie te verifiëren. Dit is van groot belang bij het verwerken van digitale informatie, die zij vervolgens moeten kunnen vertalen naar praktische politiehandelingen en andersom. Zij moeten (vak)kennis en vaardigheden hebben als het gaat over digitaal bewijsmateriaal. Het kunnen herkennen en veiligstellen van relevante digitale sporen is een belangrijke vaardigheid om te beheersen.

Tot slot is (vak)kennis van veelvoorkomende fenomenen zoals verkoopfraude, sexting, ransomware, cyberstalking en identiteitsfraude noodzakelijk. Bovendien moeten zij vertrouwd zijn met het veiligstellen en analyseren van digitaal bewijsmateriaal. Deze

---

1 OSINT in politiewerk is het verzamelen en analyseren van openbaar toegankelijke informatie, zoals sociale media, nieuwsbronnen en fora.

benoemde kennis, vaardigheden en houding helpen politiemensen om effectief en verantwoord op te treden in een steeds digitaal wordende samenleving.

### Inzichten uit de internationale literatuur

‘Digitaal’ is ook volgens de internationale, wetenschappelijke politieliteratuur de nieuwe frontlinie van criminaliteit geworden (Forouzan et al., 2018; Hitchcock et al., 2017; Wall, 2007). Het tegengaan van online criminaliteit is ‘*a mainstream area of police work*’ geworden (Lee et al., 2025, p. 8) omdat burgers en bedrijven op grote schaal door online criminaliteit worden geraakt (McNealey et al., 2025; Shandler & Gomez, 2023). Bij de meeste zaken rond online criminaliteit is de lokale politie – naast dat mensen hun bank bellen bij het ontdekken van slachtofferschap – als *first responder* aanwezig (Bossler & Holt, 2012; Cross, 2020, 2018; Cross et al., 2021; Hadlington et al., 2021; Lee et al., 2025; Schreuders et al., 2020; Wilson et al., 2022). Om deze rol als *first responders* op zich te nemen hebben lokale, uitvoerende politiemensen basiskennis nodig over online criminaliteit (zie ook Stol, Leukfeldt & Klap, 2013).

Naast het beschikken over basiskennis, moeten zij volgens de internationale literatuur in hun rol als *first responders* bij online criminaliteit:

- slachtoffers kunnen opvangen (Black et al., 2018; Cross & Blackshaw, 2015; Hadlington et al., 2021; Holt & Bossler, 2012; Lee et al., 2025);
- slachtoffers van advies kunnen voorzien (Hadlington et al., 2021; Holt & Bossler, 2012);
- slachtoffers kunnen doorverwijzen naar andere hulpverlenende instanties (Lee et al., 2025);
- aangiftes kunnen opnemen (Chudasama et al., 2020; Cross et al., 2021; Forouzan et al., 2018; Hadlington et al., 2021; Lee et al., 2025); en
- digitaal bewijs veiligstellen (Hadlington et al., 2021; Holt & Bossler, 2012; Lee et al., 2025).

Het uitvoeren van het opsporingsonderzoek rondom online criminaliteitszaken is door de meeste auteurs toebedeeld aan meer specialistisch personeel op regionaal of zelfs landelijk niveau, vanwege de vaak grote hoeveelheden data en benodigde technologische kennis (Broadhurst, 2006; Black et al., 2019; Cockcroft et al., 2021; Cross et al., 2021; Hadlington et al., 2021; Hitchcock et al., 2017; Wall, 2007). Datzelfde geldt voor internationale samenwerking (Black et al., 2019; Forouzan et al., 2018) en bijbehorende, complexe jurisdictie (Broadhurst, 2006; Cross et al., 2021).

De brede consensus in de internationale literatuur is dat de lokale politie hier echter onvoldoende op is toegerust (Black et al., 2019; Bossler & Holt, 2012; Broadhurst, 2006; Chudasama et al., 2020; Cockcroft et al., 2021; Cross et al., 2021; Forouzan et al., 2018; Hadlington et al., 2021; Hitchcock et al., 2017; Holt & Bossler, 2012; Johnson et al., 2020; Lee et al., 2025; McNealey et al., 2025; Nowacki & Willits, 2020; Wall, 2007). Daarvoor ontbreekt het hen allereerst simpelweg aan basiskennis over online criminaliteit (Chudasama et al., 2020; Cockcroft et al., 2021; Cross et al., 2021; Forouzan et al., 2018; Hadlington et al., 2021; Hinduja, 2004; Hitchcock et al., 2017; Holt & Bossler,

2012; Johnson et al., 2020; Lee et al., 2025) en de digitale wereld in het algemeen (Bossler & Holt, 2012; Forouzan et al., 2018; McNealey et al., 2025; Wall, 2007; Wilson et al., 2022).

Er is onder lokale politiemensen ook veel discussie of het aanpakken van online criminaliteit wel algemeen, lokaal politiewerk voor hen is (Black et al., 2019; Cockcroft et al., 2021). Er is op uitvoerend niveau dan ook veel weerstand tegen (Black et al., 2019; Cockcroft et al., 2021; Johnson et al., 2020) en frustratie over (Black et al., 2019; Hadlington et al., 2021) de huidige en voorgenomen aanpak van online criminaliteit door de lokale politie. Ook geven politiemedewerkers aan weinig affiniteit met online criminaliteit te hebben (Black et al., 2019; Bossler & Holt, 2012; Stambaugh et al., 2001) of er simpelweg niet gemotiveerd voor te zijn (Cockcroft et al., 2021). Daarbij speelt ook mee dat lokaal onvoldoende capaciteit wordt ervaren voor de aanpak van online criminaliteit (Black et al., 2019; Bossler & Holt, 2012; Burns, Witworth & Thompson, 2004; Forouzan et al., 2018; Holt et al., 2010; Stambaugh et al., 2001).

Online criminaliteit aanpakken is voor veel uitvoerende politiemensen geen routinewerk (Cockcroft et al., 2021; Cross et al., 2021; Forouzan et al., 2018; Martin et al., 2018; McNealey et al., 2025; Nowacki & Willits, 2020; Wall, 2007). Dit terwijl routine in de politiecultuur erg belangrijk is. Binnen politieorganisaties ligt de focus veelal op routinematig werken en vertrouwde met de materie, waarbij senior medewerkers informeel junior collega's veel sturing geven in wat wordt aangepakt en hoe er dan gewerkt wordt. Zowel online als offline delicten vragen politiecapaciteit, maar politiemedewerkers geven de voorkeur aan offline criminaliteit, omdat zij weten hoe ze dit moeten aanpakken en veronderstellen dat daarvan de impact op de slachtoffers groter is (Black et al., 2019; Button et al., 2015; Forouzan et al., 2018; Hadlington et al., 2021; McNealey et al., 2025).

Ook is, zoals eerder aangegeven, de benodigde kennis om online criminaliteit aan te pakken doorgaans niet onder zittend personeel aanwezig. Dit terwijl de overdracht van kennis en ervaring van de senior op de junior collega's doorgaans als de belangrijkste leerwijze binnen de politie wordt ingezet. Daarmee wordt online criminaliteit aanpakken nu ten onrechte als 'geen politiewerk' door senioren politiemensen opgevat en als zodanig ook door hen op junior politiemensen overgedragen (Cockcroft et al., 2021; Wall, 2007). Lokale, uitvoerende politiemedewerkers zien online criminaliteit lang niet altijd als zaken met een serieuze impact (Button, 2021; Lee et al., 2025; Skidmore et al., 2020) of vinden dat de aanpak van online criminaliteit zaken hen belemmert om op traditionele misdrijven te reageren (Hinduja, 2004; Holt & Bossler, 2012). Er is doorgaans ook weinig tegengeluid op dit negatieve sentiment vanuit het lokale en hogere management (Bossler & Holt, 2012; Hitchcock et al., 2017). Dit terwijl onderzoek aangeeft dat steun van collega's in het algemeen en leidinggevend in het bijzonder, cruciaal zijn voor lokaal politiepersoneel wat zich op taken in de aanpak van online criminaliteit gaat richten (Bossler & Holt, 2012; Bossler et al., 2020; Hinduja, 2004, 2007; Hitchcock et al., 2017; Holt & Bossler, 2012; Lee et al., 2025; Stambaugh et al., 2001; Wilson et al., 2022).

Uitvoerende politiemensen die dagelijks met slachtoffers van online criminaliteit in aanraking komen, hebben niet automatisch meer en beter begrip hoe deze aan te pakken. Dit vergt training (Forouzan et al., 2018; Hadlington et al., 2021; Hinduja, 2004; Wilson et al., 2022). Het zijn ook vaker jonge, hoogopgeleide mannen met bovengemiddelde computervaardigheden die openstaan voor vernieuwing en innovatie. Daarnaast zouden politiemedewerkers die de ernst en impact van slachtofferschap van online criminaliteit inzien, eerder hun *first responder* rol accepteren en meer over online criminaliteit en de aanpak daarvan willen leren (Dodge & Burruss, 2019; Holt & Bossler, 2012; Lee et al., 2025). Daarmee is er naast sturing vanuit het management meer opleiding nodig om de lokale politie in staat te stellen om meer bewustzijn te hebben van de impact van online criminaliteit en slachtoffers beter te kunnen helpen (Cross & Blackshaw, 2015; Lee et al., 2025). Daarnaast is facilitering door middel van heldere beleidskeuzes en procedures van invloed op de motivatie van de lokale politiepraktijk om zich voor slachtoffers van online criminaliteit in te gaan zetten (Wilson et al., 2022; Lee et al., 2025). Daarbij pleit de literatuur nadrukkelijk voor heldere, praktisch toepasbare handleidingen over hoe uitvoerende politiemedewerkers om moeten gaan met online criminaliteit (Black et al., 2019; Bossler et al., 2020; Burruss et al., 2020; Cross & Blackshaw, 2015; Cross et al., 2021; Lee et al., 2025; Wilson et al., 2022).

Naast dat online criminaliteit in de basis van elke politieopleiding opgenomen zou moeten worden (Hitchcock et al., 2017), moet ook IT systematisch in elke politieopleiding worden opgenomen. Tevens is voor de aanpak van online criminaliteit (van preventie tot opsporing) een hogere opleiding van politiemedewerkers nodig (Cockcroft et al., 2021). Daarbij geven uitvoerende politiemedewerkers uit het Verenigd Koninkrijk aan dat ‘zitten en luisteren’ niet aan deze beroepsgroep is besteed (Hadlington et al., 2021). Politiemedewerkers geven aan dat het leren over de aanpak van online criminaliteit, wat hen betreft, zou moeten plaatsvinden in verplichte, lokale, fysieke sessies die groepsgewijs leren tussen collega's stimuleert, op basis van interactie en groepsdiscussies. Hierbij moeten zij worden ondergedompeld in lokale casuïstiek en de daarbij benodigde kennis en vaardigheden (Chudasama et al., 2020; Cockcroft et al., 2021; Forouzan et al., 2018; Hadlington et al., 2021; Hitchcock et al., 2017). *Learning by doing* in gezamenlijk verband, met een duidelijke koppeling met het eigen, dagelijks werk en de eigen functie is hierbij een veelbelovende benadering (Cockcroft et al., 2021; Holt & Bossler, 2012). Nieuwe kennis en vaardigheden worden in deze benadering verkregen door participatie in een lokale, lerende gemeenschap. Daarmee wordt tegemoetgekomen aan de insteek dat leren een sociaal en cultureel gesitueerde activiteit is die niet individueel kan worden uitgevoerd (Cockcroft et al., 2021).

#### 1.4 Leeswijzer

Dit rapport is als volgt opgebouwd. In hoofdstuk 2 worden het onderzoeksdesign en de gehanteerde onderzoeksmethoden toegelicht. In hoofdstuk 3 tot en met 5 presenteren we de resultaten uit de basisteams. In hoofdstuk 3 worden de interviewresultaten besproken, gevolgd door de resultaten van de vragenlijst in hoofdstuk 4. In hoofdstuk 5

---

staat het ontwerponderzoek centraal, waarin lokale interventies worden beschreven en geanalyseerd. Hoofdstuk 6 behandelt vervolgens de resultaten van interviews gericht op landelijke opschaling. Tot slot worden in hoofdstuk 7 de belangrijkste conclusies gepresenteerd, gevolgd door een discussie en aanbevelingen.



## 2 Onderzoeksdesign en -methoden

Het gekozen hoofddesign binnen dit project is die van ontwerponderzoek. Hierin wordt door middel van geïntegreerde ontwerp- en onderzoeksactiviteiten zowel kennisgroei als praktijkverbetering nagestreefd (Van den Berg & Kouwenhoven, 2008; Van Turnhout, Andriessen & Cremers, 2023). In het eerste deel van het onderzoek (deelvragen 1 en 2) is de lokale aanpak van online criminaliteit door medewerkers van de basisteams en hun perceptie daarbij in beeld gebracht. We hebben in kaart gebracht hoe lokale politiemensen online criminaliteit ervaren, welke kennis en vaardigheden zij bezitten en waar hun belangrijkste ontwikkelbehoeften liggen. Daarna zijn we doorgegaan op de daadwerkelijke ontwerpaanpak (deelvragen 3 en 4). Tot slot hebben we gekeken naar hoe de aanpak van online criminaliteit door medewerkers van de basisteams kan worden geïntensiveerd (deelvraag 5). Hiervoor hebben we een *mixed method* aanpak gehanteerd (zie tabel 2.1).

Tabel 2.1 Methodenmatrix

| Deelvraag                                              | Desk-research | Interviews | Vragenlijst | Observaties en praktijk-gesprekken | Focusgroep |
|--------------------------------------------------------|---------------|------------|-------------|------------------------------------|------------|
| 1. Perceptie politiemensen?                            | X             | X          | X           |                                    |            |
| 2. Hoe wordt online criminaliteit momenteel aangepakt? | X             |            | X           |                                    |            |
| 3. Hoe lokale aanpak intensiveren in interventies?     | X             | X          |             |                                    |            |
| 4. Ervaringen en effecten van interventies             | X             |            | X           | X                                  | X          |
| 5. Landelijke opschaling                               |               | X          |             |                                    |            |

### 2.1 Literatuuronderzoek

Er is een beknopt literatuuronderzoek uitgevoerd. De resultaten zijn reeds in het vorige hoofdstuk gepresenteerd. In de nationale en internationale literatuur is bekeken wat er bekend is over de rol van politiebasisteams in een digitale samenleving, de aanpak van online criminaliteit en de vereiste kennis en vaardigheden van politiewerk in een digitale samenleving. Hierbij is gebruikgemaakt van de wetenschappelijke databases van de mediatheken van NHL Stenden Hogeschool en Hogeschool Saxion, en Google Scholar. Daarnaast is gebruikgemaakt van de sneeuwbalmethode, waarbij de litera-

tuurlijsten van gevonden bronnen systematisch zijn doorgenomen om aanvullende, relevante publicaties te identificeren. De resultaten hiervan zijn gebruikt voor het invullen van paragraaf 1.3 en voor het ontwikkelen van meetinstrumenten.

## 2.2 Interviews basisteams

In dit onderzoek werkten we nauw samen met twee politiebasteams. Eén basisteam is gelokaliseerd in het noorden van Nederland, hierna aangeduid als basisteam Postenveld en één basisteam was gelokaliseerd in het oosten van het land, aangeduid als basisteam Lichtblauwveen. In dit onderzoek zijn de deelnemende teams geanonimiseerd om de integriteit van het onderzoek te waarborgen en een veilige omgeving te creëren voor open participatie. Anonimiteit maakt het mogelijk dat teams vrijuit kunnen reflecteren op hun werkwijzen, ervaringen en uitdagingen, zonder het risico van externe oordelen of interne druk. We schatten daarmee de kans op eerlijke en genuanceerde inzichten hoger in, wat essentieel is voor de kwaliteit en betrouwbaarheid van de onderzoeksresultaten. In bijlage I is een uitgebreidere omschrijving van beide basisteams te vinden.

In totaal zijn 33 interviews afgenomen bij de basisteams Postenveld ( $n = 14$ ) en Lichtblauwveen ( $n = 19$ ). Het doel van de interviews was om de perceptie van de medewerkers – over de lokale aanpak van online criminaliteit – te achterhalen. Een semigestructureerde interviewmethode werd hiervoor gebruikt (zie bijlage II), waarmee gericht vragen werden gesteld over kennis, vaardigheden, motivatie en ervaring, en die tevens ruimte liet voor diepgaande vragen en onverwachte thema's (Bryman, 2012). Elke geïnterviewde heeft een toestemmingsverklaring ondertekend voor deelname aan het interview. Met toestemming zijn de interviews opgenomen, verwerkt in een interviewverslag en voorgelegd aan de geïnterviewden. De interviews duurden gemiddeld een uur.

Voor de selectie van geïnterviewden in beide basisteams zijn personen aangedragen door contactpersonen van de basisteams. Er is gevraagd om een *random* steekproef van medewerkers en leidinggevende c.q. senioren van elke functiegroep. Hierbij is gevraagd om nadrukkelijk geen rekening te houden met mensen die veel of weinig affiniteit met online criminaliteit hadden. Dit bleek ook uit de resultaten van de interviews, waar tussen de geïnterviewden een groot verschil was in de interesse voor online criminaliteit. Dit had als doel om selectiebias te voorkomen.

Bij basisteam Postenveld zijn veertien interviews afgenomen, waarvan dertien fysiek hebben plaatsgevonden en één online. Er is gesproken met een teamchef, wijkagent, twee medewerkers van I&S, een leidinggevende I&S, twee operationeel specialisten A (OS-A), een senior tactische opsporing, een aspirant, een medewerker Veel Voorkomende Criminaliteit (VVC), een medewerker belast met incidentafhandeling, een ope-

rationeel expert Gebiedsgebonden Politie (GGP) en een medewerker van het digitaal platform<sup>2</sup>. De interviews zijn gehouden tussen 12 januari en 8 februari 2024.

Bij basisteam Lichtblauwveen zijn negentien interviews afgenomen. Er is gesproken met een leidinggevende basisteamrecherche (BR), wijkagent, operationeel coördinator, senior GGP, Operationeel Coördinatie Politie (OCP: casescreeners), incidentafhandeling (basispolitiezorg (BPZ)), operationeel expert (OE), generalist tactische opsporing, generalist GGP/jeugd wijkagent, hoofdagent, leidinggevende I&S, OS-A, hoofdagent/coördinator Verdachte Afhandel Team (VAT), en een medewerker van incidentafhandeling. De interviews zijn gehouden tussen 12 december 2023 en 29 februari 2024.

Alle interviewverslagen zijn getranscribeerd en vervolgens gecodeerd in het programma ATLAS.ti, versie 24. In dit programma is een kwalitatieve analyse met *open coding* uitgevoerd volgens de richtlijnen van Friese (2014) en Saldaña (2012). Er werd een codeboek gecreëerd met vooraf gedefinieerde, afgebakende hoofdcodes op basis van de interviewvragen. Deze hoofdcodes werden uitgekristalliseerd in subcodes door het transcript van het interview te lezen en te zoeken naar variaties die de hoofdcodes verklaarden. Dit is door beide onderzoekers onafhankelijk gedaan, voor beide basisteams. De subcodevariaties van beide basisteams zijn op post-its geschreven en samengevoegd op een grote muur voor overzicht. De onderzoekers hebben uit alle post-its overlappende categorieën geabstraheerd. In bijlage III is uitgebreider verslag gedaan van het coderingsproces. In hoofdstuk 4 zijn de interviewresultaten beschreven.

### 2.3 Vragenlijst

Er is een online vragenlijst uitgezet onder een representatieve steekproef van medewerkers van basisteams in Nederland. De vragenlijst is gebaseerd op literatuur over kennis en vaardigheden van de politie (Jansen et al., 2020; Politieonderwijsraad, 2020) en de resultaten van de eerder afgenomen interviews. Tevens zijn de richtlijnen van Project Centurion,<sup>3</sup> inclusief de vier geprioriteerde delicten (i.e., aan- en verkoopfraude, hulpvraagfraude, telefonische helpdeskfraude en phishing) opgenomen. De vragenlijst is door middel van een iteratief proces tot stand gekomen. Het eerste concept is voorzien van feedback door vijf onderzoekers buiten het projectteam, de aanbager publiek-private samenwerking politie Noord-Nederland en Oost-Nederland (Team Cybercrime), een senior data-analist (Team Cybercrime, Eenheid Noord-Nederland), politiemensen verantwoordelijk voor digitale transformatie, een Vernieuwer in de aanpak gedigitaliseerde criminaliteit en door de portefeuillehouder GGP.

Vervolgens is een *pretest* uitgevoerd onder negen medewerkers van de twee meewerkende basisteams. In beide basisteams hebben een medewerker I&S, medewerker VVC, medewerker incidentafhandeling en een leidinggevende de vragenlijst getest en voorzien van feedback. De vragenlijst is verbeterd aan de hand van deze feedback. Op

2 In Noord-Nederland is binnen de districtsrecherche voor elk district een digitaal platform ingericht die politiecollega's ondersteunen in de aanpak van online criminaliteit.

3 Project Centurion ondersteunt basisteams in de opvolging van aangiften van online criminaliteit door een gezamenlijke en landelijk gecoördineerde aanpak.

basis van de zelfchecklijst voor ethische integriteit van NHL Stenden zijn geen risico's aangaande ethische en of integriteitsaspecten gevonden. De uiteindelijke vragenlijst is te vinden in bijlage IV. De vragenlijst is verwerkt in de online survey tool Qualtrics.

Er is een lijst met geanonimiseerde potentiële respondenten verstrekt door de afdeling Onderzoekscoördinatie van de politie ( $n = 3.500$ ). De vragenlijst is gestuurd naar deze geanonimiseerde e-mailadressen met een onderschrift van de lector Digitale Weerbaarheid en de portefeuillehouder GGP. De vragenlijst is verstuurd op 14 oktober 2024. Daarna zijn er twee herinneringen gestuurd; na één en na drie weken. Op 20 november 2024 is de dataverzameling voor de vragenlijst gesloten. Bij het uitsturen van de vragenlijst ontvingen onderzoekers 224 *out-of-office* berichten. Daaruit werd duidelijk dat 108 respondenten de vragenlijst niet zouden invullen in de gewenste periode in verband met pensioen, verlof, vakantie, ze niet meer werkzaam zijn bij de politie of om een onbekende reden. De vragenlijst is daarmee uiteindelijk uitgezet bij  $n = 3.392$  politiemensen.

398 (11,7%) politiemensen zijn begonnen met de vragenlijst. Elke respondent heeft een toestemmingsverklaring ondertekend voor deelname aan de vragenlijst. Vijf personen hebben de toestemmingsverklaring niet ondertekend en 117 hebben de vragenlijst niet volledig ingevuld. In totaal hebben daarmee  $n = 276$  (8,1%) respondenten de vragenlijst volledig ingevuld. De antwoorden van deze respondenten zijn dan ook gebruikt voor de verdere analyse. De gemiddelde duur voor het invullen van de vragenlijst was twintig minuten (minimaal = vijf minuten, maximaal = zes uur).<sup>4</sup>

De resultaten zijn geanalyseerd met behulp van SPSS (versie 29). Er is gezien de beschrijvende en verkennende aard van de vragenlijst vooral gebruikgemaakt van beschrijvende statistiek. Tevens is voor verschillende variabelen een vergelijkende toets uitgevoerd om te bepalen of en in welke mate de functiegroepen van elkaar verschillen. Voor deze vragen zijn de normaliteitsaannames voor een ANOVA getoetst. Vervolgens is een Welch's one-way ANOVA uitgevoerd, omdat deze methode robuuster is tegen ongelijke varianties tussen groepen. Om het risico op type-I fouten te beperken, is een Bonferroni-correctie toegepast. De effectgrootte is berekend met eta squared ( $\eta^2$ ). Cohen (1988) heeft richtlijnen opgesteld om kleine ( $\eta^2 = 0,01$ ), middelgrote ( $\eta^2 = 0,06$ ) en grote ( $\eta^2 = 0,14$ ) effecten te definiëren. In dit rapport worden alleen de significante verschillen ( $p \leq 0,05$ ) tussen functiegroepen en de bijbehorende effectgroottes besproken. Aan de hand van deze gegevens weten we of er sprake is van een significant verschil tussen de functiegroepen en hoe groot het effect is, maar nog niet waar deze verschillen precies zitten en dus welke groep hoger of lager scoort dan andere groepen.

Daarom is bij een significant verschil aanvullend een bootstrap-analyse met 1.000 herhalingen uitgevoerd om 95% betrouwbaarheidsintervallen te schatten. Een verschil tussen twee groepen werd als significant beschouwd wanneer nul niet binnen dit betrouwbaarheidsinterval viel. Vervolgens is naar het absolute verschil gekeken tussen de gemiddelden. Ter illustratie, als een groep gemiddeld 1,2 scoort en de andere groep 1,5,

4 Het was mogelijk om het invullen van de vragenlijst tussentijds te onderbreken en op een later moment te hervatten.

dan zal het absolute verschil gemiddeld 0,3 zijn. Er is uitsluitend aandacht voor verschillen waarbij het absolute verschil tussen de gemiddelde scores van de functiegroepen groter is dan 0,5, zodat alleen de noemenswaardige verschillen gerapporteerd worden. Niet-significante verschillen en verschillen onder deze drempelwaarde zijn niet gerapporteerd. In hoofdstuk 5 worden de analyseresultaten van deze vragenlijst beschreven.

### Beschrijving respondenten vragenlijst

Tabel 2.2 geeft een overzicht van het aantal respondenten per eenheid. De meest vertegenwoordigde eenheden zijn Oost-Nederland en Midden-Nederland en de minst vertegenwoordigde eenheden Zeeland-West-Brabant en Amsterdam. De verdeling is dus niet volledig gelijkmatig, en komt niet exact overeen met de steekproef, maar er is voldoende respons om een beeld te geven van de Nationale Politie in alle eenheden.

Tabel 2.2 Overzicht aantal respondenten per eenheid

| Eenheid              | Aantal respondenten | Percentage | Percentage steekproef*<br>(landelijk) |
|----------------------|---------------------|------------|---------------------------------------|
| Oost-Nederland       | 47                  | 17,1       | 16 (16)                               |
| Midden-Nederland     | 35                  | 12,7       | 11 (12)                               |
| Noord-Nederland      | 30                  | 10,9       | 10 (8)                                |
| Den Haag             | 29                  | 10,5       | 13 (14)                               |
| Oost-Brabant         | 28                  | 10,2       | 7 (7)                                 |
| Rotterdam            | 25                  | 9,1        | 13 (12)                               |
| Limburg              | 24                  | 8,7        | 6 (6)                                 |
| Noord-Holland        | 21                  | 7,6        | 8 (8)                                 |
| Amsterdam            | 19                  | 6,9        | 10 (10)                               |
| Zeeland-West-Brabant | 17                  | 6,2        | 7 (7)                                 |

*\*Notitie. De percentages van zowel de steekproef als de landelijke cijfers zijn afgerond. Hierdoor komt het totaalpercentage van de steekproef uit op 101 procent.*

Van de respondenten is 32% vrouwelijk, 63% mannelijk, 2% beschrijft zichzelf anders<sup>5</sup> en 3% wil dit liever niet zeggen. Dit komt redelijk overeen met de populatie van de basisteams en de getrokken steekproef waarin de verhouding man-vrouw respectievelijk 65-35 en 64-36% is. De gemiddelde leeftijd van respondenten is 47 jaar (minimum = 22 jaar, maximum = 69 jaar,  $n = 270$ ). Dit ligt iets hoger dan de gemiddelden van de populatie en steekproef, respectievelijk 39,2 en 42,3 jaar. Respondenten waren gemiddeld 21 jaren in dienst bij de politie (minimum = 2 jaren, maximaal = 48 aantal jaren ( $n = 246$ )). Van de respondenten heeft 20% een specifieke taak of rol met betrekking tot

5 Zes respondenten hebben een toelichting gegeven. Deze bestond uit opmerkingen over hoe zij de vraag interpreteerden, of door te antwoorden met 'mezelf' of 'stoere kerel'.

online criminaliteit. Dit betrof een portefeuillehouder online criminaliteit of taakhouder online criminaliteit ( $n = 16$ ), digitaal wijkagent ( $n = 11$ ), digi-coach ( $n = 2$ ), of een andere taak of rol ( $n = 16$ ).<sup>6</sup>

Bijna driekwart van de respondenten heeft *geen* opleiding of cursus gevolgd op het gebied van online criminaliteit (71,3%). Ongeveer een op de vijf respondenten geeft aan *wel* een opleiding of cursus gevolgd te hebben op het gebied van gedigitaliseerde criminaliteit (14,5%) en/of cybercrime (5,5%). In enkele gevallen hebben respondenten een cursus over zowel cybercrime als gedigitaliseerde criminaliteit gedaan. Een kleine groep heeft wel een opleiding gevolgd, maar weet niet of het ging over cybercrime of gedigitaliseerde criminaliteit (5,5%) of heeft een aparte opleiding gevolgd op het gebied van IT (3,3%). Ook is aan respondenten gevraagd welke functieomschrijving het best past bij hun werkzaamheden (zie tabel 2.3). Een beperking is dat per basisteam de benamingen en functies enigszins verschillen.

Tabel 2.3 Functieomschrijving van respondenten

| Functie                            | Aantal respondenten | Percentage |
|------------------------------------|---------------------|------------|
| Senior GGP-wijkagent               | 53                  | 19,3       |
| Senior GGP-overig                  | 44                  | 16,0       |
| Generalist GGP                     | 43                  | 15,6       |
| Medewerker I&S                     | 32                  | 11,6       |
| Operationeel Expert                | 26                  | 9,5        |
| Medewerker VVC/opsporing/crimeteam | 19                  | 6,9        |
| Senior Tactische Opsporing         | 17                  | 6,2        |
| Operationeel Specialist            | 10                  | 3,6        |
| Teamchef                           | 5                   | 1,8        |
| Operationeel Coördinator           | 3                   | 1,1        |
| Aspirant/stagiair                  | 3                   | 1,1        |
| Anders, namelijk <sup>a</sup>      | 20                  | 7,3        |
| <b>Totaal</b>                      | <b>275</b>          | <b>100</b> |

<sup>a</sup> Vier Digitaal Wijkagenten, drie Operationeel Experts-Wijk, twee Generalisten Tactische Opsporing, twee Senior medewerkers I&S, twee medewerkers Case screening, een Kwaliteits-HOVJ, een medewerker Leer- en Ontwikkelplek, een BOA/teamsecretariaat, een Medewerker GGP, een Ondersteuner, een medewerker Bedrijfsvoering, een Senior Intelligence, een Themahouder dierenwelzijn, en een medewerker Preventie senioren en veiligheid.

6 Vijf respondenten houden zich bezig met het screenen van online criminaliteitszaken. Vier fungeren als aanspreekpunt voor cybercrime of gedigitaliseerde criminaliteit, zowel voor politiecollega's als voor het Openbaar Ministerie. Twee respondenten nemen aangiften van online criminaliteit op, terwijl twee anderen zich richten op preventieve taken, zoals het geven van workshops op scholen. Daarnaast zijn twee respondenten specialist opsporing op het gebied van online criminaliteit. Eén respondent geeft aan 'onofficieel digitale zaken op te pakken' en één vervult de rol van aanjager van de digitale transitie.

## 2.4 Ontwerponderzoek

Samen met de basisteams hebben de onderzoekers toegewerkt naar verschillende interventies ter ondersteuning van de beweging van basisteamedewerkers naar de lokale aanpak van online criminaliteit. Daarbij is sprake van *ontwerponderzoek*. Ontwerponderzoek is een systematische benadering van problemen, waarin door middel van geïntegreerde ontwerp- en onderzoeksactiviteiten een tweeledig doel wordt nagestreefd: praktijkverbetering en kennisgroei (Van den Berg & Kouwenhoven, 2008; Van Turnhout, Andriessen & Cremers, 2023).

In de tweede fase richten wij ons op het beschrijven, ontwikkelen en evalueren van interventies die bijdragen aan een intensivering van de lokale aanpak van online criminaliteit. Daarbij sluiten wij nadrukkelijk aan bij de ontwikkeling die de twee basisteams Postenveld en Lichtblauwveen zelf doormaken. Het is niet de taak van de onderzoekers om interventies zelfstandig te ontwikkelen of te implementeren, maar om de bestaande initiatieven binnen de politieorganisatie en teams te volgen, te inventariseren en – waar nodig – te ondersteunen of verdere ontwikkeling aan te jagen. Zo draagt dit onderzoek bij aan een lerende praktijk waarin basisteams hun rol in de aanpak van online criminaliteit steeds gericht en effectiever kunnen vormgeven. Bij basisteam Postenveld zijn hiervoor vier fasen doorlopen.

In fase 1 hebben de onderzoekers bestaande interventies binnen de Nationale Politie geïnventariseerd. Dit is gedaan middels deskresearch op het intranet van de politie en in gesprekken met relevante experts binnen de politie (zoals een digi-coach, digi-professional, projectleider, digitaal wijkagent en een STO'er van Team Cybercrime). In fase 2 hebben de onderzoekers de inzichten uit de eerste fase aan de leden van het basisteam gepresenteerd en daarop gezamenlijk gereflecteerd. Vervolgens zijn, met behulp van brainstormtechnieken en een prioriteitentabel,<sup>7</sup> samen met basisteamedewerkers enkele interventies geselecteerd. In fase 3 stonden interventieontwikkeling en implementatie centraal. De medewerkers van het basisteam waren leidend in deze fase en de onderzoekers vervulden primair een ondersteunende rol (zie bijlage VIII). In fase 4 evalueerden de onderzoekers de geïmplementeerde interventies met methoden die passen bij de ontwikkelde interventies, zoals focusgroepen, een vragenlijst, observaties en individuele gesprekken. In paragraaf 5.1 is een gedetailleerdere beschrijving opgenomen van de betreffende interventieaanpak.

Bij de afsluitende fase werken de onderzoekers toe naar een integratie van de voorgaande fasen. Op basis van de input uit de interviews en vragenlijsten onder basisteamedewerkers ontwikkelden zij, samen met experts van binnen en buiten de politie, principes die richting kunnen bieden voor het landelijk opschalen van de taken van basisteams in de aanpak van online criminaliteit. Het onderzoek levert daarmee, in samenwerking met professionals, basisprincipes op die door de praktijk nader inge-

7 Waarin een score wordt gegeven per interventie op belangrijkheid, urgentie, praktisch uitvoerbaarheid en ethische geschiktheid, gebaseerd op participatief actiefonderzoek (Eelderink, 2024).

vuld kunnen worden (Van Turnhout, Andriessen & Cremers, 2023). Daarmee kenmerkt deze deelvraag zich meer als *research for design* (Bærenholdt et al., 2010).

Dit proces is concreet in drie fasen vormgegeven. De onderzoekers formuleerden in fase 1 op basis van de inzichten uit de interviews en vragenlijsten onder de basisteammedewerkers een eerste, grove versie van de principes voor landelijke opschaling. In fase 2 werden experts van binnen en buiten de politie geïnterviewd over hun visie op de landelijke opschaling van taken van basisteammedewerkers en werden daarbij expliciet gevraagd naar hun reacties op deze principes (zie paragraaf 2.5). In fase 3 scherpten de onderzoekers de principes voor landelijke opschaling aan op basis van de input van de experts.

## 2.5 Interviews intensivering

Voor het laatste onderdeel van dit onderzoek zijn, ondersteunend aan het ontwerponderzoek, interviews afgenomen met verschillende experts binnen en buiten de politie. Het interview bestond uit drie onderdelen:

1. De aanpak van online criminaliteit door de politie op landelijk niveau (stand van zaken, doelstellingen, ambities).
2. De aanpak van online criminaliteit door de politie op lokaal niveau (de rol van het basisteam, samenwerkingen met andere afdelingen, kennis- en vaardigheidsniveau, kernprobleem in de aanpak en de mening over digi-dagen als interventie voor intensivering).
3. Het verkennen en nader aanscherpen van door de onderzoekers, op basis van de resultaten van interviews met, vragenlijsten onder medewerkers van basisteams, ontworpen principes waarlangs de aanpak van online criminaliteit door de politie kan worden geïntensiveerd.

Voor deze interviews is – gezien de zeer verkennende aard van dit onderdeel van het onderzoek – een semigestructureerde interviewmethode gebruikt (zie interviewprotocol in bijlage V). Elke respondent heeft een toestemmingsverklaring ondertekend voor deelname aan het interview (zie bijlage VII). Met toestemming van de respondenten zijn de interviews op audio opgenomen. Bij elk interview waren twee onderzoekers aanwezig, waarvan één de vragen stelde en de ander notuleerde. De interviews duurden gemiddeld tachtig minuten. Acht interviews zijn digitaal via Microsoft Teams uitgevoerd en twee fysiek op locatie. Wanneer er tijdens de interpretatie onduidelijkheden waren, zijn de tijdens het interview gemaakte notulen verduidelijkt met behulp van de audio-opnames. De uitgewerkte notulen zijn, na een controle door de respondenten, door de onderzoekers die de interviews hebben afgenomen, thematisch geordend en vervolgens is dit totale document door een andere onderzoeker gecodeerd met behulp van ATLAS.ti. Na een controle van de coderingen door een vierde onderzoeker is de analyse op de onderlinge samenhang uitgevoerd door de onderzoeker die de codering heeft gedaan.

In totaal werkten tien respondenten mee aan het onderzoek (zie tabel 2.4), waarbij één respondent per keer is geïnterviewd. De deelnemers hebben uiteenlopende functies, maar allen hebben affiniteit met (de aanpak van) online criminaliteit en/of digitale transformatie in bredere zin.

Tabel 2.4 Functies en respondentnummers van de geïnterviewde politiemedewerkers

| <b>Functie</b>                                                                          | <b>Respondentnummer</b> |
|-----------------------------------------------------------------------------------------|-------------------------|
| Commissaris Politie, Nationaal Team Digitale Transformatie                              | 1                       |
| Adviseur                                                                                | 2                       |
| Adviseur digitale transformatie eenheid Oost-Nederland                                  | 3                       |
| Cybervrijwilliger/Specifieke Inzet                                                      | 4                       |
| Programmamanager landelijke portefeuille GGP                                            | 5                       |
| Senior Intelligence (Digitaal Professional)                                             | 6                       |
| Projectleider aanpak gedigitaliseerde criminaliteit<br>(hoofdinspecteur van de Politie) | 7                       |
| Politiespecialist op landelijk niveau                                                   | 8                       |
| Teamleider Digitale Transformatie en Wendbaar Organiseren<br>(OS-C, hoofdinspecteur)    | 9                       |
| Beleidsadviseur                                                                         | 10                      |



## 3 Interviewresultaten basisteam

In dit hoofdstuk wordt de visie van politiemensen in twee basisteam beschreven op de lokale aanpak van online criminaliteit. Wij interviewden in Postenveld veertien en in Lichtblauwveen negentien medewerkers van de basisteam. In paragraaf 3.1 worden de achtergrondkenmerken van respondenten verder toegelicht, om de interviewresultaten beter te duiden. In paragraaf 3.2 wordt ingegaan op hoe de prevalentie van online criminaliteit wordt gezien en geïnterpreteerd, inclusief slachtofferschap en daderschap, de rol van het basisteam in de aanpak van online criminaliteit en het ideaalbeeld. In paragraaf 3.3 is het toewijzingskader van de Portefeuille Digitalisering en Cybercrime (2023) toegelicht en de visie van respondenten op dit conceptbeleidsstuk en de uitvoering ervan. In paragraaf 3.4 is de huidige aanpak van online criminaliteit binnen het basisteam uiteengezet. In paragraaf 3.5 is beschreven op wat voor manier het team zich tot nu toe heeft ontwikkeld en paragraaf 3.6 beschrijft welke behoeften politiemensen hebben om de lokale aanpak van online criminaliteit te verbeteren.

### 3.1 Achtergrondkenmerken van de geïnterviewde politiemensen

De geïnterviewden hebben een variatie aan rollen en taken binnen het basisteam. Politie mensen uit I&S, VVC/Crime team en de incidentafhandeling zijn geïnterviewd, evenals teamchefs, operationeel coördinatoren, casescreeners, wijkagenten en een agent in opleiding (zie paragraaf 2.2). Bij de uitwerking van de resultaten presenteren we zo nu en dan quotes van geïnterviewden. Geïnterviewden uit basisteam Postenveld duiden we aan met de toevoeging 'PV' en geïnterviewden uit basisteam Lichtblauwveen met 'LV'.

Bij de meeste geïnterviewden was er enige interesse in online criminaliteit, maar tegelijkertijd leek een lage motivatie rondom de aanpak van deze zaken een grote rol te spelen. Er was een hoge variatie in affiniteit met online criminaliteit. *'Het heeft mijn interesse niet en dan wordt het ook lastiger, denk ik. Neem vroeger je school. Ik wilde graag verpleegster worden en alles wat daarmee te maken had vond ik leuk. Maar aardrijkskunde, waar had ik het voor nodig? Dan is die motivatie er niet. Als je het vakgericht hebt, met dingen die je leuk vindt, is het makkelijker iets te leren, dan iets waar je totaal geen interesse in hebt.'* (LV18)

De meeste geïnterviewde politiemensen hadden geen specifieke training, opleiding of cursus gevolgd gericht op online criminaliteit. Eén geïnterviewde had een, naar eigen zeggen 'ingewikkelde', cybercrimetraining gevolgd en een aantal hadden een cursus gevolgd over het raadplegen van openbare bronnen, zoals een OSINT-cursus.

In totaal hadden vier geïnterviewden (twee uit Postenveld en twee uit Lichtblauwveen) een privé-ervaring met online criminaliteit, van zichzelf of in hun direct omgeving, of ontvingen phishing mails op hun werkaccount. *‘Op mijn werkaccount krijg ik wekelijks ergens vanuit de wereld Engelse berichten van mensen die zieke kinderen hebben en geld vragen om een crowdfunding op te richten. [...] Bij heel veel politieagenten trouwens.’* (LV01)

### 3.2 **Perspectief op slachtofferschap, daderschap, prevalentie en de rol van het basisteam in de aanpak van online criminaliteit**

Om erachter te komen wat de politiemensen vinden van online criminaliteit hebben wij eerst vragen gesteld over hun perspectieven op slachtofferschap, daderschap en de prevalentie van online criminaliteit.

Bijna alle geïnterviewden gaven aan dat zij een groeiende trend waarnemen van online criminaliteit. Er was een verschil tussen de geïnterviewden met betrekking tot de verhouding digitale-fysieke meldingen; tussen de 50-90% van de totale criminaliteitsomvang werd als online criminaliteit geschat. De meesten waren het er wel over eens dat online criminaliteit een zeer groot deel van criminaliteit uitmaakt en groeiend is. *‘Vorig jaar of het jaar ervoor hadden we een stijging van 400%. [...] Ik denk dat het alleen maar groter en moeilijker wordt.’* (PV01)

De geïnterviewden gaven aan dat vooral gedigitaliseerde criminaliteit veel voorkomt. Als gevraagd werd naar het type criminaliteitsvormen, dan werd bankhelpdeskfraude (telefonische helpdeskfraude) bij uitstek genoemd. Maar ook WhatsAppfraude c.q. Vriend-In-Noodfraude (tevens bekend als Hulpvraagfraude), diefstal van gegevens (om bijvoorbeeld bij online winkels bestellingen mee te doen) en afpersing (bijvoorbeeld een afpersingsmail waarin wordt gesteld dat er een video is waarin de ontvanger porno kijkt en seksuele handelingen met zichzelf verricht) komen vaak voor volgens geïnterviewden. Wat minder vaak werd genoemd zijn sexting, verkoopfraude, online beleggingen, en Marktplaats-oplichting. In beide basisteams werd aangegeven dat cybercrime weinig tot nooit voorkomt op lokaal niveau. Slechts enkelen hebben met cybercrime te maken gehad, zoals hacken in de relationele sfeer, een DDoS-aanval of ransomware-aanval.

Er was onder de geïnterviewden weinig zicht op online criminaliteit en daderschap. Volgens hen zijn de daders van online criminaliteit van alle leeftijden en komen ze zowel uit Nederland als het buitenland. Enkele geïnterviewden gaven aan dat de daders opereren in een georganiseerd netwerk, waar enigszins zicht is op de loopjongens, maar niet op de daders die ‘erboven zitten’. De jonge daders willen snel geld verdienen en zijn vindingrijk. Zij hoeven niet per se digitaal onderlegd te zijn. Zo vertelde een geïnterviewde over enkele verdachten van bankhelpdeskfraude, die potentiële slachtoffers bellen om ze te verleiden om geld over te maken, het volgende: *‘De jongens van het callcenter die we recent hebben opgepakt werkten volledige lijsten af. Ze hebben een kansberekening dat 1 op de 20 reageert en dan hebben ze een jaarsalaris binnen geharkt.’*

*Ze werken professioneel. Het zijn mensen van 20-35 jaar, maar je ziet ze ook ouder.* (PV01)

Online criminaliteit is voor deze groep daders een aantrekkelijke vorm van criminaliteit door een lage pakkans. Ze vermoeden dat er een verschuiving plaatsvindt van traditionele criminaliteit naar online criminaliteit. *'Het verbaast ons dat deze verdachten bezig zijn met cybercrime, dat waren eerst onze drugsdealers.'* (PV01) Tevens ziet een geïnterviewde een vermenging tussen traditionele criminaliteit en online criminaliteit. *'Ik zie steeds meer vermenging. Mensen die zich met deze criminaliteitsvorm bezighouden, zijn gelijktijdig bezig met klassieke criminaliteitsvormen.'* (PV01). *Doordat er weinig zicht is op daders, zijn er ook weinig heterdaad acties. Als we het op straat tegenkomen is het op toeval berust.'* (PV14)

De geïnterviewden hadden meer zicht op slachtofferschap van online criminaliteit, en gaven aan dat er veel slachtoffers zijn. Deze zijn volgens onze geïnterviewden van alle leeftijden, van kinderen op scholen tot aan senioren. Een geïnterviewde merkte op dat ouderen er voornamelijk slachtoffer van zijn, en er een verschuiving lijkt te zijn naar jongeren. De meeste geïnterviewden beaamden dat online criminaliteit een grote financiële en emotionele impact kan hebben op slachtoffers. Zij benoemden dat de impact van slachtofferschap afhankelijk is van de vorm van criminaliteit en het schadebedrag. Schaamte speelt een grote rol bij slachtofferschap, bij zowel bedrijven als burgers. Door de schaamte denken slachtoffers: *'Hoe heb ik daarin kunnen trappen?'* (PV04, PV05) Slachtoffers kunnen boos of emotioneel zijn, kunnen er niet van slapen en raken soms het vertrouwen in de medemens kwijt, aldus de geïnterviewden. Enkele geïnterviewden gaven aan dat slachtofferverhalen hen ook persoonlijk raken:

*'Nou, dat raakt me soms wel eens. Dan kom je bij zo een oud mensje die misschien wel € 20.000 kwijt is en die hebben soms wel zes uur aan de lijn gehangen met iemand. En dan vertellen ze ook nog dat ze uitgescholden worden.'* (PV05)

*'Dat stoort me mateloos, dat ik denk; die daders hebben half niet door wat voor impact het emotioneel heeft op die mensen. Dat is gewoon echt heel sneu. De emotionele impact weegt veel zwaarder dan financieel.'* (PV13)

*'Ze trekken ze helemaal leeg. Dan gaan ze er nog grapjes over maken naar elkaar, hoe ze die oude tang helemaal naar de grond getrokken hebben. Ik vind dat heel erg. Ik vind het een smerige manier. Als je het hebt over de impact, dan gaat het over hele families die ontferd worden. Ik vind dat heel erg.'* (PV01)

Vervolgens vroegen we naar het ideaalbeeld over de lokale aanpak van online criminaliteit. Een groot deel van de geïnterviewden uit beide basisteams deelden dezelfde mening. Deze groep stelde dat basisteams alleen gedigitaliseerde criminaliteit moeten aanpakken en dus geen cybercrime. Deze meerderheid wil op de hoogte blijven van de nieuwste criminele (online) ontwikkelingen en vindt het essentieel dat de kwaliteit van

aangiften van online criminaliteit verbetert. Enkele geïnterviewden (drie uit Postenveld, twee uit Lichtblauwveen) gaven aan behoefte te hebben aan een snellere informatievoorziening en praktisch stappenplan om slachtoffers beter te begeleiden bij het opnemen van aangiften. Enkele andere geïnterviewden gaven aan een integrale samenwerking met andere politieafdelingen ('korte lijntjes') en regelmatige kennisuitwisseling met praktijkvoorbeelden te willen. Tot slot werd voorgesteld om een deel van de aanpak op landelijk niveau centraal te coördineren, zoals Project Centurion (zie paragraaf 2.3). Een enkeling in Lichtblauwveen vond het belangrijk om goed zichtbaar te zijn in de digitale wereld; een taak die weggelegd zou zijn voor de wijkagenten. Er is de geïnterviewden vervolgens gevraagd naar hun visie op de rol van het basisteam in de aanpak van online criminaliteit. De primaire taken van het basisteam worden gezien in de opsporing, preventie van (herhaald) slachtofferschap en opname van goede aangiften. De meeste geïnterviewden gaven aan het opsporen en aanhouden van verdachten te zien als de primaire taak van het basisteam op dit gebied. Hoewel opsporing als kerntaak werd beschouwd, is het belangrijk dat deze taak beperkt blijft tot kleinere en minder complexe onderzoeken.

*'Ik vind wel dat we het kleinere online criminaliteit aan moeten kunnen pakken. Dus dat houdt in WhatsApp fraude, Marktplaatsfraude, Vriend-In-Nood fraude, helpdeskfraude, dat soort dingen. Grotere zaken vind ik te complex om bij een basisteam te laten, dus die moet je eigenlijk doorzetten naar het Cybercrimeteam. Als het echt over crypto gaat, of om grotere bedragen, grote bedrijven, echte hacks dat is veel te lastig voor ons als basisteam, maar de kleinere oplichtingszaken en criminaliteit die moeten wij kunnen draaien. Voor de complexere zaken gaat het vooral om dat wij wel signaleren en het vervolgens doorzetten, eventueel met behulp van het Cybercrimeteam.'* (PV14)

Daarnaast vinden de meeste geïnterviewden dat de preventie van (herhaald) slachtofferschap onder burgers belangrijk is, bijvoorbeeld door voorlichting te geven bij scholen en ouderen. In beide basisteams gaven medewerkers aan dat de preventieve rol vooral bij de wijkagent ligt. Hoewel preventie als een belangrijke taak wordt gezien, vinden geïnterviewden dat preventie tegelijkertijd integraal opgepakt moet worden of volledig bij andere partijen, zoals gemeenten en de rijksoverheid, kan liggen, waarin de politie volgens hen een aanjagende rol heeft. Preventie moet gericht zijn om slachtofferschap en herhaald slachtofferschap te voorkomen. Enkele geïnterviewden gaven aan dat ook daderpreventie een taak van de politie is, met name jongeren 'die aan het begin staan'. Eén politiemedewerker zag geen preventieve rol voor de politie weggelegd: *'Dan was ik wel maatschappelijk werker geworden.'* (LV01)

Het zorgvuldig en accuraat opnemen van aangiften van online criminaliteit kwam ook naar voren als een kerntaak van de basisteams. Specifiek het opnemen van aangiften met de juiste informatie of een aangifte opnemen bij oudere mensen thuis vinden ze

belangrijk bij online criminaliteit. *'Aangifte moet van digitale criminaliteit net zo makkelijk zijn als een mishandeling of beroving.'* (PV01)

Sommige geïnterviewden vinden dat het verstoren van online criminaliteit, bijvoorbeeld door stopgesprekken te voeren met geldezels, ook een taak is van het basisteam. Een andere aanpak van verstoring kan zijn door als politie actief op de voorgrond te treden op sociale media bij bijvoorbeeld stalking, bedreiging of cyberpesten.

Eén van de geïnterviewden vat de visie op de primaire kerntaken van het basisteam als volgt samen: *'Het basisteam hoeft geen groot of diepgravend onderzoek te draaien. Rechtshulpverzoeken en andere ingewikkelde toeren uithalen hoeft niet. Ze moeten wel de info die wordt aangeleverd bij aangifte verifiëren. Waar zitten de opsporingskansen, dus eigenlijk de eerste handelingen om de zaak te kunnen duiden.'* (PV12)

### 3.3 Toewijzingskader

Volgens het concepttoewijzingskader van de Portefeuille Digitalisering & Cybercrime (2023) zouden basisteams zich in de nabije toekomst moeten gaan richten op online criminaliteitszaken waarbij de dader bekend is en er sprake is van een lage complexiteit in combinatie met veel opsporingsindicaties. Hierbij kan gedacht worden aan het aanhouden en afhandelen van geldezels, sextortion-zaken waarbij de dader bekend is en zonder letsel voor (of de dood van) het slachtoffer en cyberpesten in de lokale sfeer, hacken in de relationele sfeer (onrechtmatig inloggen of in mailboxen of sociale media van een ander kijken), DDoS-aanvallen met bekendheid van de dader (een doelbewuste overbelasting van de digitale infrastructuur van een organisatie om deze uit de lucht te halen) en diefstal van gegevens door medewerkers van een bedrijf. Wij hebben de geïnterviewden gevraagd of zij bekend waren met dit toewijzingskader en wat zij hiervan vonden.

In zowel Postenveld als Lichtblauwveen zijn de meeste geïnterviewden op de hoogte van de prioritering van de aanpak van online criminaliteit en vinden dit een goed en ambitieus initiatief. In Lichtblauwveen was meer dan de helft van de geïnterviewde politiemensen bekend met dit toewijzingskader. In Postenveld waren zij niet op de hoogte van dit specifieke toewijzingskader, maar wel van de algemene beleidsplannen. Eén geïnterviewde gaf aan de plannen 'redelijk zwaar' te vinden. Hoewel de meesten het in principe een goed plan vonden, gaven zij tegelijkertijd een aantal kanttekeningen bij de uitvoering ervan. De belangrijkste zorgen werden geuit over de capaciteit en haalbaarheid van het kader. De geïnterviewden uitten zorgen over of de basisteams dit wel aan kunnen en zien een groot verschil in de plannen van het toewijzingskader en de praktische realiteit waar de politie mee te maken heeft. Online criminaliteit moet volgens onze geïnterviewden niet bij het huidige takenpakket worden toegevoegd. Er moet geprioriteerd worden of er moet meer personeel worden aangenomen, en het liefst beide.

Ook gaven geïnterviewden aan dat werkzaamheden behapbaar moeten blijven voor medewerkers en zij niet van alle verschillende vormen van online criminaliteit op de hoogte kunnen zijn. Er zijn zorgen over de kennis en kunde van politiemensen om on-

line criminaliteit aan te pakken. *‘Met de kennis die we nu hebben [is het] onrealistisch.’* (PV14)

Er wordt geadviseerd om verschillende werkgroepen te maken die elk een thema behandelen, zoals DDoS-aanvallen, hacking, malware et cetera, die tevens zijn verdeeld in heterdaad en langdurige zaken. Ook werd door een aantal geïnterviewden benoemd dat het selectiviteitskader van het Openbaar Ministerie (OM) mogelijk een obstakel vormt in het uitvoeren van het toewijzingskader. Zo worden bijvoorbeeld fraudezaken onder een bepaald bedrag direct door het OM afgewezen. Dit roept bij geïnterviewden de vraag op in hoeverre de strafrechtelijke vervolging van de dader daadwerkelijk mogelijk is. Een complexer probleem is dat online criminaliteit grensoverschrijdend is – daders en slachtoffers bevinden zich in andere politie-eenheden, regio's of zelfs landen – en het daarom lastig aan te pakken valt in de lokale context.

*‘In theorie een heel mooi uitgangspunt [red. het toewijzingskader]. Alleen het spreekt nogal de realiteit tegen wat mij betreft. Ten eerste is opsporing natuurlijk niet een hele populaire tak van sport binnen de basisteams. Ze staan niet echt in de rij om het zo maar te zeggen. Sommige mensen moeten verplicht dan een periode bij de opsporing. Er is niet zo heel veel animo voor. Dat komt ook door de financiën. We hebben natuurlijk niet de allerdikst betaalde baan. De mensen die onregelmatig werken, die hebben nog een redelijk aanvulling in hun salaris. Dat hebben mensen in de opsporing niet, die worden alleen voor dagdiensten gepland. Er zijn mensen die de onregelmatigheidstoeslag nodig hebben. Ten tweede, het is een administratieve functie en je zit de hele dag binnen. Ten derde, veel mensen hebben geen affiniteit met digitale criminaliteit. Dan kan je als politie willen dat mensen die affiniteit voelen, maar dan kan je beter mensen bij de opsporing zetten die er al affiniteit mee hebben.’* (PV08)

### 3.4 Huidige aanpak van online criminaliteit

In deze paragraaf is uiteengezet wat de huidige lokale aanpak van online criminaliteit volgens geïnterviewden is. Tijdens de interviews bleek dat beide basisteams in enige mate online criminaliteit opsporen. In Postenveld wordt onder andere gekeken naar trends en naar de vraag of jeugdgroepen van de straat naar de online omgeving verplaatsen. In Lichtblauwveen werd ook genoemd dat het Dark Web en Telegram worden bekeken, er vorderingen worden gedaan, bijvoorbeeld voor IP-logs of bij internetproviders<sup>8</sup>. Beide basisteams richten zich op geldezels door bijvoorbeeld stopgesprekken uit te voeren. Bij stopgesprekken worden de geldezels gewaarschuwd om te stoppen met criminele activiteiten en veelal aangegeven dat ze het afgenomen geld aan de slachtoffers dienen te vergoeden. In ruil hiervoor vindt er geen strafrechtelijke vervolging plaats. Het overgaan tot stopgesprekken wordt beslist in overleg met het Open-

8 Internetproviders zijn organisaties of personen die diensten leveren op of via het internet. IP-logs zijn een verzameling aan loggingdata waaronder IP-adressen.

baar Ministerie. In het basisteam Lichtblauwveen werd door een geïnterviewde genoemd dat zij de focus expliciet leggen op gedigitaliseerde criminaliteit.

Bij complexere criminaliteitsvormen in het verzorgingsgebied worden deze doorgezet naar een andere afdeling. In beide basisteams wordt ook samengewerkt met specialisten, zoals het digitaal platform (specifiek voor basisteam Postenveld), Team Cybercrime c.q. het Cybercrimeteam of de recherche. In Lichtblauwveen wordt tevens een intern cyberteam ingezet: *‘Er zijn altijd een paar Whizzkids bij een team. We hebben ruim 200 mensen in ons team. Die Whizzkids vinden het leuk en zijn er meer in gespecialiseerd. Die hebben een Cybercrimeteampje georganiseerd. Dit soort onderzoeken worden meer naar hen geschoven. En om die reden misschien niet meer bij ons terechtkomen.’* (LV11)

In Lichtblauwveen wordt samengewerkt met de HUB.<sup>9</sup> In Postenveld wordt samengewerkt met jongerenwerkers en de gemeente om waarschuwingsbrieven naar geldezels te sturen.

Ten tijde van de interviews is er binnen de basisteams gecommuniceerd over Project Centurion binnen de landelijke politieorganisatie, maar is het project nog niet lokaal opgevolgd (zie paragraaf 2.3). In Postenveld waren de meeste geïnterviewden bekend met Project Centurion en hadden zij een beeld van wat het project betekent voor hun werkzaamheden (geïnterviewden benoemden Project Centurion spontaan). Bij het basisteam in Lichtblauwveen kwam Centurion niet ter sprake tijdens de interviews. Dit werd ook niet door de interviewers bevraagd.

De meeste geïnterviewden van het basisteam Lichtblauwveen vermelden in plaats daarvan het gebruik van de digitale meldkamer. De digitale meldkamer staat voor een experiment/werkwijze waarin politiemensen fysiek bij slachtoffers van online criminaliteit langsgaan om aangifte op te nemen en sporen veilig te stellen (Politie, 2024). Dit experiment is gestart in politie-eenheid Oost-Nederland en is ten tijde van de interviews alleen daar ingezet.<sup>10</sup> In basisteam Postenveld is de digitale meldkamer niet genoemd.

De meeste geïnterviewden gaven aan dat er wel informatie op intranet staat of dat zij weten bij wie zij moeten zijn bij vragen over (de aanpak van) online criminaliteit. Er zijn ook politiemensen die dit overzicht niet hebben of niet weten waar zij terecht kunnen. *‘In onze optiek is er geen centraal punt om informatie, data of hulp (iemand die meekijkt) wat structureel in de organisatie is geïmplementeerd.’* (PV08)

Vanuit de politieorganisatie worden online verschillende hulpmiddelen, zoals handboeken en handleidingen beschikbaar gesteld en aangereikt. Een deel van de geïnterviewden in Postenveld heeft deze hulpmiddelen ontvangen en geeft aan deze ook te gebruiken. Hulpmiddelen die zij hebben/gebruiken zijn het handboek aangifte, cyber-

9 De HUB voor Oost-Nederland betreft een regionale samenwerking tussen in opsporing van online criminaliteit gespecialiseerde (of zich daarin specialiserende) politiemedewerkers en zaaksofficieren van het O.M. en heeft als doel om resultaten te bereiken in de aanpak van digitale criminaliteit door het werkproces efficiënter te maken en hierdoor de basisteams te ondersteunen (bron: intranet, politie).

10 Ondertussen wordt de digitale meldkamer bij meerdere eenheden geïmplementeerd of zijn daar ontwikkelingen gaande.

crime handboek en het Vriend-In-Nood-fraude (VIN) hulpmiddel (waarin informatie wordt toegestuurd naar de aangever die de informatie zelf moet aanleveren). Zij halen deze informatie van intranet en één geïnterviewde bewaart een geprinte map met handleidingen voor veelvoorkomende oplichting in zijn kluisje. *‘Er zijn meer collega’s die ze vinden, maar nog niet iedereen. Ik heb ook mails opgesteld met linkjes erin waar dingen te vinden zijn, maar nog niet iedereen gebruikt het.’* (PV10)

Enkele geïnterviewden in Lichtblauwveen gaven aan dat zij behoefte hebben aan hulpmiddelen. Het betreffende basisteam heeft enkele weken voor het interview een digitale hulplijn (digitaal informatiepunt) gekregen waar zij vragen kunnen stellen. In Postenveld is het digitaal platform het aanspreekpunt bij vragen over online criminaliteit:

*‘Daar kon je dan aangifte van opnemen. Zij ontwikkelde ook brieven en handelingskaders, met bankhelpdeskfraude, dat was een formulier wat je kon toesturen naar mensen, formulieren met vragen die je kon stellen (opgesteld met digitaal platform) met informatie die belangrijk was. Die formulieren met werkwijze moeten we invoeren hier, wat ik met leidinggevende besproken heb. De formulieren toesturen naar slachtoffers vonden ze heel fijn, en kreeg ik snel terug. Dat ook geprobeerd naar de collega’s te krijgen, vonden ze moeilijk en ze zien het gemak er niet van in. Daardoor krijg je aangiften terug omdat er informatie mist of opsporing moest er weer achter aan.’* (PV10)

### 3.5 Teamontwikkeling

Wij hebben gevraagd op welke manier de respondenten zich willen ontwikkelen in kennis en vaardigheden aangaande de aanpak van online criminaliteit en welke leervormen eerder voor hen hebben gewerkt. De politiemensen geven de voorkeur aan een *learning by doing* aanpak, waarbij ze werken met echte zaken of realistische casuïstiek. Ze willen graag leren van collega’s binnen de politie of van externe partners om online criminaliteit effectiever aan te pakken. Succesverhalen van collega’s over succesvolle opsporing, inbeslagname en vervolging verhogen hun motivatie om online criminaliteit aan te pakken, aldus de respondenten

In Postenveld wordt de ‘triage’ aanpak als positief ervaren. Triage is een werkwijze waarin wordt besproken welke aangiften opgepakt worden en welke vragen gesteld moeten worden voor een betere aangifte. Ten tijde van de interviews was iemand van het digitaal platform eenmalig langs geweest en was het voornemen dat verschillende inhoudelijke experts periodiek zouden aansluiten tijdens de triage, vanuit het digitaal platform en financiële opsporing.

*‘De belangrijkste parate kennis is door kennis te delen tijdens de triage. Ze krijgen de meldingen binnen in service portaal, dat komt bij het Regionaal service centrum binnen. Soms staan er twee/drie zinnen waar je niks mee kan, soms wel en dan is er een discussie wat er staat. Dan gaan we ze de vijf eerste vragen bij langs (is het wat voor*

*de opsporing, is het strafbaar, et cetera.) en als dat allemaal ja is, dan maken ze er een aangifte van.’ (PV09)*

In Lichtblauwveen wordt de digitale hulplijn (digitaal informatiepunt) zeer positief ervaren, omdat medewerkers een collega met expertise hebben aan wie zij telefonisch vragen kunnen stellen. Verder worden hier een training van een ICT-expert over veilig online zoeken en een cursus witwassen bestrijden als positieve interventies genoemd. In Postenveld betrof dit webinars en een presentatie van het digitaal platform. Opvallend is dat het webinar werd georganiseerd vanuit de eenheid waarin Lichtblauwveen actief is, terwijl de geïnterviewden binnen Lichtblauwveen dit zelf niet als interventie hebben genoemd.

Er zijn ook verschillende ingezette interventies die negatief door de geïnterviewden zijn ervaren:

*‘Al volg ik tien keer dezelfde workshop, het kwartje valt niet.’ (LV18)*

*‘Soms zit je bij een voorlichting, maar bij sommige termen zoals dit denk ik echt: ik lig eraf, want ik heb geen idee wat het betekent. Je moet echt bij de basis beginnen om ze erin mee te nemen. Het is lastig om ze ervoor te enthousiasmeren.’ (LV17)*

*‘Je hebt het Inspiratiepunt. Dat zijn cursussen waarvoor je je kan opgeven. In de praktijk is het vaak zo dat daar geen tijd voor is. We kunnen niet overal naartoe, omdat het werk gewoon doorgaat. De agenda staat vol. Dat gaat voor.’ (LV13)*

De meeste ontevredenheid werd geuit over de e-learning als leermiddel. In Postenveld worden daarnaast mails gestuurd met bijvoorbeeld links naar hulpmiddelen voor de aanpak van online criminaliteit, maar dit wordt gezien als te veel leeswerk. In Lichtblauwveen worden workshops of voorlichtingen georganiseerd die niet goed aansluiten bij de doelgroep. Ook worden cursussen verzorgd op het gebied van online criminaliteit (inspiratiepunten) waar gevoelsmatig geen tijd voor is.

Van andere interventies is niet duidelijk of deze positief of negatief zijn ervaren. In Postenveld wordt bijvoorbeeld informatie gedeeld via BBM Enterprise (een variant op WhatsApp dat door de politie wordt gebruikt) en een presentatie gegeven door Cybercrimeteam. Tevens is het basisteam Postenveld voornemens om een aantal collega's te stimuleren om naar de landelijke GGP Digi Vakdag te gaan. Op deze vakdag komen netwerkpartners samen en worden verschillende workshops georganiseerd over digitalisering en politiewerk. In Lichtblauwveen zijn workshops binnen de clusters uitgezet en is een hulpkoffer aangeboden voor meldingen van online criminaliteit.

De laatste jaren zijn de basisteams ontwikkeld in hun aanpak van online criminaliteit, maar niet alle geïnterviewden zien dit hetzelfde. De één vindt dat er 'enorme stappen zijn gezet' (PV13), terwijl de ander de gezette stappen veel te weinig vindt (PV08). Een geïnterviewde van VVC geeft aan dat de kwaliteit van aangiften beter is geworden. Er

wordt over het algemeen wel verbetering gezien, maar iedereen is het erover eens dat de verbetering in de aanpak van online criminaliteit te langzaam gaat.

Op basis van de resultaten lijkt het erop dat een *hands-on* praktische benadering beter werkt voor deze doelgroep. Een geïnterviewde zegt dan ook: *‘Zolang het praktisch is, dan leren we wel.’* (PV01) De politiemensen lijken het liefste en meeste te leren van echte zaken en contact met politiecollega’s met meer expertise. Een theoretische benadering die niet direct bruikbaar is voor de praktijk wordt minder goed ontvangen.

### 3.6 Behoeften in de lokale aanpak van online criminaliteit

Aan de politiemensen is gevraagd welke kennis en vaardigheden zij nodig hebben om online criminaliteit beter aan te pakken. Ook hun behoeften en randvoorwaarden voor deze ontwikkeling, zoals interventies, zijn bevraagd.

#### 3.6.1 Benodigde kennis en vaardigheden

Om online criminaliteit lokaal beter aan te pakken vinden de geïnterviewden het belangrijk dat zij verschillende vormen van online criminaliteit, zowel online als offline, kennen en herkennen. Zij moeten in staat zijn online criminaliteit te definiëren en te onderscheiden van offline criminaliteit. Dit vraagt om een helder begrip van wat er wel en niet onder specifieke criminaliteitsvormen valt, en inzicht in de bijbehorende trends en ontwikkelingen, zoals de nieuwste *modus operandi* van criminelen. Hiervoor is het ook van belang dat politiemensen een goed begrip hebben van relevante begrippen, zoals ‘wallets’ en ‘crypto currency’, die veelvuldig voorkomen binnen online criminaliteit.

Daarnaast vinden politiemensen dat zij opsporingsmogelijkheden van digitale sporen moeten herkennen: *‘Collega’s die op de auto zitten en die een melding krijgen van bankhelpdeskfraude, dat ze dan weten wat ze moeten doen, en waar ze op moeten letten. Dat de apparaten open moeten blijven staan bijvoorbeeld.’* (PV13)

Een belangrijk onderdeel hiervan is het identificeren van digitale sporen, zoals gegevens op telefoons, laptops of pc’s van aangevers, en het correct registreren en overdragen aan gespecialiseerde afdelingen binnen de politie voor verder onderzoek. Het juist herkennen en interpreteren van digitale sporen en vaststellen van opsporingsindicaties is zowel voor het basisteam als andere opsporingsteams binnen de politie belangrijk. Het vermogen om zelfstandig open bronnenonderzoek (OSINT) te verrichten is ook gewenst. Dit omvat het gebruik van open bronnen om digitale sporen vast te leggen en het proces van digitale opsporing te begrijpen, zodat informatie kan worden gebruikt in een (potentiële) zaak. Enkele geïnterviewden vinden dat politiemensen op het basisteam digitale gegevens moeten veiligstellen, terwijl anderen vinden dat dit een rol is van meer gespecialiseerde afdelingen. Daarbij vond de ene groep dit echt algemeen politiewerk wat elke medewerker moet kunnen waar de andere groep dit echt werk voor een specialist vond omdat de kans op het maken van fouten te groot werd geacht.

Verder vinden politiemensen dat ze voldoende kennis moeten hebben om correcte aangiften van online criminaliteit op te nemen en opsporingsmogelijkheden goed in kaart moeten kunnen brengen: *‘Als je zo’n melding krijgt of dat je tegelijk ter plaatse kan gaan en dingen in beslag kan nemen. Of als er een aangever komt dat je dan zegt: ‘hé je moet je laptop meenemen die wil ik in beslag nemen om daar verder in te kijken.’ (PV14)* Politiemensen moeten weten welke gegevens zij moeten verzamelen, zoals telefoonnummers, gespreksgeschiedenis en screenshots, en hoe deze bewijzen op de juiste wijze vastgelegd en gedocumenteerd moeten worden:

*‘Als je een huis binnenkomt en er schijnt een modem te zijn die wifi verbinding maakt met de telefoons en tien telefoons kan onthouden. Het is belangrijk om je wifi uit te zetten als je naar binnen gaat. Als je daar niet bij stilstaat dan hebben we tien politieagenten die naar binnen lopen met tien keer wifi aan. Die router maakt een verbinding met de telefoons, maar de telefoons van de criminelen is het dan weer vergeten. Dat zijn allemaal dingen waar we ons bewust van moeten zijn.’ (PV02)*

Tevens moeten zij bekend zijn met de juridische kaders die van toepassing zijn op online criminaliteit, zoals relevante wetgeving en strafbare feiten en met de wettelijke vereisten waaraan zij zelf moeten voldoen tijdens de opsporing en aangiftebehandeling.

Ten slotte is een juiste omgang met slachtoffers essentieel. Het is daarbij belangrijk om voldoende empathie te tonen richting het slachtoffer. Daarnaast willen politiemensen weten hoe zij slachtoffers kunnen informeren over vervolgstappen na een aangifte om slachtoffers op weg te helpen en potentieel herhaald slachtofferschap te voorkomen. Een geïnterviewde gaf aan dat er ook interesse is in de achterliggende motieven van daders en slachtoffers, om beter te begrijpen waarom criminelen online criminaliteit plegen en waarom mensen slachtoffer worden.

### 3.6.2 *Randvoorwaarden interventies*

Er is aan de geïnterviewden gevraagd wat nodig is om de aanpak van online criminaliteit te verbeteren. De eerste factor is de afweging tussen prioriteit en capaciteit. Een belangrijke randvoorwaarde voor de aanpak van online criminaliteit is de mate waarin politie en het Openbaar Ministerie deze vorm van criminaliteit prioriteren. In de praktijk kan de politie specifieke doelen stellen, zoals het jaarlijks behandelen van een vastgesteld aantal zaken (PV07). Echter, uit interviews blijkt dat in Postenveld weinig sturing of richtlijnen vanuit de leiding wordt ervaren op het gebied van online criminaliteit. Dit gebrek aan ervaren prioriteit van online criminaliteit werkt belemmerend voor een effectieve aanpak. Ook uit interviews op het basisteam in Lichtblauwveen komen geluiden over behoeften aan scherpere prioritering omtrent online criminaliteit: *‘We moeten keuzes maken in wat we belangrijk vinden en prioriteren. Ik denk dat we daar nog wel wat in te doen hebben.’ (LV03)*

Uit de interviews komt verder naar voren dat een gebrek aan capaciteit vaak een rol speelt in het oppakken van zaken rond online criminaliteit, dit heeft vaak impact op de prioriteit: *‘Als wij er 100 man bij zouden krijgen – dat is een utopie, maar dat zou mooi zijn – dan kun je wat doen. Nu is het constant kiezen: Wat gaan we niet doen? Het trieste is dat het niet lukt om ook de simpele zaken op te pakken. Als ze te groot zijn hebben we geen capaciteit. Als ze te klein zijn, zijn ze niet belangrijk genoeg.’* (LV04)

Er wordt ook gerefereerd aan de belevingswereld van politiewerknemers op de werkvloer. Een beleving van weinig capaciteit en prioriteit dat impact heeft op handelen: *‘Het wordt beleefd dat wij daar [online criminaliteitszaken] geen tijd voor hebben. Dus zo wordt dat beleefd, wij hebben geen tijd, we hebben geen capaciteit voor deze zaken en zo wordt dat beleefd door collega’s.’* (LV02)

Een probleem wat ook in de literatuur naar voren komt en uit de interviews is de lage motivatie voor en onzekerheid over het aanpakken van online criminaliteit, resulterend in het vermijden van deze zaken. Sommige geïnterviewden gaven aan online criminaliteit te mijden, omdat ze niet weten hoe ze deze moeten behandelen. Een geïnterviewde beschrijft dit als volgt: *‘Mensen die onzeker worden van de materie die ze voorgelegd krijgen, slaan dicht en gaan aan zichzelf twijfelen: waarom snap ik dit nou niet?’* (PV01)

Het lijkt erop dat politiewerknemers proactief andere taken op zich nemen om online-gerelateerde zaken te ontwijken: *‘Ik wil niet zeggen [dat ik een] negatief [beeld heb over online criminaliteitszaken], maar het is wel een ver-van-mijn-bed-show. Nog niet alles, maar wel veel. Onbekend, onbemand. Laat het alsjeblieft daar liggen. Doe mij de drugsdealer maar. Dat vind ik makkelijker. Als je mij nu de straat opstuurt, kun je mij beter een drugs crimineel laten pakken. Dan weet ik van vroeger nog hoe het werkt. Als je mij nu [vraagt] om die Whatsappfraude op te lossen, heb ik een probleem. Dan moet ik allerlei machtigingen gaan schrijven en vorderingen gaan doen.’* (LV07)

De handelingskaders – route naar een oplossing – lijken helderder te zijn in de offline wereld dan in het online landschap.

Een andere belemmering is de beperkte slagkracht van de politieorganisatie. De bureaucratische structuur zorgt ervoor dat initiatieven om online criminaliteit tegen te gaan, zoals preventieve voorlichting over bankhelpdeskfraude, pas maanden of zelfs een jaar na het voorstel kan worden uitgevoerd, aldus een van de geïnterviewden. Deze geïnterviewde noemt als knelpunt dat beslissingen langs te veel personen moeten, waardoor initiatieven doodlopen.

Een succesfactor is de samenwerking tussen basisteams en specialisten, zoals het Digitaal Platform, het Team Digitale Opsporing en het Cybercrimeteam. In de eenheid Noord-Nederland is het Digitaal Platform een ondersteunende dienst, die geen opsporingsonderzoeken draait. Het platform is een vraagbaak en ondersteunt bij digitale aspecten van onderzoeken, zoals het uitlezen van telefoons. Echter, de geïnterviewden geven aan dat de samenwerking bemoeilijkt wordt door onduidelijke aanspreekpunten en meerdere doorverwijzingen tussen afdelingen. Dit leidt tot frustratie en demotivatie onder agenten, wat ook de aanpak van online criminaliteit belemmert.

Er zijn wisselende meningen over de behoefte aan technische ondersteuning en hulpmiddelen. Een geïnterviewde vraagt om meer hulp bij het uitlezen en analyseren van telefoongegevens door het Digitaal Platform. Terwijl een andere geïnterviewde aangeeft dat het digitaal platform transferium waar alle data uit de telefoon onderzocht kunnen worden, juist als prettig wordt ervaren.

Een gedeelde mening onder de geïnterviewden is dat meer kennis en expertise over online criminaliteit binnen de politie essentieel zijn. Informatie moet toegankelijk en praktisch toepasbaar zijn. Het zou volgens hen helpen om beeldmateriaal te gebruiken zoals vlogs en visuele hulpmiddelen in plaats van lange teksten. Praktijkgerichte activiteiten, zoals oefendagen en casusgerichte trainingen, worden als effectiever ingeschat dan e-learningen of handleidingen.

### 3.6.3 Interventies

In deze paragraaf worden verschillende potentiële interventies besproken. De eerste potentiële interventie is een gerichte personele ingezet. Hoewel de geïnterviewden initieel aangaven zelf beter op de hoogte te willen zijn, geven geïnterviewden in deze fase van het interview aan dat ze liever specifieke politiemensen aanwijzen binnen basisteams die zich richten op online criminaliteit. In andere eenheden worden ‘digi-coaches’, ‘digi-profs’ of ‘digi-vrijwilligers’ ingezet, die collega’s kunnen ondersteunen en motiveren bij online criminaliteitszaken, zonder dat zij deze overnemen. Het aanstellen van politiemensen met een natuurlijke affiniteit voor online criminaliteit kan helpen om de doorgaans lage motivatie te verhogen en kennisdeling te stimuleren. Tevens kan HR-beleid hierbij ondersteunen, door bijvoorbeeld nieuwe kandidaten aan te nemen met een interesse op het gebied van digitale kennis en vaardigheden.

Er wordt ook gesproken over een vast kernteam die de rest ‘besmet’: *‘Maar het gaat meer om bevlekken en besmetten, daar zit die veel meer als je daar de juiste mensen neerzet. Dan gaat het stapje voor stapje.’* (LV03)

In andere bewoording wordt er gesproken over het effect dat een ‘clubje’ binnen het basisteam wordt opgericht, die zich bezighoudt met online criminaliteit aangiften: *‘Ik denk dat je binnen je basisteam een clubje mensen moet hebben, bijvoorbeeld onder begeleiding van [geanonimiseerde naam van digitaal expert], die via het OCP dit soort aangiften gaat krijgen, weten welke vorderingen ze nodig hebben en daar tijd voor krijgen. Dat zijn mensen met een bepaalde achtergrond.’* De argumentatie rond deze verwijzing naar ‘anderen moeten het oppakken’ lijkt verbonden te zijn met hoe de werknemer zijn of haar functie en bijbehorende vaardigheden beschouwd: *‘Voor mij is het soms: je zit achter de knuppel van een vliegtuig. Je hebt nog nooit één les gehad. Taxi dat ding maar van gate A naar gate B. Dat lukt niet.’* (LV01)

De tweede potentiële interventie – nadat medewerkers door hun collega’s zijn ‘besmet’ met de aanpak van online criminaliteit – is opleiding en kennisontwikkeling. Digitale kennis en vaardigheden moeten structureel opgenomen worden in de politieopleiding, zodat politiemensen ‘startbekwaam’ met voldoende digitale basiskennis, naar de basisteams komen. Dit geldt niet alleen voor politiewerknemers die instromen, maar ook op

het gebied van doorontwikkeling: *‘Als je wilt dat ik met een opleiding in die wereld duik van digitale fraude en moet leren hoe dat werkt en wat je daarvoor nodig hebt – met IP-adressen opzoeken, DDoS-aanvallen of bedreigingen, en erachter komen wie de verdachte is – zeg ik: ja oké. Ik ben niet opgegroeid met die dingen. Ik moet het me dan eigen maken, maar wel op mijn tempo. De jongere generatie is geboren met zo’n ding in de wieg.’* (LV01)

Daarnaast kan in de praktijk verder worden geleerd door middel van praktijkgerichte trainingen met casuïstiek. Een specifiek voorbeeld wat is benoemd: een opleiding waarin aangiften van vormen van online criminaliteit worden opgenomen. Zelfstudie, bijvoorbeeld door het volgen van e-learnings en webinars of het raadplegen van de webapp cybercrime, wordt over het algemeen als minder effectief beschouwd. Er zijn echter uitzonderingen. Er is één geïnterviewde die juist de ‘Tech Gym Live’ webinars over technologische ontwikkelingen volgt. Samenwerking met collega’s met meer expertise wordt vooral gezien als een effectieve manier om kennis te vergroten.

Aanvullend is er behoefte aan betere informatievoorziening. Er is veel informatie te vinden binnen het intranet, maar het is niet duidelijk waar het is te vinden of wordt in de praktijk niet gebruikt. Agora wordt als onoverzichtelijk ervaren en kennisbanken worden weinig gebruikt. Er lijkt behoefte te zijn aan een kennismanagementsysteem met de juiste kennis op het juiste moment. Hierbij wordt verwezen naar beslisbomen en handelingskaders.

*‘Misschien ook een handelingskader zodat je direct op straat hulp kunt vragen. Van de politieacademie had je van die apps. Dat zijn beslisbomen. Je kunt dan doorklikken. Ik tref op straat een auto met de aanhanger. Ik weet niet of het mag, maar hij ziet er zo en zo uit. Dan klik ik erop. Dan komt eruit wat de eisen zijn. Voldoet die daaraan? Nee. Dan kun je die bekeuring schrijven. Is er nog meer aan de hand? Ja. Wat? Zo kun je verder. [Interviewer vraagt: ‘Checklists?’]. Precies. Dat zou je voor digitaal ook kunnen doen. Het mooiste zou zijn als het verweven zit in je RAPP. Ik tref dit strafbare feit of ik krijg hiermee van doen. Dat je op een i’tje kunt drukken. Denk hieraan en wil je meer informatie hierover, klik dan daarop. Dan kom je bij die beslisboom uit. Dan kun je het zo helemaal doorlopen. Dat je het een beetje beschikbaar maakt. Een beetje on-demand naslagwerk. Dat is wat je nodig hebt, want je gaat het niet allemaal onthouden.’* (LV16)

Om politiemensen te motiveren om online criminaliteit aan te pakken, kan het regelmatig delen van concrete succesverhalen motiverend werken en de drempel verlagen om toekomstige online zaken op te pakken. In Postenveld wordt met enige regelmaat een update gestuurd met alle zaken die ze hebben opgepakt en wat het vervolg is geweest. Dit kan ook demotiverend werken als er veel zaken zijn geseponneerd. Het is dus belangrijk om realistische verwachtingen te scheppen.

In Lichtblauwveen wordt ook gesproken over succesverhalen, specifiek voor het verhogen van affiniteit en motivatie onder de politiemensen. Op de vraag ‘Hoe krijg je politiemensen aan het werk op dit online thema?’ wordt geantwoord:

*'Het is niet zo moeilijk, alleen het is onbekend. Je zou ervoor moeten zorgen dat ze er meer mee in aanraking komen. Ook meer met de verhalen die erachter zitten. Bijvoorbeeld een woninginbraak is vaste prik, maar als mensen dan geëmotioneerd zijn of daar een verhaal bij hebben, dan wil je er harder voor lopen. Het zou niet mogen, maar zo werkt het nou eenmaal. Je moet de verhalen horen. We doen ook nu het project van de digitale meldkamer. Volgens mij heeft dat dezelfde insteek. Dat je geconfronteerd wordt met het leed wat er is, zodat je politiehart wat sneller gaat kloppen. Ik denk dat dat een goede impuls is.'* (LV16)

Er wordt hier dus gesproken van zowel succesverhalen als slachtofferverhalen om het leed tastbaar te maken. Deze insteek wordt door meerdere geïnterviewden in Lichtblauwveen gedragen. *'Misschien dat ze toch een beetje zouden schrikken van hoeveel zaken of wat de impact is van slachtoffers, want dat blijft altijd een beetje achterwege.'* (LV09)

Bijna alle geïnterviewden geven aan dat politiemensen het beste leren door te doen: *learning by doing*. Er zijn verschillende concrete voorstellen gedaan voor praktische initiatieven en samenwerkingen. Zoals de clusterdagen, meeloopdagen op andere afdelingen (om ervaring op te doen), het gebruikmaken van menukaarten, het gebruiken van een digitale wegwijzer voor slachtoffers om ze verder te verwijzen en gezamenlijke actieweken voor bijvoorbeeld het aanpakken van geldezels.



## 4 Vragenlijstresultaten basisteams

In de vragenlijst wordt ingegaan op huidige werkzaamheden van basisteammedewerkers die te maken hebben met online criminaliteit, welke kennis en vaardigheden respondenten hebben en missen in hun werk en waar de mogelijkheden liggen om de lokale aanpak te intensiveren en op welke wijze dat effectief kan. Tevens worden bij enkele vragen verschillen tussen functiegroepen weergegeven, voor zover relevant. Alleen significante verschillen ( $p < 0,05$ ) met een voldoende effectgrootte en/of absolute verschillen worden toegelicht (zie paragraaf 2.3).

### 4.1 Werkzaamheden van respondenten

Aan respondenten is gevraagd welke omschrijving het beste past bij hun dagelijkse werkzaamheden binnen het basisteam. Er is gevraagd naar vier algemene functiegroepen (gebaseerd op Jansen et al., 2020). In tabel 4.1 is te zien dat de grootste groep respondenten werkzaam is binnen de incidentenafhandeling, daarna de Basisteamrecherche en de kleinste groepen zijn leidinggevenden of vergelijkbare werkzaamheden (hierna: leidinggevende) en I&S.

Van de groep die 'anders, namelijk' heeft ingevuld, beschrijven de meesten werkzaamheden in de wijk of zijn wijkagent ( $n = 25$ , waarvan  $n = 5$  digitaal wijkagent). Andere werkzaamheden zijn onder andere casescreeening, ondersteuning aan andere afdelingen, bedrijfsvoering, praktijkbegeleider, taakaccenthouder Cybercrime en thematische werkzaamheden voor ondermijning/jeugd. Op basis van deze werkzaamheden hebben respondenten specifieke vragen gekregen over kennis en vaardigheden die passen bij hun functie.

Tabel 4.1 Omschrijving die volgens respondenten het beste past bij hun dagelijkse werkzaamheden

| Werkzaamheden                                | Aantal respondenten | Percentage |
|----------------------------------------------|---------------------|------------|
| Incidentafhandeling                          | 94                  | 34,2       |
| Basisteamrecherche/opsporing (VVC/crimeteam) | 46                  | 16,7       |
| Leidinggevende of operationeel specialist    | 35                  | 12,7       |
| I&S                                          | 32                  | 11,6       |
| Anders, namelijk                             | 68                  | 24,7       |
| <b>Totaal</b>                                | <b>275</b>          | <b>100</b> |

## 4.2 **Bekendheid met en de aanpak van online criminaliteitsvormen bij basisteams**

### 4.2.1 *Bekendheid met online criminaliteitsvormen*

Aan de respondenten is gevraagd hoever hun kennis rijkt ten aanzien van online criminaliteitsvormen, in hoeverre zij er in hun werkzaamheden mee te maken hebben gehad, en hoe bekwaam zij zichzelf achten in het aanpakken van online criminaliteit. Deze vragen zijn gesteld voor tien verschillende criminaliteitsvormen.

De geselecteerde online criminaliteitsvormen in de vragenlijst zijn gebaseerd op het Toewijzingskader Cybercrime en Digitalisering en Cybercrime (2023). Ter herinnering, dit voorgenomen beleidsstuk stelt vast dat politiebasissteams enkelvoudige zaken met een lage complexiteit, zoals voldoende opsporingsindicaties en een lage politieke gevoeligheid, dienen op te pakken. Daaruit zijn drie gedigitaliseerde criminaliteitsvormen met lage complexiteit gekozen (geldezel/katvanger, sextortion (zonder letsel of dood) en cyberpesten) en drie cybercriminaliteitsvormen met lage complexiteit (diefstal van gegevens, eenvoudige DDoS-aanvallen en eenvoudige hacking waarbij dader(s) bekend is/zijn). Tevens zijn de vier criminaliteitsvormen van Project Centurion uitgevraagd (aan- en verkoopfraude, hulpvraagfraude, telefonische helpdeskfraude en phishing).

Tabel 4.2 toont de gerapporteerde mate van kennis van respondenten met de bevroegde vormen van online criminaliteit. Hulpvraagfraude<sup>11</sup> (76%) en telefonische hulpvraagfraude<sup>12</sup> (74,9%) zijn de vormen van online criminaliteit waar de respondenten de meeste kennis van hebben. Ook zijn zij naar eigen zeggen goed op de hoogte van de fenomenen geldezel/katvanger (68,7%) en cyberpesten (66,5%). Van phishing (60,7%), diefstal van persoonlijke gegevens (58,9%) en aan- en verkoopfraude (58,5%) hebben zij naar hun eigen inschatting een relatief minder goed beeld dan van hulpvraag- helpdeskfraude. In lijn met de interviewresultaten hebben de respondenten meer kennis van gedigitaliseerde criminaliteitsvormen en de vormen die horen bij Project Centurion dan van cybercriminaliteitsvormen. Bij DDoS-aanvallen (55,3%) en hacking (47,3%) geeft een groot deel van de respondenten aan dat zij maar ‘enigszins’ weten wat deze criminaliteitsvormen inhouden. Een relatief grote groep is niet bekend met wat DDoS-aanvallen (14,2%) en sextortion (9,1%) inhouden.

11 Hulpvraagfraude zoals Vriend-in-noodfraude/ WhatsAppfraude.

12 Telefonische helpdeskfraude zoals Bank-/helpdeskfraude.

Tabel 4.2 Kennis van online criminaliteitsvormen (n = 275, in percentages)

| Online criminaliteitsvorm          | Ik ken dit niet | Ik ken dit enigszins | Ik ken dit goed |
|------------------------------------|-----------------|----------------------|-----------------|
| Hulpvraagfraude                    | 1,8             | 22,2                 | 76,0            |
| Telefonische helpdeskfraude        | 1,1             | 24,0                 | 74,9            |
| Werken als een geldezel/katvanger  | 1,8             | 29,5                 | 68,7            |
| Cyberpesten                        | 3,3             | 30,2                 | 66,5            |
| Phishing                           | 1,8             | 37,5                 | 60,7            |
| Diefstal van persoonlijke gegevens | 2,9             | 38,2                 | 58,9            |
| Aan- en verkoopfraude              | 4,7             | 36,7                 | 58,5            |
| Sextortion                         | 9,1             | 41,8                 | 49,1            |
| Hacking                            | 4,7             | 47,3                 | 48,0            |
| DDoS-aanvallen                     | 14,2            | 55,3                 | 30,5            |

Vervolgens is gevraagd in hoeverre respondenten vanuit hun werk in de basisteams betrokken zijn geweest bij online criminaliteitszaken (zie tabel 4.3). De zaken die worden geprioriteerd in Project Centurion komen het vaakst voor op dagelijkse/maandelijkse basis. Telefonische helpdeskfraude (27,3%) wordt het vaakst behandeld op dagelijkse of wekelijkse basis, gevolgd door aan- en verkoopfraude (17,4%), hulpvraagfraude (17,1%) en phishing (17%). Daarentegen worden DDoS-aanvallen (zelden 21,5%,<sup>13</sup> 57,1% nooit) en hacking (25,8% zelden, 42,5% nooit) door de meerderheid nauwelijks of helemaal niet behandeld. De respondenten komen in hun werk dus het minst in aanraking met cybercriminaliteitsvormen.

13 Eén of enkele keren per jaar.

Tabel 4.3 Hoe vaak bent in u de afgelopen twaalf maanden binnen het basisteam betrokken geweest bij zaken over online criminaliteit (n = 275, in percentages)

| Online criminaliteitsvorm                                      | Dagelijks/<br>wekelijks | Maandelijks/<br>elk kwartaal | Eén of enkele<br>keren per jaar | Nooit | Totaal |
|----------------------------------------------------------------|-------------------------|------------------------------|---------------------------------|-------|--------|
| Telefonische helpdeskfraude                                    | 27,3                    | 40,0                         | 23,3                            | 8,4   | 98,9   |
| Aan- en verkoopfraude                                          | 17,4                    | 36,7                         | 25,1                            | 16    | 95,3   |
| Hulpvraagfraude                                                | 17,1                    | 35,6                         | 30,2                            | 15,3  | 98,2   |
| Phishing                                                       | 17,0                    | 24,7                         | 28,7                            | 27,6  | 98,2   |
| Een zaak waarbij een geldezel/<br>katvanger betrokken is       | 11,0                    | 30,5                         | 39,3                            | 17,5  | 98,2   |
| Diefstal van persoonlijke gegevens                             | 9,9                     | 25,5                         | 39,3                            | 22,5  | 97,1   |
| Cyberpesten                                                    | 6,9                     | 34,2                         | 26,9                            | 28,7  | 96,7   |
| Sextortion                                                     | 6,9                     | 26,6                         | 31,3                            | 26,2  | 90,9   |
| Eenvoudige hacking (waarbij dader(s)<br>bekend is/zijn)        | 6,2                     | 20,7                         | 25,8                            | 42,5  | 95,3   |
| Eenvoudige DDoS-aanvallen (waarbij<br>dader(s) bekend is/zijn) | 0,7                     | 6,5                          | 21,5                            | 57,1  | 85,8   |

Er is ook gevraagd in hoeverre de respondenten zichzelf bekwaam achten om vormen van online criminaliteit aan te pakken (zie tabel 4.4). Met ‘aanpakken’ bedoelen wij alle werkzaamheden in relatie tot online criminaliteit die uitgevoerd kunnen worden op een basisteam, zoals aangiften opnemen/screenen, opsporen, herkennen van digitale sporen et cetera. Dit is sterk afhankelijk van de online criminaliteitsvorm. Het algemene beeld is dat meer dan driekwart van de respondenten (enigszins) weet hoe ze de meeste online criminaliteitszaken moeten aanpakken.

Telefonische helpdeskfraude wordt het vaakst aangeduid als een criminaliteitsvorm die men goed aan kan pakken, de helft (50,2%) van de respondenten geeft namelijk aan dit te weten. Daarna volgen hulpvraagfraude (42,5%) en aan- en verkoopfraude (39,3%), waarin de meeste respondenten weten hoe ze dit (enigszins, respectievelijk 41,8% en 42,2%) moeten aanpakken. Bij de meeste vormen van online criminaliteit, zoals diefstal van persoonlijke gegevens (53,1%), sextortion (48,4%), cyberpesten (49,1%) en zaken met geldezels (48,0%) geeft een groot deel van de respondenten aan dat ze ‘enigszins’ weten hoe ze dit moeten aanpakken. Bij meer technisch complexe vormen, zoals DDoS-aanvallen (68,4%), hacking (46,9%), phishing (31,3%) en diefstal van persoonlijke gegevens (25,1%) geven de meeste respondenten aan niet te weten hoe ze dit moeten aanpakken. Slechts een kleine groep geeft aan dit wel te weten (DDoS-aanvallen 6,5% en hacking 16,4%).

Tabel 4.4 Hoe goed weet u hoe u deze online criminaliteitsvorm kunt aanpakken in uw werk? (n = 275, in percentages)

| Online criminaliteitsvorm                                                                                                                      | Ik weet <i>niet</i> hoe ik het moet aanpakken | Ik weet <i>enigszins</i> hoe ik het moet aanpakken | Ik weet <i>wel</i> hoe ik het moet aanpakken |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------|----------------------------------------------|
| Telefonische helpdeskfraude*                                                                                                                   | 11,3                                          | 38,5                                               | 50,2                                         |
| Hulpvraagfraude*                                                                                                                               | 15,6                                          | 41,8                                               | 42,5                                         |
| Aan- en verkoopfraude*                                                                                                                         | 18,5                                          | 42,2                                               | 39,3                                         |
| Een zaak waarbij een geldezel/katvanger betrokken is*                                                                                          | 16,7                                          | 48                                                 | 35,3                                         |
| Sextortion*                                                                                                                                    | 23,3                                          | 48,4                                               | 28,4                                         |
| Cyberpesten*                                                                                                                                   | 22,9                                          | 49,1                                               | 28,0                                         |
| Phishing*                                                                                                                                      | 31,3                                          | 42,2                                               | 26,5                                         |
| Diefstal van persoonlijke gegevens*                                                                                                            | 25,1                                          | 53,1                                               | 21,8                                         |
| Eenvoudige hacking (waarbij dader(s) bekend is/zijn)*                                                                                          | 46,9                                          | 36,7                                               | 16,4                                         |
| Eenvoudige DDoS-aanvallen (waarbij dader(s) bekend is/zijn)                                                                                    | 68,4                                          | 25,1                                               | 6,5                                          |
| * Notitie. Er is een vergelijkende analyse uitgevoerd om de verschillen tussen de functiegroepen op deze vraag te onderzoeken (zie tabel 4.6). |                                               |                                                    |                                              |

#### 4.2.2 *Vergelijking tussen functiegroepen*

Om meer inzicht te krijgen in eventuele verschillen in antwoorden over online criminaliteit tussen de functiegroepen (I&S, incidentafhandeling, basisteamrecherche, leidinggevend en 'anders') binnen hun basisteams is een vergelijkende analyse uitgevoerd. Alle functiegroepen zijn met elkaar vergeleken. In deze paragraaf worden alleen de significante verschillen toegelicht.

De eerste vergelijking gaat over hoe vaak men in het afgelopen jaar betrokken was bij online criminaliteitszaken (zie ook tabel 4.3 voor percentages van alle respondenten). Bij deze vraag gaven respondenten aan in hoeverre zij de afgelopen twaalf maanden betrokken zijn geweest bij een specifieke vorm van online criminaliteit. Er is voor de verschillende groepen in kaart gebracht welke online criminaliteitsvormen ze het meest en het minst bij betrokken zijn geweest (zie tabel 4.5). Daarbij is per groep gekeken welk deel van de respondenten wekelijks of vaker betrokken was en welk deel zelden tot nooit.<sup>14</sup>

Er zijn weinig verschillen tussen de groepen in de mate van betrokkenheid bij verschillende vormen van online criminaliteit. Alle groepen hebben het vaakst te maken gehad met telefonische helpdeskfraude en daarna hulpvraagfraude en aan- en verkoopfraude. Opvallend is dat ongeveer de helft van de I&S respondenten aangeeft deze vormen van

14 De 'Anders'-functiegroep is niet meegenomen.

online criminaliteit vaak tegen te komen, terwijl dit bij andere groepen voor een (veel) kleiner percentage geldt. Verder geldt voor alle groepen dat ze zelden te maken met DDoS-aanvallen. Dit geldt ook voor hacken, met uitzondering van de I&S-groep.

Tabel 4.5 Online criminaliteitsvormen waar functiegroepen het meest en minst bij betrokken zijn geweest het afgelopen jaar

|                                                                                                                      | Online criminaliteitsvorm                                    | waar respondenten het vaakst* bij betrokken zijn geweest, in percentages | Online criminaliteitsvorm          | waar respondenten zelden** bij betrokken zijn geweest, in percentages |
|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--------------------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------------|
| <b>I&amp;S</b>                                                                                                       | Telefonische helpdeskfraude                                  | 56,3                                                                     | DDoS-aanvallen                     | 62,5                                                                  |
|                                                                                                                      | Aan- en verkoop-fraude                                       | 46,9                                                                     | Geldezels-zaken                    | 40,6                                                                  |
|                                                                                                                      | Phishing                                                     | 40,6                                                                     | Cyberpesten                        | 25,0                                                                  |
| <b>Incident-afhandeling</b>                                                                                          | Telefonische helpdeskfraude                                  | 21,3                                                                     | DDoS-aanvallen                     | 83,0                                                                  |
|                                                                                                                      | Hulpvraagfraude                                              | 12,8                                                                     | Hacking                            | 80,9                                                                  |
|                                                                                                                      | Phishing                                                     | 11,7                                                                     | Diefstal van persoonlijke gegevens | 70,2                                                                  |
| <b>Basisteam-recherche</b>                                                                                           | Telefonische helpdeskfraude                                  | 37,0                                                                     | DDoS-aanvallen                     | 76,1                                                                  |
|                                                                                                                      | Aan- en verkoop-fraude                                       | 30,4                                                                     | Hacking                            | 67,4                                                                  |
|                                                                                                                      | Hulpvraagfraude/ phishing                                    | 26,1                                                                     | Diefstal van persoonlijke gegevens | 58,7                                                                  |
| <b>Leiding-gevende</b>                                                                                               | Telefonische helpdeskfraude                                  | 20,0                                                                     | DDoS-aanvallen                     | 82,9                                                                  |
|                                                                                                                      | Phishing, hulpvraag-fraude, aan- en verkoopfraude, geldezels | 11,4                                                                     | Hacking                            | 74,3                                                                  |
|                                                                                                                      | Diefstal van persoonlijke gegevens, sextortion               | 8,6                                                                      | Cyberpesten, phishing              | 62,9                                                                  |
| Notitie. *vaak is maandelijks of vaker, ** zelden is enkele keren per jaar tot nooit in de afgelopen twaalf maanden. |                                                              |                                                                          |                                    |                                                                       |

Aanvullend is gekeken naar statistisch significante verschillen tussen functiegroepen.<sup>15</sup> Er zijn significante verschillen gevonden bij de betrokkenheid van alle online criminaliteitsvormen. Er zijn grote effecten gevonden bij hacking, diefstal van persoonlijke gegevens, sextortion en aan- en verkoopfraude. Middelgrote effecten zijn gevonden voor DDoS-aanvallen, phishing, werken als een katvanger/geldezel, hulpvraagfraude, telefonische helpdeskfraude en cyberpesten.

Als vervolgens naar de absolute verschillen wordt gekeken, beschrijven we alleen de grootste verschillen.<sup>16</sup>

- De leidinggevende groep scoort hoger dan de basisteamresearchgroep op het gebied van telefonische helpdeskfraude (absolute verschil = 0,639) en hulpvraagfraude (0,528).
- De basisteamresearchgroep scoort gemiddeld hoger dan de 'Anders'-groep op cyberpesten (0,533).
- De incidentafhandeling groep scoort gemiddeld hoger dan de leidinggevende groep bij zaken met een geldezel (0,545).
- De 'Anders'-groep scoort gemiddeld hoger bij zaken met een geldezel/katvanger in vergelijking met de leidinggevende groep (0,563).

De tweede vergelijkende analyse betreft het kunnen aanpakken van verschillende vormen van online criminaliteit (zie ook tabel 4.4 en 4.6). Aan respondenten is de vraag gesteld: *Hoe goed weet u hoe u deze online criminaliteitsvorm kunt aanpakken in uw werk?*

Alle groepen weten ongeveer allemaal even goed hoe ze bepaalde vormen van criminaliteit moeten aanpakken voor telefonische helpdeskfraude en hulpvraagfraude. Daarentegen hebben alle groepen de meeste moeite met het aanpakken van DDoS-aanvallen en hacking-zaken.

Als gekeken wordt naar de gemiddelden, dan valt op dat de I&S-groep het meest vertrouwen lijkt te hebben in de aanpak van online criminaliteit. Ter illustratie, telefonische helpdeskfraude is de criminaliteitsvorm waarvan relatief de meeste respondenten weten hoe ze deze moeten aanpakken. Zo geeft 78,1% van de I&S-respondenten aan dat zij telefonische helpdeskfraude kunnen aanpakken. Dit percentage ligt aanzienlijk

15 We hebben een vergelijkende ANOVA-analyse uitgevoerd om mogelijk verschillen tussen de functiegroepen te achterhalen. Er zijn significante verschillen gevonden bij alle online criminaliteitsvormen, met een Welch's significante van  $p < 0,001$  (phishing, aan- en verkoopfraude, telefonische helpdeskfraude, diefstal van persoonlijke gegevens, DDoS-aanvallen, hacking, sextortion en werken als een geldezel/katvanger),  $p = 0,001$  (hulpvraagfraude) en  $p = 0,002$  cyberpesten. De grootste effecten zijn gevonden bij hacking ( $\eta^2 = 0,254$ ), diefstal van persoonlijke gegevens ( $\eta^2 = 0,184$ ) sextortion ( $\eta^2 = 0,171$ ), aan- en verkoopfraude (0,149) en werken als een katvanger/geldezel ( $\eta^2 = 0,114$ ). Er zijn middelgrote effecten gevonden voor DDoS-aanvallen ( $\eta^2 = 0,129$ ), phishing ( $\eta^2 = 0,118$ ) en hulpvraagfraude ( $\eta^2 = 0,09$ ), telefonische helpdeskfraude ( $\eta^2 = 0,088$ ) en cyberpesten ( $\eta^2 = 0,084$ ).

16 In dit rapport worden alleen statistische significante resultaten beschreven waarbij het absolute verschil in gemiddelde scores tussen groepen minimaal 0,5 bedraagt. De vraag heeft een schaal van 1 (dagelijks) tot 6 (nooit). Als we geen onderscheid zouden maken in het absolute verschil, dan worden 42 statistische significante verschillen gevonden tussen de verschillende functiegroepen in de betrokkenheid bij online criminaliteitsvormen.

lager bij andere functiegroepen: 60,9% bij de basisteamrecherche, 40% bij de leidinggevenden en 39,4% bij de incidentafhandeling.

Een vergelijkbare verdeling is te zien bij Hulpvraagfraude. Van de I&S-respondenten geeft 75% aan dit te kunnen aanpakken, in tegenstelling tot 58,7% van de basisteamrecherche, 30,9% van de incidentafhandeling en 28,6% van de leidinggevenden. Ook voor cybercriminaliteitsvormen lijkt de I&S-groep meer vertrouwen te hebben in hun aanpak. Zo weet slechts een op de vijf I&S-medewerkers (21,9%) niet hoe ze hacking moeten aanpakken, terwijl bij andere functiegroepen deze groep twee tot bijna drie keer zo groot is (basisteamrecherche: 39,1%, leidinggevende: 54,3% en incidentafhandeling: 59,6%). Opvallend is dat voor de basisteamrecherche phishing wel vaak voor komt (tabel 4.5), maar dat ongeveer een op de vier respondenten (23,9%) aangeeft dat ze niet weten hoe deze zaken aangepakt moeten worden.

Tabel 4.6 Online criminaliteitsvormen die functiegroepen het vaakst wel of niet weten aan te pakken

|                                              | Online criminaliteits-<br>vorm | waarbij de meeste<br>respondenten<br>aangeven te weten<br>hoe dit aangepakt<br>moet worden (in<br>percentages) | Online criminaliteits-<br>vorm     | waarbij de meeste<br>respondenten<br>aangeven <u>niet</u> te<br>weten hoe dit<br>aangepakt moet<br>worden (in<br>percentages) |
|----------------------------------------------|--------------------------------|----------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>I&amp;S</b><br>(n = 32)                   | Telefonische<br>helpdeskfraude | 78,1                                                                                                           | DDoS-aanvallen                     | 56,3                                                                                                                          |
|                                              | Hulpvraagfraude                | 75,0                                                                                                           | Hacking                            | 21,9                                                                                                                          |
|                                              | Sextortion                     | 71,9                                                                                                           | Aan- en verkoopfraude              | 18,8                                                                                                                          |
| <b>Incident-<br/>afhandeling</b><br>(n = 94) | Telefonische<br>helpdeskfraude | 39,4                                                                                                           | DDoS-aanvallen                     | 79,8                                                                                                                          |
|                                              | Hulpvraagfraude                | 30,9                                                                                                           | Hacking                            | 59,6                                                                                                                          |
|                                              | Aan- en verkoopfraude          | 26,6                                                                                                           | Phishing                           | 38,3                                                                                                                          |
| <b>Basisteam-<br/>recherche</b><br>(n = 46)  | Telefonische<br>helpdeskfraude | 60,9                                                                                                           | DDoS-aanvallen                     | 63,0                                                                                                                          |
|                                              | Hulpvraagfraude                | 58,7                                                                                                           | Hacking                            | 39,1                                                                                                                          |
|                                              | Geldezak                       | 54,3                                                                                                           | Diefstal van gegevens,<br>Phishing | 23,9                                                                                                                          |
| <b>Leiding-<br/>gevende</b><br>(n = 35)      | Telefonische<br>helpdeskfraude | 40,0                                                                                                           | DDoS-aanvallen                     | 68,6                                                                                                                          |
|                                              | Aan- en verkoopfraude          | 31,4                                                                                                           | Hacking                            | 54,3                                                                                                                          |
|                                              | Hulpvraagfraude                | 28,6                                                                                                           | Phishing                           | 40,0                                                                                                                          |

Aanvullend is gekeken naar statistische significante verschillen tussen functiegroepen in de aanpak van online criminaliteit. We beschrijven ze in volgorde van effectgrootte. Er is één groot effect gevonden bij sextortion en middelgrote effecten bij hacking, cy-

berpesten, geldezel zaken, aan- en verkoopfraude, phishing en diefstal van persoonlijke gegevens. Er zijn significante, maar kleine effecten gevonden bij telefonische helpdeskfraude en DDoS-aanvallen.<sup>17</sup> Vervolgens hebben we gekeken welke groepen precies van elkaar verschillen. We beschrijven hiervoor alleen de grootste absolute verschillen en beschrijven ze per functiegroep.<sup>18</sup>

- De I&S-groep geeft aan vaker te weten hoe ze aan- en verkoopfraude (absoluut verschil is 0,904), phishing (0,895) en geldezel-zaken (0,649) moeten aanpakken dan de 'Anders'-groep. De I&S-groep geeft ook vaker aan te weten hoe ze phishing (0,990) en diefstal van persoonlijke gegevens (0,615) moeten aanpakken dan de basisteamrecherchegroep.
- De basisteamrecherchegroep geeft aan vaker te weten hoe ze hulpvraagfraude (0,973), telefonische helpdeskfraude (0,739) en aan- en verkoopfraude (0,714) aan moeten pakken dan de leidinggevende groep. En de basisteamrecherchegroep geeft aan beter geldezel-zaken (0,639) te kunnen aanpakken dan de 'Anders'-groep.
- De 'Anders'-groep geeft aan vaker te weten hoe ze phishing (0,545) moeten aanpakken dan de leidinggevende groep.

Als wordt gekeken naar de gemiddelden, dan wijkt de groep I&S af van de andere functiegroepen. Ze geven aan meer vertrouwen te hebben in de aanpak van online criminaliteitsvormen in vergelijking met de andere functiegroepen. Dit verschil is overigens niet statistisch significant, wat mogelijk is te verklaren door de kleine groepsgrootte. Deze resultaten moeten dus voorzichtig worden geïnterpreteerd.

## Resumé

In de resultaten is een duidelijke samenhang te zien tussen bekendheid, de frequentie van betrokkenheid en het ingeschatte eigen vermogen om online criminaliteit aan te pakken. Eenvoudigere en vaker voorkomende criminaliteitsvormen worden relatief goed herkend en aangepakt. De meest bekende criminaliteitsvormen zijn vormen van gedigitaliseerde criminaliteit (zoals uit Project Centurion).

Zo zijn telefonische helpdeskfraude en hulpvraagfraude niet alleen bekend, maar komen ze ook frequent voor, en ongeveer de helft van de respondenten geeft naar eigen zeggen aan te weten hoe ze dit moeten aanpakken. Maar er is ook een groep die niet weet hoe ze veelvoorkomende online criminaliteit moeten aanpakken. Zo weet een op de tien niet hoe ze telefonische helpdeskfraude moeten aanpakken, ongeveer een op de

17 Voor alle online criminaliteitsvormen zijn significante verschillen gevonden tussen de functiegroepen ( $p < 0,05$ ). Er is een groot effect gevonden bij sextortion ( $\eta^2 = 0,140$ ), middelgrote effecten bij hacking ( $\eta^2 = 0,097$ ), hulpvraagfraude ( $\eta^2 = 0,085$ ) cyberpesten ( $\eta^2 = 0,076$ ), geldezel zaken ( $\eta^2 = 0,072$ ), aan- en verkoopfraude ( $\eta^2 = 0,071$ ), phishing ( $\eta^2 = 0,064$ ) en diefstal van persoonlijke gegevens ( $\eta^2 = 0,063$ ). Er zijn significante, maar kleine effecten gevonden bij telefonische helpdeskfraude ( $\eta^2 = 0,056$ ) en DDoS-aanvallen ( $\eta^2 = 0,044$ ).

18 De vraag had drie antwoord categorieën (1 = ik weet het, 2 = ik weet het enigszins en 3 = ik weet het niet). Er is voor gekozen om alleen de verschillen te beschrijven als er een absoluut verschil van minimaal 0,5 is. Als we geen onderscheid zouden maken in het absolute verschil, dan worden 58 statistische significante verschillen gevonden tussen de verschillende functiegroepen in de betrokkenheid bij online criminaliteitsvormen.

zes weet dit niet voor hulpvraagfraude en aan- en verkoopfraude en een op de drie personen weet dit niet voor phishing.

Bij diverse criminaliteitsvormen geven respondenten aan dat ze ‘enigszins’ weten hoe ze deze moeten aanpakken. Er lijkt dus een zekere basiskennis aanwezig te zijn bij de meeste respondenten om online criminaliteit aan te pakken. Een uitzondering hierop zijn de technisch uitdagende of minder bekende criminaliteitsvormen (zoals DDoS-aanvallen en hacking) die minder vaak voorkomen en als moeilijke zaken worden ervaren. Deze zaken komen minder vaak voor in het dagelijks werk, worden minder goed begrepen en er is meer onzekerheid over de aanpak ervan.

Maar er is ook nog een groep die niet weet hoe ze online criminaliteitsvormen moeten aanpakken. Een deel van de respondenten (variërend van 11%-68,4%) weet niet hoe specifieke vormen van online criminaliteit aangepakt moeten worden, ondanks het feit dat online criminaliteit voorkomt op de basisteams. Respondenten weten vooral niet hoe ze (‘eenvoudige’) cybercriminaliteitszaken moeten aanpakken, zoals DDoS-aanvallen (68,4%), hacking (46,9%) en diefstal van persoonlijke gegevens (25,1%). Maar ook voor veelvoorkomende online criminaliteitsvormen van Project Centurion weet ongeveer een derde dat niet voor phishing (31,3%).

Als wij de verschillende functiegroepen vergelijken, dan vallen enkele zaken op. Ten eerste dat de I&S-groep aangeeft relatief vaak in aanraking te komen met online criminaliteit en ook aangeeft relatief vaak te weten hoe ze dit moeten aanpakken. Ruim driekwart van de I&S-medewerkers weet naar eigen zeggen hoe ze de meest veelvoorkomende online criminaliteitsvormen (telefonische helpdeskfraude) moeten aanpakken. Het is echter de vraag of dit vanuit een ander perspectief ook zo is. Zo rapporteerden Van Steden en collega's (2025) de nodige klachten van andere afdelingen binnen de basisteams over de kwaliteit van de aangiften van online criminaliteit die door I&S waren opgenomen. Verder valt op dat hoewel phishing vaker voorkomt bij de basisteamrecherche, een op de vier respondenten aangeeft niet te weten hoe dit aangepakt moet worden.

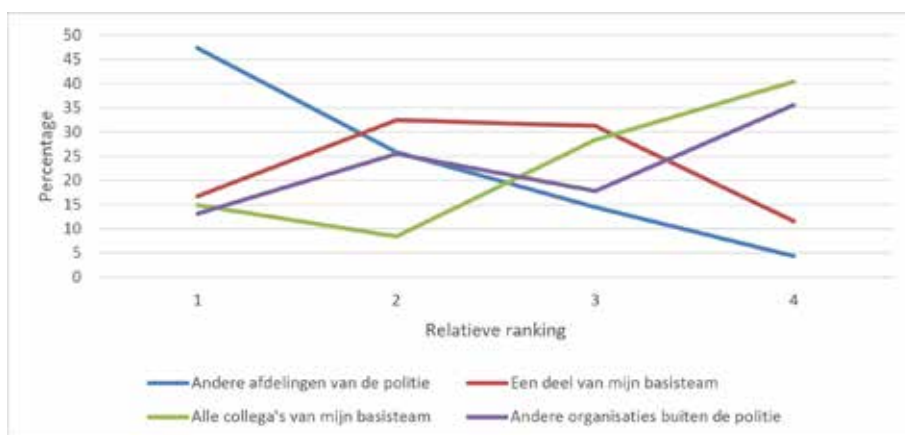
Kortom, de meeste respondenten geven aan ‘enigszins’ te weten hoe ze veelvoorkomende, geprioriteerde, gedigitaliseerde criminaliteit kunnen aanpakken. Cybercriminaliteit en meer onbekende vormen kunnen enkel door een kleine groep worden opgepakt. Er is dus verbeterpotentie in alle vormen van online criminaliteit. Tevens lijkt er vooral handelingsverlegenheid te zitten op cybercriminaliteit, met die kanttekening dat respondenten voor zichzelf hier veelal geen rol in zien. In de volgende paragraaf brengen wij in kaart hoe respondenten de lokale politietaak op het gebied van online criminaliteit invullen.

#### 4.3 De lokale politietaak van online criminaliteit volgens respondenten

In deze paragraaf is uiteengezet in hoeverre respondenten het belangrijk vinden om als basisteam online criminaliteit aan te pakken en of ze behoeften hebben aan ontwikkeling in de kennis, vaardigheden en aanpak.

Om te onderzoeken of basisteammedewerkers de aanpak van online criminaliteit belangrijk vinden, is hen gevraagd hoe zij de impact van online criminaliteit op de samenleving inschatten. De meerderheid (85%) is van mening dat online criminaliteit een grote impact heeft op de samenleving, terwijl 15% aangeeft dat de impact gemiddeld is (geen van de respondenten heeft voor een kleine impact van online criminaliteit gekozen,  $n = 275$ ).

Respondenten werd gevraagd wie volgens hen verantwoordelijk zou moeten zijn voor het aanpakken van online criminaliteit in hun werkgebied ( $n = 253$ ). Ze konden een rangorde aangeven tussen vier opties: alle collega's binnen mijn basisteam, een deel van mijn basisteam, andere afdelingen van de politie of andere organisaties buiten de politie. De grootste groep respondenten (47,3%) vindt dat primair andere afdelingen van de politie online criminaliteit in hun werkgebied moeten aanpakken (zie figuur 4.1). Op de tweede (32,4%) en derde (21,3%) plaats vinden de meeste respondenten dat *een deel* van het basisteam een taak moet hebben in de lokale aanpak van online criminaliteit. Twee op de vijf respondenten (40,4%) zetten op de laatste plaats de optie dat *alle* collega's binnen het basisteam verantwoordelijk zouden moeten zijn voor het bestrijden van online criminaliteit. Respondenten zien daarnaast ook een rol weggelegd voor organisaties buiten de politie, maar vinden dat de politie hierin de grootste verantwoordelijkheid draagt.



*Notitie.* De horizontale as toont een relatieve ranking en de verticale as toont percentages van respondenten die het item hebben gekozen.

Figuur 4.1 Antwoorden op rankingvraag wie online criminaliteit in het werkgebied van respondenten moet aanpakken ( $n = 253$ )

Vervolgens is gevraagd welke taken respondenten belangrijk vinden in het basisteam ten opzichte van online criminaliteit (zie tabel 4.7). Volgens hen dient de focus in eerste instantie te liggen bij de opsporing van online criminaliteit (33,1%). Daaropvolgend vinden respondenten het belangrijk om nazorg te geven aan slachtoffers (29,8%), zoals het geven van adviezen aan aangevers om herhaald slachtofferschap te voorkomen.

Ook het verstoren van online criminaliteit (29,5%), preventie van slachtofferschap (24%) en alternatieve interventies (22,9%) zijn volgens de respondenten taken van een basisteam. Voorbeelden van alternatieve interventies zijn het versturen van een waarschuwingsbrief of een stopgesprek met een geldezel. Er is een duidelijk verschil met preventie van daderschap van online criminaliteit, hoewel de meesten hier wel een bepaalde taak zien weggelegd voor het basisteam, is het geen prioriteit in vergelijking met de andere taken.

Tabel 4.7 Prioriteit taken van basisteam ten opzichte van online criminaliteit (n = 275, in percentages)

| Stelling: ik vind ... een belangrijke taak van mijn basisteam  | Sterk mee oneens | Mee oneens | Niet mee oneens/niet mee eens | Mee eens | Helemaal mee eens |
|----------------------------------------------------------------|------------------|------------|-------------------------------|----------|-------------------|
| Opsporing van online criminaliteit                             | 2,5              | 8,4        | 8,4                           | 47,6     | 33,1              |
| Nazorg aan slachtoffers                                        | 1,5              | 7,3        | 10,9                          | 50,5     | 29,8              |
| Verstoren van online criminaliteit                             | 3,3              | 8,0        | 13,5                          | 45,8     | 29,5              |
| Preventie van <u>slachtofferschap</u> van online criminaliteit | 3,6              | 8,7        | 13,5                          | 50,2     | 24,0              |
| Alternatieve interventies                                      | 1,5              | 5,5        | 14,9                          | 55,3     | 22,9              |
| Preventie van <u>daderschap</u> van online criminaliteit       | 3,6              | 12,7       | 17,5                          | 52,4     | 13,8              |

Ook is gevraagd welke taken met betrekking tot online criminaliteit respondenten en hun collega's (naar de herinnering van de respondenten) het afgelopen jaar binnen het eigen basisteam hebben uitgevoerd. Zoals is te zien in tabel 4.8 waren de voornaamste werkzaamheden in het basisteam gericht op nazorg aan slachtoffers van online criminaliteit (68,4%). De taken in de aanpak van online criminaliteit waren veel minder gericht op alternatieve interventies (9,5%), opsporing (8,0%) of preventie van slachtofferschap (4,4%). In enkele gevallen werden taken uitgevoerd om online criminaliteit te verstoren (0,7%) of daderschap te voorkomen (0,4%).

Een deel van de respondenten (8,6%) vulde 'anders, namelijk ...' in. Uit de open antwoorden blijkt dat respondenten hier geen zicht op hebben ( $n = 7$ ), er geen van deze taken binnen het basisteam worden uitgevoerd ( $n = 6$ ), ze aangiften opnemen ( $n = 2$ ) of de vraag niet van toepassing was ( $n = 2$ ). Individuele antwoorden omvatten: inzet van cybervrijwilligers, beeld gemaakt wie in onze wijk zich ermee bezighoudt, samenwerking met externen en interne opleidingsplannen en beoordeling van specifiek cyberzaken binnen de basiseenheid. Ook wordt door een respondent aangegeven 'Het basisteam gaat zich steeds meer focussen en ontwikkelen op het gebied van online criminaliteit/cybercrime. Het is goed en van belang dat hier meer aandacht aan wordt besteed.'

Tabel 4.8 De taken met betrekking tot online criminaliteit die volgens de respondenten het afgelopen jaar zijn uitgevoerd binnen het eigen basisteam (n = 275, in percentages)

| Taken                                                          | %    |
|----------------------------------------------------------------|------|
| Nazorg aan slachtoffers                                        | 68,4 |
| Alternatieve interventies                                      | 9,5  |
| Opsporing van online criminaliteit                             | 8,0  |
| Preventie van <u>slachtofferschap</u> van online criminaliteit | 4,4  |
| Verstoren van online criminaliteit                             | 0,7  |
| Preventie van <u>daderschap</u> van online criminaliteit       | 0,4  |
| Anders, namelijk ...                                           | 8,6  |

### Vergelijking tussen functiegroepen

Er is gevraagd welke taken de respondenten hebben uitgevoerd om online criminaliteit aan te pakken, waarbij vooral nazorg aan slachtoffers is verleend. Als we dit bekijken per functiegroep (tabel 4.9), dan zien we enkele verschillen. Zo heeft de incidentafhandelingsgroep als enige groep ingezet op verstoring of preventie van daderschap. Deze groep heeft als enige iets gedaan op alle voorgestelde taken. De I&S-groep heeft zich vooral gericht op de nazorg van slachtoffers en enkele alternatieve interventies uitgevoerd. De basisteamrecherchegroep richt zich ook vooral op nazorg van slachtoffers en op de tweede plek op opsporing van online criminaliteit. De leidinggevende groep heeft zich naast de nazorg aan slachtoffers beziggehouden met alternatieve interventies.

Tabel 4.9 De taken met betrekking tot online criminaliteit van het afgelopen jaar die zijn uitgevoerd per functiegroep (n = 275, in percentages)

| Taken                                                          | I&S  | Incident-afhandeling | Basisteam-recherche | Leidinggevende |
|----------------------------------------------------------------|------|----------------------|---------------------|----------------|
| Nazorg aan slachtoffers                                        | 90,6 | 66,0                 | 54,3                | 62,9           |
| Alternatieve interventies                                      | 3,1  | 6,4                  | 13,0                | 17,1           |
| Opsporing van online criminaliteit                             | 0,0  | 7,4                  | 28,3                | 2,9            |
| Preventie van <u>slachtofferschap</u> van online criminaliteit | 0,0  | 9,6                  | 0,0                 | 5,7            |
| Verstoren van online criminaliteit                             | 0,0  | 2,1                  | 0,0                 | 0,0            |
| Preventie van <u>daderschap</u> van online criminaliteit       | 0,0  | 1,1                  | 0,0                 | 0,0            |
| Anders, namelijk ...                                           | 6,3  | 7,4                  | 4,3                 | 11,4           |

### Resumé

Uit de voorgaande resultaten kan opgemaakt worden dat respondenten vinden dat online criminaliteit een grote impact op de samenleving heeft. Tevens zien ze een belang-

rijke rol weggelegd voor een deel van het basisteam, in samenwerking met andere afdelingen van de politie en externe partijen.

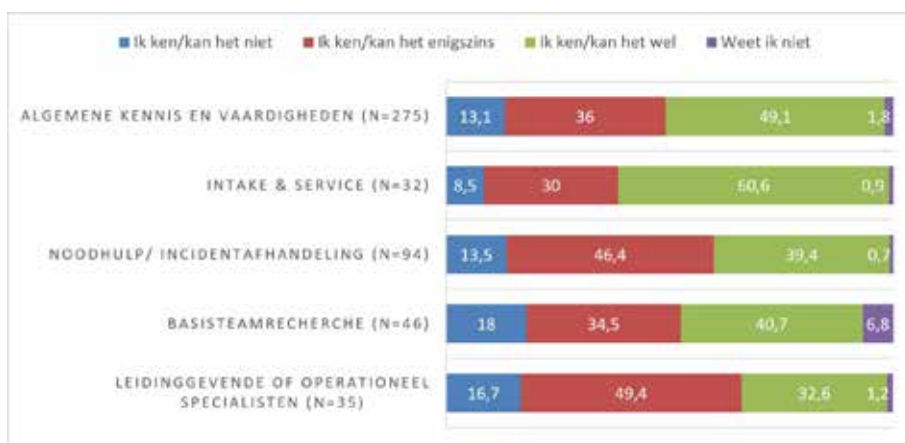
Respondenten vinden vrijwel alle voorgestelde taken om online criminaliteit aan te pakken bijna even belangrijk (met uitzondering van preventie van daderschap). Ongeveer een derde vindt vooral opsporing, nazorg en verstoring van online criminaliteit belangrijk. In de praktijk blijkt dat voornamelijk nazorg aan de slachtoffers het afgelopen jaar is bewerkstelligd. De andere taken, zoals opsporing van criminaliteit (8,0%) en verstoring (0,7%) zijn weinig tot niet in de praktijk uitgevoerd. Het is de vraag wat de oorzaak is van deze discrepantie tussen de door de respondenten geprioriteerde taken en werkelijk uitgevoerde taken. Immers, respondenten geven ook aan dat online criminaliteit wel voorkomt op de basisteams (zie vorige paragraaf).

In de vergelijking tussen de functiegroepen komt naar voren dat de I&S-groep vooral meer prioriteit lijkt te geven aan nazorg van slachtoffers dan de andere functiegroepen. De incidentaafhandelingsgroep heeft als enige groep ingezet op alle voorgestelde taken. In de volgende paragraaf brengen wij de specifieke beschikbare kennis en vaardigheden bij de basisteams in kaart.

#### 4.4 Kennis en vaardigheden

In deze paragraaf worden de kennis en vaardigheden beschreven bij de basisteams. Ter herinnering, in de vragenlijst is onderscheid gemaakt tussen verschillende functiegroepen: I&S-medewerkers, incidentaafhandeling, basisteamrecherche en leidinggevers. Aan alle respondenten is gevraagd in hoeverre ze 'algemene kennis en vaardigheden' bezitten of kunnen toepassen. Als de respondenten aangaven bij een specifieke functiegroep te horen, dan kregen ze in de vragenlijst ook vragen te zien over functie specifieke kennis- en vaardighedenitems.

In figuur 4.2 wordt een algemeen beeld geschetst van de gemiddelde zelfgerapporteerde kennis en vaardigheden die zijn uitgevraagd bij de respondenten. De meeste respondenten geven aan enigszins of volledig de benodigde kennis en vaardigheden te bezitten om online criminaliteit aan te pakken. Slechts een kleine groep geeft aan deze kennis en vaardigheden helemaal niet te bezitten of te kunnen toepassen. Er zijn geen grote verschillen tussen de functiegroepen. Hierna worden alle gestelde vragen per functiegroep toegelicht.



Figuur 4.2 Gemiddelde scores op kennis/vaardigheden items voor alle respondenten en per functiegroep (in percentages)

De algemene kennis en vaardighedenitems die aan alle respondenten zijn voorgelegd zijn uiteengezet in tabel 4.10. Hieruit blijkt dat er grote verschillen zijn in kennis en kunde tussen de respondenten. Tevens blijkt de meeste respondenten op bijna alle items aangeven dit (enigszins) te kunnen. De grootste groep durft in hun werk om hulp te vragen over online criminaliteit (84,4% kan het en 10,9% enigszins). Daaropvolgend weten de meesten ook waar ze binnen de politie deze vragen kunnen stellen (60% weet dit en 28,4% enigszins). Iets meer dan de helft is goed bekend met digitale platformen en socialmediakanalen (58,5% en 32,7% enigszins). Minder dan de helft van de respondenten weet goed waar politie informatie gevonden kan worden over online criminaliteit (48,7% en 38,9% enigszins). Een derde van de respondenten weet digitale sporen goed te herkennen op bijvoorbeeld een telefoon of het internet (35,6% en 41,8% enigszins).

Er zijn ook een aantal items die respondenten niet kennen of bezitten. Ongeveer een op de zeven respondenten geeft aan dat ze niet weten hoe ze als politiemedewerker online informatie kunnen verzamelen (15,6%). Een of de vijf respondenten geeft aan digitale sporen niet te kunnen herkennen (21,5%). Tot slot kent een op de vier respondenten de juridische bevoegdheden voor het gebruik van informatie niet (24,7%).

Tabel 4.10 Algemene kennis en vaardigheden (n = 275, in percentages)

| Kennis en vaardigheden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Ik ken/kan het niet | Ik ken/kan het enigszins | Ik ken/kan het wel | Weet ik niet |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------------|--------------------|--------------|
| Ik durf in mijn werk te vragen om hulp over online criminaliteit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2,5                 | 10,9                     | 84,4               | 2,2          |
| Ik weet waar ik binnen de politie vragen kan stellen over online criminaliteit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 9,8                 | 28,4                     | 60                 | 2,2          |
| Ik ken digitale platformen en socialmediakanalen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 7,3                 | 32,7                     | 58,5               | 1,5          |
| Ik weet waar ik binnen de politie informatie kan vinden over online criminaliteit*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 10,2                | 38,9                     | 48,7               | 2,2          |
| Ik kan digitale sporen herkennen (telefoon, internet, etc cetera)*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 21,5                | 41,8                     | 35,6               | 1,1          |
| Ik weet hoe ik als politiemedewerker online informatie kan verzamelen*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 15,6                | 50,5                     | 32,7               | 1,1          |
| Ik ken de juridische bevoegdheden voor het gebruik van digitale informatie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 24,7                | 48,7                     | 24                 | 2,5          |
| <b>Gemiddelde</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 13,1                | 36                       | 49,1               | 1,8          |
| <i>Notitie. Er zijn drie significante verschillen gevonden tussen de functiegroepen (*), maar deze hebben een kleine effectgrootte.<sup>a</sup></i>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                     |                          |                    |              |
| <sup>a</sup> Voor het item 'herkennen van digitale sporen' is een significant verschil ( $p = 0,022$ ) tussen de functiegroepen gevonden met een klein effect ( $\eta^2 = 0,039$ ). Voor het item 'ik weet waar ik binnen de politie informatie kan vinden over online criminaliteit' is ook een significant verschil ( $p = 0,004$ ) gevonden met een klein effect ( $\eta^2 = 0,058$ ). Tot slot is voor het item 'ik weet waar ik binnen de politie vragen kan stellen over online criminaliteit' een significant verschil ( $p = 0,048$ ) gevonden met een ook een kleine effectgrootte ( $\eta^2 = 0,036$ ). |                     |                          |                    |              |

Voor de I&S-medewerkers ( $n = 32$ ) is ook gevraagd naar specifieke kennis en vaardigheden die zij bezitten om online criminaliteit aan te pakken (zie tabel 4.11). Opnieuw is op te merken dat er grote verschillen zijn in de kennis en kunde binnen deze groep respondenten. Gemiddeld geeft 60,6% van de respondenten aan deze functie specifieke kennis en vaardigheden wel te bezitten.

De respondenten geven aan de meeste kennis en vaardigheden wel of enigszins te bezitten of kunnen. Vooral kennis over de procedure om een aangifte op te nemen (84,4% wel) en het op de juiste wijze opnemen van een aangiften (87,5% wel) worden hoog ingeschat. De helft van de respondenten rapporteert ook voldoende kennis te hebben om slachtoffers te adviseren in vervolgstappen (46,9%), hoe ze digitale sporen in kaart moeten brengen bij het opnemen van een aangifte of hoe ze aangevers moeten adviseren om digitale sporen veilig te stellen.

Er wordt relatief laag gescoord op items die te maken hebben met het veiligstellen van digitale sporen. Ongeveer een op de zeven respondenten weet niet hoe ze digitale sporen die van belang zijn voor de opsporing in kaart gebracht moeten worden bij de aangiften (15,6%). Een op de vijf respondenten (21,9%) weet niet hoe ze aangevers moeten adviseren om digitale sporen veilig te stellen.

Tabel 4.11 Kennis en vaardigheden van I&amp;S-medewerkers (n = 32, in percentages)

| Kennis en vaardigheden                                                                                                                                                                                 | Ik ken/kan het niet | Ik ken/kan het enigszins | Ik ken/kan het wel |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------------|--------------------|
| Ik kan op de juiste wijze een aangifte registreren in de politiesystemen                                                                                                                               | 3,1                 | 9,4                      | 87,5               |
| Ik ken de procedure voor het opnemen van aangifte van online criminaliteit                                                                                                                             | 6,3                 | 9,4                      | 84,4               |
| Ik ken vormen van online criminaliteit bij het opnemen van meldingen en aangiften                                                                                                                      | 6,3                 | 15,6                     | 78,1               |
| Ik weet welke gedrag op het internet strafbaar is                                                                                                                                                      | 6,3                 | 28,1                     | 65,6               |
| Ik ben bekend met informatieproducten die zijn ontwikkeld voor de intake van online criminaliteit (bijvoorbeeld factsheets, hulpmiddelen aangever, handreikingen, webapp cybercrime)                   | 3,1                 | 37,5                     | 59,4               |
| Ik weet naar welke partijen ik slachtoffers van online criminaliteit kan doorverwijzen (bijvoorbeeld Slachtofferhulp Nederland, banken, verzekeringsmaatschappijen, Offlimits, Stop it Now! et cetera) | 6,3                 | 34,4                     | 59,4               |
| Ik kan aangevers adviseren om (herhaald) slachtofferschap van online criminaliteit te voorkomen                                                                                                        | 6,3                 | 37,5                     | 56,3               |
| Ik kan slachtoffers van online criminaliteit adviseren in hun vervolgstappen*                                                                                                                          | 9,4                 | 40,6                     | 46,9               |
| Ik weet hoe ik digitale sporen die voor de opsporing van belang zijn in kaart moet brengen bij het opnemen van de aangifte                                                                             | 15,6                | 50,0                     | 34,4               |
| Ik weet hoe ik aangevers moet adviseren om digitale sporen veilig te stellen**                                                                                                                         | 21,9                | 37,5                     | 34,4               |
| <b>Gemiddelde</b>                                                                                                                                                                                      | <b>8,5</b>          | <b>30,0</b>              | <b>60,6</b>        |
| <i>Notitie. *1 respondent antwoordde: 'weet ik niet'. **2 respondenten antwoordden: 'weet ik niet'.</i>                                                                                                |                     |                          |                    |

Voor de incidentafhandeling groep ( $n = 94$ ) zijn de scores op de verdere kennis- en vaardighedenvragen in tabel 4.12 weergegeven. Er zijn grote verschillen in de kennis en kunde binnen deze functiegroep. Gemiddeld genomen hebben de meeste respondenten enige (46,4%) of goede (39,4%) basiskennis en vaardigheden bij de incidentafhandeling en heeft de kleinste groep helemaal geen kennis/vaardigheden op dit gebied (13,5%). Ruim de helft geeft aan goed te kunnen communiceren met burgers via het internet of sociale media (56,4%). Iets minder dan de helft van de respondenten kan aangevers goed adviseren om (herhaald) slachtofferschap te voorkomen (48,9%) of relevante digitale gegevensdragers te herkennen op een plaats delict (42,6%). De grootste groep respondenten geeft aan enigszins op de hoogte te zijn van de taken op een plaats delict bij online criminaliteit (59,6%). Er is de minste kennis over het juridisch kader voor werkzaamheden op een plaats delict bij online criminaliteit (23,4% niet).

Tabel 4.12 Kennis en vaardigheden van incidentafhandeling medewerkers (n = 94, in percentages)

| Kennis en vaardigheden                                                                                                                           | Ik ken/kan het niet | Ik ken/kan het enigszins | Ik ken/kan het wel |
|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------------|--------------------|
| Ik weet hoe ik met burgers via internet en sociale media kan communiceren**                                                                      | 7,4                 | 34                       | 56,4               |
| Ik kan aangevers adviseren om (herhaald) slachtofferschap van online criminaliteit te voorkomen*                                                 | 9,6                 | 40,4                     | 48,9               |
| Ik weet hoe ik relevante digitale gegevensdragers kan herkennen op een plaats delict                                                             | 11,7                | 45,7                     | 42,6               |
| Ik heb kennis over hoe ik aangevers kan adviseren om vervolgstappen te zetten wanneer zij het slachtoffer van online criminaliteit zijn geworden | 16                  | 43,6                     | 40,4               |
| Ik ben op de hoogte van mijn taken op een plaats delict bij online criminaliteit*                                                                | 12,8                | 59,6                     | 26,6               |
| Ik ken het juridisch kader voor mijn werk op een plaats delict ten aanzien van online criminaliteit                                              | 23,4                | 55,3                     | 21,3               |
| <b>Gemiddelde</b>                                                                                                                                | 13,5                | 46,4                     | 39,4               |
| <i>Notitie. *1,1% (n = 1) antwoordde: 'weet ik niet'. **2,1% (n = 2) antwoordde: 'weet ik niet'.</i>                                             |                     |                          |                    |

In tabel 4.13 is de verdeling van kennis en vaardigheden voor de basisteamrecherche groep (n = 46) weergegeven. Ook in deze functiegroep zijn grote verschillen in de kennis en kunde om online criminaliteit aan te pakken. Gemiddeld genomen heeft de grootste groep goede (40,7%) of enige (34,5%) kennis/vaardigheden en de kleinste groep geen kennis/vaardigheden op dit gebied (18%). De grootste groep respondenten weet wel wie ze moeten benaderen als ze vragen hebben op het gebied van online criminaliteit (67,4%) en kunnen een vordering opmaken om online gegevens van een dader te achterhalen (58,7%). Daarna weet 45,7% van de respondenten enigszins welke online sporen (mogelijk) te vorderen zijn. Respondenten hebben de minste kennis over interceptiemogelijkheden (26,1% niet), het kunnen veiligheidstellen van digitale sporen (26,1% niet) en hoe onderzoeksbevindingen van online criminaliteit geanalyseerd en geduid moeten worden (30,4% niet).

Tabel 4.13 Kennis en vaardigheden van de basisteamrecherche groep (n = 46, in percentages)

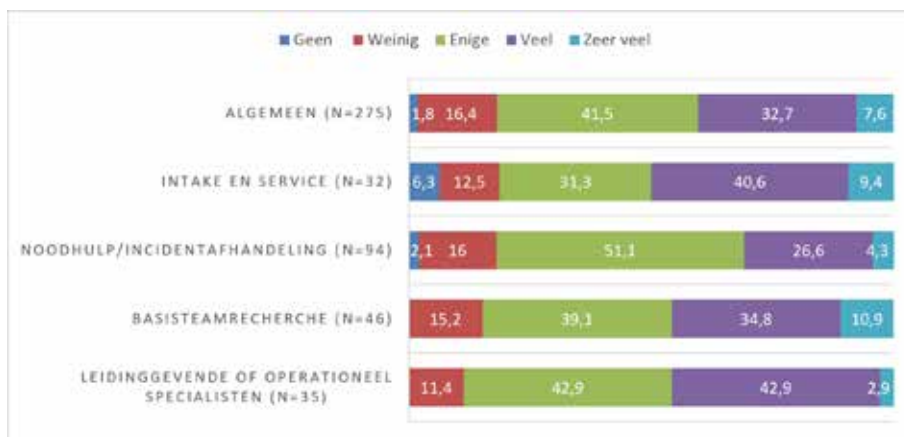
| Kennis en vaardigheden                                                                           | Ik ken/kan het niet | Ik ken/kan het enigszins | Ik ken/kan het wel | Weet ik niet |
|--------------------------------------------------------------------------------------------------|---------------------|--------------------------|--------------------|--------------|
| Ik weet wie ik moet benaderen als ik vragen heb op het gebied van online criminaliteit           | 10,9                | 17,4                     | 67,4               | 4,3          |
| Ik kan een vordering opmaken om online gegevens van een dader te achterhalen (zoals IP-adressen) | 8,7                 | 28,3                     | 58,7               | 4,3          |
| Ik kan een proces verbaal opmaken voor vormen van online criminaliteit                           | 10,9                | 39,1                     | 41,3               | 8,7          |
| Ik weet welke online sporen (mogelijk) te vorderen zijn                                          | 13,0                | 45,7                     | 37,0               | 4,3          |
| Ik ken de interceptiemogelijkheden bij online criminaliteit                                      | 26,1                | 30,4                     | 32,6               | 10,9         |
| Ik kan digitale sporen veiligstellen                                                             | 26,1                | 39,1                     | 26,1               | 8,7          |
| Ik weet hoe ik onderzoeksbevindingen van online criminaliteit moet analyseren en duiden          | 30,4                | 41,3                     | 21,7               | 6,5          |
| <b>Gemiddelde</b>                                                                                | 18,0                | 34,5                     | 40,7               | 6,8          |

In tabel 4.14 worden de specifieke kennis en vaardigheden voor de leidinggevende of operationeel specialisten weergegeven. In lijn met de vorige resultaten zijn er ook in deze functiegroep grote verschillen in de kennis en kunde om online criminaliteit aan te pakken. Opvallend is dat bij alle vragen de grootste groepen respondenten aangeven hier enigszins (49,4%) kennis of kunde van te hebben. De grootste groepen respondenten hebben naar eigen inzicht enigszins kennis over slachtofferschap (62,9%) en daderschap (57,1%) van online criminaliteit in het werkgebied van het basisteam. De meesten kunnen enigszins (45,7%) of goed (42,9%) intern samenwerken op het gebied van online criminaliteit, maar minder goed extern samenwerken op het gebied van online criminaliteit (28,6% niet). Ze kunnen ook het minst goed richting geven aan de aanpak van online criminaliteit (25,7% niet).

Tabel 4.14 Kennis en vaardigheden van leidinggevende of operationeel specialisten (n = 35, in percentages)

| Kennis en vaardigheden                                                                                                              | Ik ken/kan het niet | Ik ken/kan het enigszins | Ik ken/kan het wel |
|-------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------------|--------------------|
| Ik kan intern samenwerken op het gebied van online criminaliteit                                                                    | 11,4                | 45,7                     | 42,9               |
| Ik kan medewerkers faciliteren en stimuleren om hun kennis en vaardigheden voor het aanpakken van online criminaliteit te vergroten | 11,4                | 51,4                     | 37,1               |
| Ik heb voldoende basiskennis over de inhoud van en ontwikkelingen rondom online criminaliteit om mijn team hierop aan te sturen*    | 17,1                | 42,9                     | 37,1               |
| Ik heb kennis over slachtofferschap van online criminaliteit in het werkgebied van het basisteam                                    | 5,7                 | 62,9                     | 31,4               |
| Ik kan richting geven aan de aanpak van online criminaliteit*                                                                       | 25,7                | 42,9                     | 28,6               |
| Ik heb kennis over ouderschap van online criminaliteit in het werkgebied van het basisteam                                          | 17,1                | 57,1                     | 25,7               |
| Ik kan extern samenwerken op het gebied van online criminaliteit*                                                                   | 28,6                | 42,9                     | 25,7               |
| <b>Gemiddelde</b>                                                                                                                   | 16,7                | 49,4                     | 32,6               |
| <i>Notitie. *2,9% (n=1) antwoordde: 'weet ik niet'.</i>                                                                             |                     |                          |                    |

Vervolgens is aan alle respondenten gevraagd in hoeverre ze interesse hebben om zich verder te ontwikkelen in de aan hun voorgestelde kennis en vaardigheden (zie figuur 4.3). De meerderheid van de respondenten heeft interesse om zichzelf verder te ontwikkelen op kennis en vaardigheden om online criminaliteit beter aan te pakken. Van alle respondenten hebben de meesten enige (41,5%) of veel (32,7%) interesse, gevolgd door weinig (15%) of zeer veel interesse (8,0%). Opvallend is dat er slechts enkele respondenten aangeven helemaal geen interesse te hebben om zichzelf verder te ontwikkelen op de voorgestelde kennis en vaardigheden (2,0%). Er is geen significant verschil gevonden in een vergelijking tussen de functiegroepen.



*Notitie. Er is geen significant verschil gevonden tussen de functiegroepen in de interesse om zichzelf verder te ontwikkelen in de voorgestelde kennis en vaardigheden.*

Figuur 4.3 Interesse om zichzelf verder te ontwikkelen in voorgestelde kennis en vaardigheden (in percentages)

## Resumé

Er zijn grote verschillen in de ingeschatte kennis en kunde voor alle functiegroepen. De algemene kennis en vaardigheden zijn bij de meeste respondenten (enigszins) bekend. Vrijwel iedereen durft om hulp te vragen als het gaat om online criminaliteit en ze weten ook bij wie ze binnen de politie deze vragen kunnen stellen. Respondenten zijn het minst bekend met mogelijkheden om online informatie te verzamelen en de juridische bevoegdheden voor het gebruik van digitale informatie.

De I&S-respondenten geven relatief vaak aan kennis en vaardigheden 'enigszins' te bezitten. Ten opzichte van andere groepen zijn de scores van I&S het hoogst. Ze vinden dat de meeste kennis ligt bij het op de juiste wijze registreren van een aangifte in de politiesystemen en ze kennen de procedure om aangiften van online criminaliteit op te nemen. Ze weten het minst over digitale sporen, hoe ze deze in kaart moeten brengen of hoe ze een aangever kunnen adviseren om digitale sporen veilig te stellen.

De incidentafhandelingsgroep geeft ook relatief vaak aan de kennis en vaardigheden 'enigszins' te bezitten. De meesten geven aan goed met burgers te kunnen communiceren via internet en sociale media en hebben de minste kennis over het juridische kader voor werk op een plaats delict waar online criminaliteit voorkomt. De grootste groep bezit de kennis of vaardigheden enigszins.

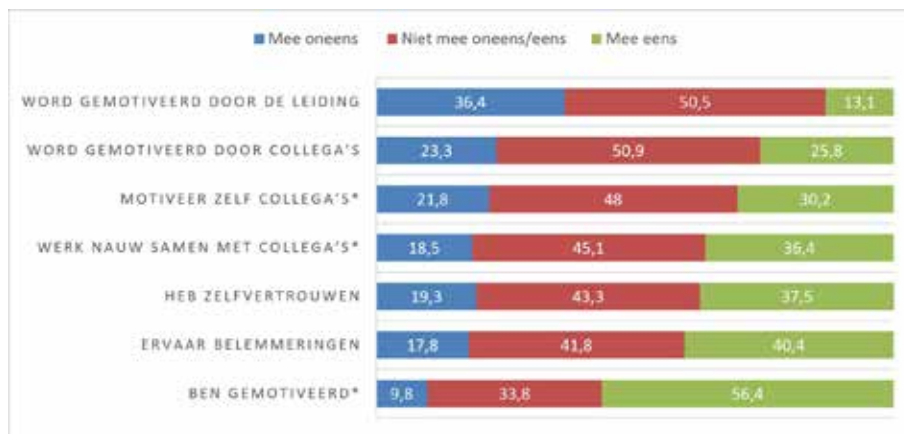
Van de basisteamresearchgroep hebben de meeste respondenten ook wel enige of goede kennis over wat ze kennen en kunnen betreft online criminaliteit. Ze weten vooral wie ze moeten benaderen voor vragen op het gebied van online criminaliteit. Ze weten het minst over digitale sporen, welke mogelijk te vorderen zijn, hoe ze veiligge-

steld moeten worden en hoe de onderzoeksbevindingen geanalyseerd en geduid moeten worden.

De leidinggevende groep geeft aan vooral enigszins kennis/vaardigheden te hebben wat betreft online criminaliteit. Ze hebben vooral enigszins kennis over ouderschap en slachtofferschap van online criminaliteit in het werkgebied van het basisteam. En de meesten kunnen intern samenwerken, maar minder goed extern samenwerken op het gebied van online criminaliteit. Tot slot hebben vrijwel alle respondenten in een bepaalde mate interesse om zichzelf verder te ontwikkelen, waarvan bijna de helft veel tot zeer veel interesse heeft.

#### 4.5 Bevorderende en belemmerende factoren van interventies

In de vragenlijst hebben wij de vraag gesteld op welke manier de respondenten gemotiveerd worden om online criminaliteit aan te pakken (figuur 4.4). Ruim de helft (56,4%) van de respondenten zegt gemotiveerd te zijn en een kleine groep helemaal niet (9,8%). Tegelijkertijd ervaart ook een redelijke groep respondenten belemmeringen (40,4%) om online criminaliteit aan te pakken. Ruim een derde van de respondenten heeft zelfvertrouwen om online criminaliteit aan te pakken (37,5%) en een vijfde van de respondenten heeft dat zelfvertrouwen niet (19,3%). Ongeveer een derde geeft ook aan nauw samen te werken met collega's (36,4%) om online criminaliteit aan te pakken en motiveert hierin zelf collega's (30,2%). Respondenten vonden het minst dat ze werden gemotiveerd door collega's (23,3%) of de leiding (36,4%). Belangrijk om op te merken is dat een relatief grote groep het niet eens of oneens was met de stellingen.



*Notitie. \*Voor deze items zijn significante maar kleine verschillen gevonden tussen de functiegroepen.<sup>19</sup>*

Figuur 4.4 Ik ... om online criminaliteit aan te pakken in mijn werk binnen het basisteam (n = 275, in percentages)

Er zijn ook vragen gesteld om te achterhalen op welke manier basisteammedewerkers het beste leren (zie tabel 4.15). Respondenten konden aangeven welke setting of randvoorwaarden wel of niet belangrijk voor ze waren. Uit de resultaten blijkt dat respondenten vooral willen leren in een fysieke setting (72,7%), van politiecollega's met expertise (72%) en tijdens reguliere werkzaamheden (67,6%). De respondenten willen liever niet leren in een online setting (42,5%), alleen (35,6%) of door zelf informatie op te zoeken of te lezen (21,8%).

Tabel 4.15 Randvoorwaarden om het beste te leren (n = 275 tenzij anders weergegeven, in percentages)

| Ik leer het beste (door)                                                                                                                                                                                                                                                                                                                                                                    | Niet belangrijk | Enigszins belangrijk | Wel belangrijk |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----------------------|----------------|
| In een fysieke setting (n = 273)                                                                                                                                                                                                                                                                                                                                                            | 3,3             | 23,3                 | 72,7           |
| Leren van politiecollega's buiten het basisteam (Team Cybercrime, ECDO, digitaal platform et cetera)                                                                                                                                                                                                                                                                                        | 0,4             | 27,6                 | 72,0           |
| Tijdens reguliere werkzaamheden (meedraaien met onderzoek met ervaren collega's)*                                                                                                                                                                                                                                                                                                           | 2,9             | 29,5                 | 67,6           |
| Leren van collega's binnen het basisteam                                                                                                                                                                                                                                                                                                                                                    | 2,9             | 34,2                 | 62,9           |
| Informatie die wordt aangeboden (cursus, training, escaperoom)                                                                                                                                                                                                                                                                                                                              | 3,6             | 40,0                 | 56,4           |
| Leren van externen (buiten de politie)                                                                                                                                                                                                                                                                                                                                                      | 5,5             | 42,2                 | 52,4           |
| Buiten reguliere werkzaamheden (bijvoorbeeld clusterdagen, trainingsdagen)*                                                                                                                                                                                                                                                                                                                 | 8,7             | 41,1                 | 50,2           |
| Fysiek hulpmiddel (handleiding/handboek) (n = 274)*                                                                                                                                                                                                                                                                                                                                         | 8,7             | 44,4                 | 46,9           |
| In een team (n = 274)                                                                                                                                                                                                                                                                                                                                                                       | 4,7             | 48,0                 | 46,9           |
| Technologisch hulpmiddel (webapp cybercrime, chatbot)                                                                                                                                                                                                                                                                                                                                       | 12,4            | 47,3                 | 40,4           |
| Zelf informatie op te zoeken/te lezen (handboek/ intranet/ mailing)*                                                                                                                                                                                                                                                                                                                        | 21,8            | 50,2                 | 28,0           |
| Alleen (n = 271)                                                                                                                                                                                                                                                                                                                                                                            | 35,6            | 50,5                 | 12,4           |
| In een online setting                                                                                                                                                                                                                                                                                                                                                                       | 42,5            | 46,2                 | 11,3           |
| <i>Notitie. *Voor deze items zijn significante, maar kleine verschillen gevonden tussen de functiegroepen.<sup>a</sup></i>                                                                                                                                                                                                                                                                  |                 |                      |                |
| <sup>a</sup> Voor de volgende vier items zijn significante, maar kleine verschillen gevonden tussen de functiegroepen: Tijdens reguliere werkzaamheden ( $p = 0,10$ , $\eta^2 = 0,049$ ), Zelf informatie op te zoeken/lezen ( $p = 0,014$ , $\eta^2 = 0,049$ ), Buiten reguliere werkzaamheden ( $p = 0,009$ , $\eta^2 = 0,040$ ) en Fysiek hulpmiddel ( $p = 0,016$ , $\eta^2 = 0,039$ ). |                 |                      |                |

Ook is gevaagd welke factoren volgens respondenten belangrijk zijn voor de ontwikkeling van kennis en vaardigheden in de aanpak van online criminaliteit (n = 266). Ze

19 Voor de volgende drie items zijn significante maar kleine verschillen gevonden tussen de functiegroepen: Ben gemotiveerd ( $p = 0,002$ ,  $\eta^2 = 0,034$ ), Werk nauw samen met collega's ( $p = 0,008$ ,  $\eta^2 = 0,047$ ) en Motiveer zelf collega's ( $p < 0,001$ ,  $\eta^2 = 0,097$ ). Het laatste item, Motiveer zelf collega's, heeft wel een middelgroot effect, maar er zijn geen noemenswaardige verschillen tussen de functiegroepen (er is namelijk geen absoluut verschil van de gemiddelden van de functiegroepen groter dan 0,5).

konden zowel individuele als organisatorische factoren rangschikken op volgorde van belangrijkheid. Per factor wordt beschreven op welke rangpositie deze het vaakst door respondenten is geplaatst.

De 'eigen motivatie' komt naar voren als belangrijkste factor: 29,1% van de respondenten plaatst deze op de eerste plaats. Dit benadrukt het belang van een persoonlijke bereidheid om verder te ontwikkelen op het digitale thema. Daarnaast is ook prioritering vanuit de werkgever belangrijk (24% van de respondenten plaatst dit op nummer 1). Actieve sturing en aandacht voor het digitale thema binnen de organisatie zijn dus ook van belang om ontwikkeling te stimuleren. Dit wordt gevolgd door facilitering vanuit de organisatie in de beschikbaarheid van een goed leeraanbod (27,6% plaatst dit op nummer 2), tijd van de werkgever (18,2% plaatst dit op nummer 2) wat de nadruk van toegankelijke en kwalitatieve scholing onderstreept. Ondersteunende factoren zijn goede hulpmiddelen (laptops, telefoons et cetera) (22,9% plaatst dit op nummer 3) en het leren van enthousiaste collega's (21,5% plaatst dit op nummer 4).

Wat verder opvalt, is dat bijna alle respondenten (87,6%) de 'Ik wil helemaal niets leren over online criminaliteit' op de laatste plaats zetten. Ook de beloning vanuit de werkgever wordt door een heel grote groep (68,0% plaatst dit op nummer 7) niet gezien als een belangrijke factor om aan te zetten tot de ontwikkeling van kennis en vaardigheden.

## Resumé

De meeste respondenten zijn 'enigszins' geïnteresseerd om te leren over online criminaliteit. Ruim de helft van de respondenten uit de basisteams van de politie lijkt tevens gemotiveerd om te ontwikkelen in hun kennis en vaardigheden om online criminaliteit beter aan te pakken. Terwijl iets minder dan de helft van de respondenten belemmeringen ervaart om hierin te ontwikkelen. De meesten zien een intrinsieke motivatie en prioritering vanuit de werkgever als belangrijkste randvoorwaarden. Tevens zijn randvoorwaarden vanuit de organisatie nodig om in de digitale transformatie te faciliteren, zoals de beschikbaarheid van een goed leeraanbod, tijd van de werkgever en goede hulpmiddelen. Ze willen het liefst leren in een fysieke setting, van politiecollega's binnen of buiten het basisteam en tijdens reguliere werkzaamheden. Ze willen niet leren in een online setting, noch alleen, noch door zelf informatie op te zoeken of te lezen. Opvallend is dat de beloning vanuit de werkgever en de stelling 'ik wil helemaal niets leren' duidelijk laag scoren in belangrijkheid. Kortom, ontwikkeling lijkt vooral gedreven door een intrinsieke motivatie en duidelijke prioritering door de organisatie met bijbehorende facilitering. Extrinsieke prikkels zoals een beloning spelen hierbij een relatief beperkte rol.

## 5 Ontwerponderzoek: lokale interventies

In dit hoofdstuk worden de lokale interventies die zijn ontwikkeld, uitgevoerd en geëvalueerd besproken. Bij basisteam Postenveld gaat het om twee interventies: HINT-oefeningen en kennislunches (paragraaf 5.1). Bij basisteam Lichtblauwveen zijn door te grote weerstand onder de basisteammedewerkers geen interventies uitgevoerd. Wel wordt door ons verslag gedaan van het proces wat daar is doorlopen (paragraaf 5.2).

### 5.1 Interventieaanpak Postenveld

In dit traject staat de interventieaanpak zoals doorlopen in basisteam Postenveld centraal, waarin achtereenvolgens de voorbereiding, interventieontwikkeling, uitvoering en evaluatie worden gerapporteerd. Tijdens de uitvoering zijn twee interventies daadwerkelijk toegepast in de praktijk, waarna in de evaluatiefase is nagegaan in hoeverre de beoogde doelen van de interventie zijn behaald en welke verbeterpunten er zijn. Aan het einde van deze paragraaf worden principes voor intensivering gepresenteerd. Voordat we hier op ingaan, beschrijven we eerst de ontwikkelingen die zich binnen het basisteam hebben afgespeeld.

Tussen de dataverzameling (lokale interviews en landelijke vragenlijst) en de terugkoppeling van de resultaten (paragraaf 5.1.1) is circa een jaar verstreken. In deze periode hebben zich binnen basisteam Postenveld verschillende organisatorische en personele veranderingen voorgedaan. Zo is een digitaal wijkagent aangesteld die de ontwikkeling van de aanpak van online criminaliteit binnen het team aanjaagt. Samen met een nieuwe interim OS-C fungeert hij als belangrijkste contactpersoon voor dit thema in deze fase van het project.

Daarnaast zijn zowel landelijk als lokaal stappen gezet om de aanpak van online criminaliteit te intensiveren. In mei 2025 is met de digitaal wijkagent en interim OS-C de actuele stand van zaken besproken en gereflecteerd op veranderingen ten opzichte van de situatie ten tijde van de eerdere interviews. Hieruit blijkt onder meer dat de samenwerking met het digitaal platform – dat politiecollega's op districtsniveau ondersteunt bij de bestrijding van online criminaliteit – is aangepast. In plaats van de geplande structurele deelname aan triage – een werkwijze om te bepalen welke aangiften worden opgepakt en welke vragen nodig zijn voor een betere aangifte – is gekozen voor direct contact met de basisteamrecherche vanwege het beperkt aantal digitale zaken op het basisteam.

Ook zijn nieuwe middelen en werkwijzen geïntroduceerd. Zo is begin 2025 de digi-assistent ingevoerd, een app die politiemedewerkers ondersteunt bij meldingen van on-

line criminaliteit. Tevens is in de loop van 2025 een landelijke werkwijze geïmplementeerd (Digitaal Ter Plaatse, voorheen Digitale Meldkamer), waarvan de communicatie en borging binnen het basisteam zijn belegd bij de digitaal wijkagent. Binnen het team is daarnaast concrete ontwikkelbereidheid zichtbaar, bijvoorbeeld doordat zeventien medewerkers interesse hebben in een OSINT-cursus en er plannen zijn voor meerdere HINT-oefendagen in het najaar van 2025 (zie ook paragraaf 5.1.2).

### Voorbereiding

In mei 2025 zijn de eerdere resultaten uit het onderzoek teruggekoppeld aan het basisteam. Aanwezig waren de digitaal wijkagent, de interim OS-C, toekomstige OS-C, een OS-A (portefeuillehouder digitaal), een senior tactische opsporing van Team Cybercrime en drie onderzoekers. Tijdens deze bijeenkomst zijn de belangrijkste bevindingen gepresenteerd en gezamenlijk besproken. Aansluitend zijn doelstellingen vastgelegd.

Uit de eerdere dataverzameling in dit onderzoek blijkt dat politiemedewerkers een duidelijke **toename van online criminaliteit** in de samenleving ervaren, maar dat het **zicht op de lokale omvang beperkt** is. Gedigitaliseerde vormen van criminaliteit, zoals telefonische helpdeskfraude, hulpvraagfraude, diefstal van gegevens en afpersing, worden vaker herkend dan meer complexe cybercrime, zoals DDoS-aanvallen. Tegelijkertijd onderschrijven medewerkers de noodzaak om deze problematiek als basisteam op te pakken, in lijn met het Toewijzingskader Cybercrime (2023), waarin een rol is weggelegd voor basisteams bij enkelvoudige zaken met 'lage complexiteit' en 'lage politieke gevoeligheid'.

De haalbaarheid van deze ambitie wordt echter door medewerkers van basisteams sterk betwijfeld. Zes belangrijke knelpunten worden door hen benoemd:

- i. een **tekort aan digitale kennis en vaardigheden**;
- ii. **lage motivatie** om online criminaliteitszaken op te pakken;
- iii. **onduidelijke doelstellingen** omtrent de aanpak van online criminaliteit;
- iv. een **verschil in affiniteit** met online criminaliteit;
- v. de **kwetsbaarheid van enkele enthousiastelingen** (bijvoorbeeld door overvraging en bij eventueel vertrek zijn er nog minder kennis en ervaring aanwezig); en
- vi. **capaciteitsgebrek** over de gehele organisatie. Over dit laatste punt geeft een van de aanwezigen aan dat capaciteitsgebrek een te gemakkelijk argument is. Volgens deze respondent zouden hierover gesprekken gevoerd moeten worden, maar ligt de nadruk vooral op het stellen van duidelijke prioriteiten vanuit het management.

De eerste drie knelpunten worden als beïnvloedbaar beschouwd door de aanwezigen. Dat betekent dat zij denken hier zelf iets aan te kunnen doen. Deze knelpunten vormen daarom belangrijke aangrijpingspunten voor de interventies (zie paragraaf 5.1.2). Vrijwel alle deelnemers aan de voorbereidingssessie zien ontwikkelmogelijkheden om het kennis- en vaardighedeniveau omhoog te brengen en meer dan 80% heeft (enige) interesse in verdere professionalisering. De behoefte richt zich inhoudelijk op kennis over (het herkennen van) online criminaliteitsvormen, trends, juridische kaders en

opsporingsmogelijkheden. Qua vaardigheden ligt de nadruk op het verbeteren van aangiften, slachtofferadvisering, inzicht in en begrip van *modus operandi* en het uitvoeren van online bronnenonderzoek. Daarnaast worden organisatorische behoeften benoemd, zoals betere samenwerking met specialistische teams, korte communicatielijnen en meer leren aan de hand van 'echte' praktijkcasussen. Ook is er behoefte aan een kernteam van specialisten binnen het basisteam.

De bevindingen uit de interviews en vragenlijsten onder medewerkers van de basisteams worden door de aanwezigen breed herkend. Tegelijkertijd blijkt dat het formuleren van concrete doelen voor interventies op basis van deze resultaten lastig is, mede doordat landelijke en eenheidsdoelen als abstract worden ervaren. Ondanks dit spanningsveld is er duidelijk draagvlak binnen het managementteam voor verdere ontwikkeling op de aanpak van online criminaliteit en bestaat er behoefte aan concrete, lokaal toepasbare doelstellingen. Daarbij adviseren zij dat doelstellingen niet individueel per basisteam opgesteld moeten worden, maar op eenheidsniveau.

### **Interventieontwikkeling en uitvoering**

Tijdens de bijeenkomst rondom de ontwikkeling van de interventie is met de deelnemers verkend hoe interventies effectief kunnen worden vormgegeven. Daarbij is aangesloten bij enkele duidelijke ontwerpprincipes op basis van het voorgaande onderzoek: leren vindt bij voorkeur plaats in een fysieke setting, samen met en van collega's en zo veel mogelijk in de praktijk (*learning by doing*). Minder effectief worden individueel en online leren, of het zelfstandig bestuderen van informatie, geacht. Deze uitgangspunten vormen de basis voor de verdere ontwikkeling van interventies binnen dit onderzoek.

Voor de ontwikkeling van interventies in basisteam Postenveld is een gefaseerd en iteratief proces doorlopen. In de voorbereidingsfase is via deskresearch<sup>20</sup> en praktijkgesprekken<sup>21</sup> een inventarisatie gemaakt van bestaande interventies gericht op het vergroten van digitale kennis en vaardigheden binnen basisteams.<sup>22</sup> Deze inzichten zijn in mei gedeeld met het basisteam, waarna gezamenlijk is gereflecteerd en doelstellingen en interventiemogelijkheden zijn vastgesteld. In maandelijkse vervolgbijeenkomsten zijn deze uitgewerkt tot een concreet actieplan.

In totaal vonden acht formele overlegmomenten plaats, aangevuld met frequent informeel contact, waarbij onderzoekers en teamleden gezamenlijk optrokken. Dit resulteerde in twee uitgevoerde interventies. De eerste is een 'HINT'-oefening. HINT staat voor Heterdaad INternetfraude en verwijst naar een handelingskader dat is ontwikkeld om de kans op heterdaadsituaties bij online fraude te vergroten. Dit kader is ge-

20 Het deskresearch beperkte zich tot een zoektocht op het Intranet van de Politie.

21 Praktijkgesprekken vonden in een periode van april-oktober 2025 onder andere plaats met digi-coaches, digi-professionals, projectleiders, digitaal wijkagenten en een Senior Tactische Opsporing (STO'er) van Team Cybercrime.

22 De geïnventariseerde interventies betreffen actiedagen (zoals HINT-oefendagen), gaming varianten (Digi-beat gericht op basisteam en online criminaliteit), het inzetten van een escaperoom (via het VAK), het doorlopen van een cybercrisissimulatie met het basisteam en de inzet van een digi-coach of digi-prof.

richt op basisteams en biedt informatie over fysieke signalen die kunnen wijzen op online criminaliteit en informatie over hoe daarmee om te gaan. De tweede is een kennislunch met ondersteunende *nudges*. Deze twee interventies hadden tot doel om bij te dragen aan: I) vergroten van kennis en vaardigheden, II) verhogen van de lage motivatie en III) werken met concrete doelen.<sup>23</sup> De interventies zijn hierna nader uitgewerkt. In bijlage VIII is een volledige tijdlijn van de interventieontwikkeling opgenomen en de mate van participatie van de onderzoeker uiteengezet.

### *Interventie 1: HINT-oefening*

De eerste interventie bestond uit de uitvoering van zogenoemde HINT-oefeningen (i.e. actiedagen). Dit is een bestaande interventie gericht op het vergroten van de heterdaadkracht bij online criminaliteit. De interventie beoogde zowel de bewustwording, het urgentiebesef als de digitale handelingsvaardigheden van operationele collega's te versterken. Daarbij lag de nadruk op het herkennen van signalen van online criminaliteit in het dagelijks werk, het benutten van digitale opsporingskansen, het toepassen van bevoegdheden en het verbeteren van de hulpverlening aan slachtoffers. Tevens werd aandacht besteed aan het kennen en benutten van specialistische ondersteuning binnen de politieorganisatie.

De opzet van de actiedagen was uniform. Iedere sessie startte met een gezamenlijke introductie over de aard en omvang van online criminaliteit en het bijbehorende handelingskader dat werd ingezet. Vervolgens werkten deelnemers in kleine groepen aan realistische casuïstiek, afgewisseld met inhoudelijke toelichting door een collega van het digitaal platform. De eerste casus speelde zich af in een schoolomgeving en de tweede casus betrof het doorzoeken van een auto op een parkeerterrein. De casuïstiek bood deelnemers de mogelijkheid om signalen te herkennen, digitale gegevensdragers te identificeren en het handelingskader in de praktijk toe te passen. De oefening werd afgesloten met een debriefing, bestaande uit een korte vragenlijst en een groepsgeprek waarin ervaringen en leerpunten werden besproken. De casus in de schoolomgeving is ter observatie meegenomen in het onderzoek en was als volgt:

*Een docent meldt verdacht gedrag van een groep studenten op een hogeschool. De jongeren lopen in en uit het gebouw, hebben veel bankpassen en telefoons op tafel liggen, gedragen zich verdacht en lijken regelmatig te bellen. Er lijkt moeilijk contact te zijn tussen de docent en de studenten. Bij aankomst van de politie herhaalt de docent deze melding.*

23 De interventies kenden ook enkele basisteamspecifieke doelen, maar die vallen buiten beschouwing van onderhavig onderzoek. Hierbij kan gedacht worden aan het stimuleren van digitaal wijkgericht werken.

*Studenten zijn geïnstrueerd om in een studieruimte te zitten en chaos te veroorzaken. Ze plegen gezamenlijk bankhelpdeskfraude/nepagentenfraude vanuit de schoollocatie en gebruiken daar middelen zoals bankpassen, een ledger,<sup>24</sup> telefoons en een laptop. Op de laptop staat meerdere tabbladen open, waaronder een leadslijst,<sup>25</sup> Anydesk<sup>26</sup> en internetbankieren. Ook liggen er andere relevante spullen, zoals een politievest (nepagentenfraude), een identiteitsbewijs, lijst met pincodes en simkaarten. De studenten zijn geïnstrueerd om de politie op het verkeerde spoor te zetten met een alternatief verhaal dat ze aan een schoolopdracht werken, dat de spullen van vrienden zijn en verder vaag te blijven.*

In totaal zijn drie oefensessies uitgevoerd (op 11 september, 17 september en 2 oktober 2025) voor medewerkers van de basisteamrecherche en de incidentafhandeling. Verdeeld over deze drie sessies sloten 29 medewerkers van het basisteam aan. De uitvoering liet zien dat deelnemers in wisselende mate in staat waren om digitale signalen te herkennen en hierop te handelen. Over het geheel genomen werd zichtbaar dat collega's actief van elkaar leerden en elkaar aanspoorden in het handelen. Eén deelnemer uit de eerste oefenronde gaf aan: *'Ach, zo moeilijk is het allemaal niet, het is hetzelfde als traditioneel onderzoek, met wat digitale elementen.'* Tegelijkertijd bleek dat digitale elementen, zoals het veiligstellen van gegevensdragers en het herkennen van specifieke hulpmiddelen, niet altijd consistent werden benut. In sommige gevallen lag de focus vooral op aanhouding, terwijl digitale bewijsvoering minder aandacht kreeg.

Tussen de sessies was sprake van ontwikkeling. In de eerste uitvoeringen viel op dat relevante digitale informatie soms werd gemist (bijvoorbeeld het niet vinden van digitale apparaten in een chaotische context) en dat sturing tijdens de casus beperkt was. In latere oefeningen, met name wanneer een digitaal specialist aanwezig was, verbeterde dit zichtbaar. Deelnemers kregen gerichte feedback tijdens en na de oefening, waardoor zij beter inzicht kregen in digitale opsporingsmogelijkheden, het veiligstellen van sporen en het gebruik van hulpmiddelen, zoals de digi-koffer.<sup>27</sup> Dit droeg bij aan meer bewust en doelgericht handelen. Feedback bestond onder andere uit het verstrekken van informatie (bijvoorbeeld over verschillende digitale gegevensdragers en wat leadslijsten zijn), stellen van vragen (bijvoorbeeld: *'Ga je dit zelf doen, of bel je iemand?'*), maar ook door aan te geven wat goed gaat en wat er eventueel gemist is.

24 Een ledger is een merk van hardware wallets voor cryptocurrency. Het is een fysiek apparaat, vergelijkbaar met een USB-stick, waarop *private keys* worden opgeslagen, zodat men toegang krijgt tot hun digitale valuta.

25 Leadslijsten bestaan uit contactgegevens zoals naw-gegevens, bankrekeningnummers en telefoonnummers. Deze worden gebruikt om bijvoorbeeld bankhelpdeskfraude te plegen.

26 Anydesk is software voor *remote access*, waarmee op afstand verbinding gemaakt kan worden met een ander digitaal apparaat. Door dit programma kan een ander besturingssysteem (zoals een computer) beheerd worden alsof je er zelf achter zit.

27 De digi-koffer bevat fysieke hulpmiddelen om digitale sporen veilig te stellen, zoals een mouse jigglers en op-laadkabels.

### *Interventie 2: Kennislunch*

De tweede interventie bestond uit de ontwikkeling en uitvoering van kennislunches, aangevuld met *nudges*. Het doel was het vergroten van digitale bewustwording en handelingsbekwaamheid binnen het basisteam, door maandelijks een digitaal thema centraal te stellen. Elke themamaand zou worden geopend met een kennislunch waarin een onderwerp op laagdrempelige wijze werd besproken. Ter versterking van de thematische aandacht zouden gedurende de maand aanvullende *nudges* worden ingezet, in de vorm van korte en activerende prikkels zoals kennistoetsen, interactieve puzzels en bespreken van casuïstiek. De keuze voor een lunchsessie was zowel praktisch als strategisch. Deze sloot aan bij bestaande routines van medewerkers (lunchen op het politiebureau) en fungeerde tegelijkertijd als extra stimulans voor deelname.

Voor de eerste kennislunch is gekozen voor het overkoepelende thema online criminaliteit, waarbij zowel verschillende vormen van cybercrime als gedigitaliseerde criminaliteit, en relevante juridische aspecten (zoals strafbaarstelling) aan bod kwamen. De interventie werd actief onder de aandacht gebracht onder alle basisteammedewerkers via e-mailuitnodigingen, een herinnering vooraf, communicatie tijdens de briefing, ondersteunende posters en een prijsuitreiking voor deelnemers van een kennistoets (zie hierna). Op basis hiervan meldden zich 27 medewerkers aan en namen uiteindelijk ongeveer dertig medewerkers deel, voornamelijk afkomstig uit opsporing en I&S. De kennislunch vond plaats op 15 oktober 2025 in een volledig bezette kantine. Het inhoudelijke deel duurde circa dertig minuten, en het geheel ongeveer vijfenveertig minuten. Voor en na de inhoud was er respectievelijk ruimte voor de introductie van het kennislunchconcept en was er ruimte voor vragen en een korte evaluatie. Ter ondersteuning zijn twee *nudges* ingezet. De eerste was een online kennistoets of quiz op basis van online casuïstiek, waarin deelnemers negen meerkeuzevragen beantwoordden over het handelingsperspectief van politiemedewerkers, met directe feedback op hun antwoorden. Deelname werd gestimuleerd door een kleine *incentive*, waarbij een prijs werd uitgereikt onder de deelnemers tijdens de kennislunch. De tweede *nudge* bestond uit een fysieke puzzel waarin deelnemers vormen van online criminaliteit koppelden aan de juiste definities.

De uitvoering van de interventie week af van de oorspronkelijke planning. Aanvankelijk was het de bedoeling om de verschillende kennislunches op meerdere locaties en momenten binnen het basisteam aan te bieden, maar door capaciteitsproblemen en tijdsdruk binnen het basisteam is dit teruggebracht tot één sessie op één locatie. Daarnaast werd de uitvoering overgenomen door de cybervrijwilliger en de onderzoeker, nadat de digitaal wijkagent hier door tijdsgebrek niet toe in staat was. Een tweede sessie die was voorbereid, gericht op bankhelpdeskfraude (in aansluiting op de HINT-oefening), is uiteindelijk niet uitgevoerd binnen het tijdsbestek van het onderzoek.

### **Evaluatie**

Tijdens de uitvoering van beide interventies zijn (on)gestructureerde observaties gedaan. Daarnaast is de HINT-oefening geëvalueerd met een vragenlijst die is afgenomen via Microsoft Forms ( $n = 26$ ; 90% nettorespons). Tien respondenten waren werk-

zaam bij VVC en zestien bij de incidentafhandeling van het basisteam. De gemiddelde invultijd voor de vragenlijst was vierenhalve minuut. Daarnaast zijn drie focusgroepen georganiseerd, die ieder dertig minuten duurden. De eerste focusgroep ( $n = 10$ ) vond plaats op 11 september, de tweede ( $n = 9$ ) op 17 september en de derde ( $n = 10$ ) op 2 oktober 2025, aansluitend op de debriefing van de drie HINT-oefeningen. De focusgroepen dienden om de ervaringen en leeropbrengsten van de oefening te verdiepen. Daarbij is onder andere ingegaan op de waardering van de oefening, het ervaren leer-effect en de meest waardevolle onderdelen. Ook zijn verbeterpunten en toekomstige leerbehoeften en voorkeuren voor leervormen geïnventariseerd. De antwoorden zijn ter plekke genoteerd door een onderzoeker. De kennislunch is geëvalueerd met observaties voor, tijdens en na de tijd. Deelnemers werd gevraagd naar hun motivatie voor deelname, hoe de sessie in zijn geheel is bevonden, wat hen inhoudelijk is bijgebleven en welke thema's in de toekomst centraal moeten komen te staan.

#### *Bevindingen vragenlijst HINT-oefening*

De evaluatie van de HINT-oefening laat een overwegend positief beeld zien van zowel de ervaren opzet als de leeropbrengsten (zie tabel 5.1). Uit de vragenlijsten blijkt dat deelnemers de oefening (redelijk) goed konden volgen en actief konden participeren. De meerderheid geeft aan dat de behandelde vaardigheden toepasbaar zijn in de praktijk en dat hun kennis over online criminaliteit, in het bijzonder bankhelpdeskfraude, is toegenomen. Ook voelt een deel van de deelnemers zich beter in staat om meldingen zelfstandig af te handelen. Tegelijkertijd blijft ongeveer de helft van de groep terughoudend of neutraal in het vertrouwen om dit daadwerkelijk te doen.

Tabel 5.1 Antwoorden op vragenlijst na HINT-oefening in aantallen (n = 26)

| Stelling                                                                                                             | Goed | Redelijk goed | Neutraal | Een beetje | Niet |
|----------------------------------------------------------------------------------------------------------------------|------|---------------|----------|------------|------|
| <i>Volgbaarheid HINT-oefening</i>                                                                                    |      |               |          |            |      |
| Ik vind dat ik tijdens de HINT-oefening goed heb mee kunnen doen (n = 25)                                            | 16   | 8             | 1        | 0          | 0    |
| <i>Kennis en vaardigheden</i>                                                                                        |      |               |          |            |      |
| Ik verwacht dat ik de vaardigheden die ik tijdens de HINT-oefening heb geleerd, kan toepassen in de praktijk         | 9    | 12            | 2        | 2          | 1    |
| Mijn kennis en vaardigheden in het aanpakken van bankhelpdeskfraude zijn door de HINT-oefening toegenomen            | 7    | 13            | 5        | 1          | 0    |
| Door de HINT-oefening voel ik mij beter in staat om zelfstandig een melding van bankhelpdeskfraude af te handelen    | 5    | 9             | 9        | 3          | 0    |
| <i>Zelfvertrouwen</i>                                                                                                |      |               |          |            |      |
| Door de HINT-oefening heb ik meer vertrouwen gekregen in mijn eigen kunnen bij het afhandelen van bankhelpdeskfraude | 3    | 10            | 10       | 3          | 0    |
| Door de HINT-oefening voel ik minder terughoudendheid bij het afhandelen van bankhelpdeskfraude                      | 3    | 8             | 11       | 4          | 0    |
| Door de HINT-oefening neem ik sneller actie bij een melding van bankhelpdeskfraude                                   | 4    | 15            | 7        | 0          | 0    |
| <i>Affiniteit</i>                                                                                                    |      |               |          |            |      |
| Ik heb affiniteit in het aanpakken van online criminaliteit                                                          | 2    | 9             | 6        | 7          | 2    |

De invloed op zelfvertrouwen en handelingsbereidheid is gematigd positief. Ongeveer de helft van de deelnemers ervaart meer zelfvertrouwen en minder terughoudendheid bij het afhandelen van meldingen, terwijl de andere helft slechts beperkte of geen verandering aangeeft. Wel geven de meeste deelnemers aan sneller geneigd te zijn actie te ondernemen bij signalen van online criminaliteit. De affiniteit met het thema verschilt. Het merendeel ervaart een redelijke of beperkte betrokkenheid, terwijl slechts een enkeling zich sterk verbonden voelt met het onderwerp.

Tot slot is gevraagd wat goed en minder goed werkte bij de HINT-oefening. De waardering voor de werkvorm is positief. Met name de combinatie van een theoretische introductie en het oefenen met praktische casuïstiek wordt als effectief gezien. Er zijn twee, enigszins tegenstrijdige, verbeterpunten gegeven. Eén deelnemer vond dat er onnodig veel diepgang was en de oefening meer gericht moest zijn op het praktische politiewerk. Een andere deelnemer zocht juist meer verbreding en gaf aan dat het: 'rele-

*vant [zou] zijn om meer kennis op te doen over andere relevante vormen van digitale criminaliteit. Ik weet er nog te weinig van.'*<sup>28</sup>

### *Bevindingen focusgroepen HINT-oefening*

De focusgroepen verdiepen dit beeld en laten zien dat de oefening vooral heeft bijgedragen aan bewustwording. Deelnemers geven aan dat zij beter in staat zijn om digitale signalen en hulpmiddelen te herkennen, zoals het herkennen van een ledger, flipper zero<sup>29</sup> en andere tools en digitale gegevensdragers. Meerdere deelnemers realiseerden zich dat ze dergelijke objecten in de praktijk hadden gezien zonder hun betekenis te herkennen. Daarnaast geven deelnemers aan het belang van zorgvuldig handelen van digitale sporen beter te begrijpen.

Een praktische oefening werkt volgens hen beter dan enkel naar iemand te luisteren of door het volgen van een e-learning. Eén deelnemer verwoordde dit treffend: *'Alleen theorie houden we niet vol. Door het te doen en te zien, onthoud ik het beter.'* Tegelijkertijd bestaat er nog onzekerheid over de praktische toepassing, met name rond het veiligstellen van digitale gegevens en het correct inzetten van bevoegdheden. Dit hangt samen met ervaren tekorten in kennis, capaciteit en ondersteuning binnen het basisteam. Ook zegt een van de deelnemers: *'De kans dat het op deze manier in de praktijk voorkomt is klein, maar je weet nu wel waar je op moet letten.'*

Een terugkerend punt in alle drie de focusgroepen is behoefte aan betere samenwerking en afstemming tussen disciplines, in het bijzonder tussen incidentafhandeling en opsporing. Deelnemers benadrukken dat duidelijkheid over rollen, verantwoordelijkheden en vervolgacties essentieel is voor effectief handelen. Zo lijkt het hen verstandig om eerst af te stemmen met een gespecialiseerde collega, zoals Senior Tactische Opsporing, over wat relevant en haalbaar is. Zoals een deelnemer stelde: *'Als je iets in beslag neemt, moet je er ook onderzoek naar doen. Maar dat onderzoek is niet in enkele dagen gedaan.'* Daarnaast wordt gewezen op een bredere organisatorische opgave. Hoewel online criminaliteit als prioriteit wordt gezien, ontbreekt het vaak structureel aan tijd en expertise om hier adequate uitvoering aan te geven.

Net als in de eerdere onderzoeksresultaten komt ook in de focusgroepen naar voren dat er sprake is van een lage motivatie voor het aanpakken van online criminaliteit. Er lijkt ook een terughoudendheid te zijn om te handelen uit angst fouten te maken of bewijsmateriaal te verliezen. Praktijkervaring en herhaling worden gezien als belangrijke voorwaarden om dit te doorbreken. Deelnemers geven dan ook een duidelijke voorkeur aan praktijkgerichte leerinterventies boven e-learning, en pleiten voor meer structurele en herhaalde trainingsmomenten, bij voorkeur geïntegreerd in het reguliere werk. Tot slot wordt gewezen op aanvullende leerbehoeften, zoals verdieping in juridische kaders, digitale opsporingsmiddelen en het veiligstellen van bewijs, en op innovatie leermiddelen, zoals VR-brillen of virtuele simulaties, waarmee realistische

28 Andere deelnemers gaven geen antwoord op deze vraag (n = 11), antwoordden met *niet van toepassing* (n = 9) of gaven een opmerking, zoals *'alleen maar positief'* of *'kan niks bedenken, alles was leerzaam'*.

29 De flipper zero is een hardware apparaat, een multitoel, die diverse draadloze signalen kan opvangen en nabootsen. Dit apparaat kan worden gebruikt om te hacken.

scenario's kunnen worden geoefend. Ook het thema fysieke en digitale veiligheid van politiemedewerkers zelf wordt expliciet genoemd als aandachtspunt. Dit duidt erop dat het thema (digitale) weerbaarheid ook binnen het basisteam verdere aandacht behoeft.

### *Bevindingen kennislunch*

Tijdens de sessie werd actief geluisterd en na een korte verstoring, waarin een deelnemer twijfelde over de relevantie van het onderwerp voor het basisteam en meerdere deelnemers zich ergerden aan deze twijfel, herstelde de aandacht zich snel. De werkvorm bleek toegankelijk en effectief. Vrijwel alle aanwezigen vulden de beschikbare puzzel in en waardeerden de combinatie van inhoud en spelelementen. Dit leidde ertoe dat na afloop een aanvullende *hand-out* is ontwikkeld, waarin kernbegrippen en definities overzichtelijk zijn samengebracht en samen met de presentatie en puzzel met de deelnemers is gedeeld.

De bijbehorende kennistoets werd door achttien medewerkers ingevuld, grotendeels voorafgaand aan de kennislunch. De inzet van een incentive, in de vorm van een verloting, droeg zichtbaar bij aan betrokkenheid en een positieve sfeer. Daarbij lag de nadruk bewust op deelname (de eerste deelnemer 'wint') in plaats van prestatie (beste score), om de drempel tot meedoen te verlagen en digitale terughoudendheid te verminderen.

Uit een korte mondelinge evaluatie en reacties achteraf blijkt dat het initiatief breed werd gewaardeerd. We kregen meerdere positieve reacties terug, zoals: '*Goed dat jullie dit organiseren*' en '*Leuk gedaan, graag vaker*'. Tegelijkertijd kwam naar voren dat er behoefte is aan meer inhoudelijke verdieping en meer taakspecifieke invulling, afgestemd op verschillende afdelingen zoals I&S, opsporing en incidentafhandeling. De kennislunch wordt met name geschikt geacht voor I&S en opsporing. Voor de incidentafhandeling lijkt deelname lastiger vanwege de beperkte planbaarheid van het werk, wat vraagt om alternatieve interventievormen.

### *Overkoepelend beeld*

Afsluitend is er een evaluatiegesprek gehouden met de digitaal wijkagent, de cybervrijwilliger en een OS-C. Beide interventies laten ook bij hen een positief beeld achter. De samenwerking werd als constructief ervaren en de gekozen interventies droegen bij aan zichtbare voortgang op het digitale thema. Er is volgens hen sprake van meer bewustwording en een stimulans in kennis en vaardigheden, al blijven kennis, zelfvertrouwen en capaciteit nog kwetsbare factoren. Om duurzame verandering te realiseren, zijn structurele organisatiebrede ondersteuning en scholing noodzakelijk, waarbij wij hebben kunnen laten zien welke benadering werkt en dat politiemedewerkers bereikt konden worden.

Voor de toekomst is het voornemen om de kennislunch structureel voort te zetten en verder te differentiëren naar doelgroep. Ook bestaat de ambitie om de interventie uit te breiden naar andere locaties binnen het basisteam, ondanks praktische beperkingen zoals een lage bezetting per locatie. Tegelijkertijd wordt ingezet op verdere versterking van het digitale thema binnen het team, onder meer door uitbreiding van capaciteit,

continue afstemming en duidelijkere rolverdeling. De OS-C geeft aan dat daarmee het thema nog niet geborgd is, maar wel dat eraan wordt gewerkt. De OS-C sluit het evaluatiegesprek af: *‘Ik vond het een fijne manier van actief onderzoek doen in de praktijk zelf en er gelijk mee aan de slag [gaan]’*, en de digitaal wijkagent: *‘Jammer dat het eindigt’*.

## 5.2 Interventieaanpak Lichtblauwveen

Hoewel het uiteindelijk niet is gelukt om ook binnen basisteam Lichtblauwveen een interventie daadwerkelijk te implementeren, zijn in het voorjaar van 2025 hiertoe door de onderzoekers wel stappen gezet om via cocreatie met de teamleiding en medewerkers van het basisteam tot de ontwikkeling van een interventie te komen die zou bijdragen aan de intensivering van de lokale aanpak van online criminaliteit. De onderzoekers hebben hiervoor contact gezocht met het basisteam, maar al snel bleek dat belangrijke contactpersonen waren vertrokken naar andere teams of afdelingen en dat degenen die hen waren opgevolgd onvoldoende waren ingewerkt of zelf onvoldoende overtuigd waren van de lokale aanpak van online criminaliteit.

De personeelswisselingen – die overigens kenmerkend zijn voor hoe de politieorganisatie werkt – zorgden ervoor dat de enige, overgebleven contactpersoon te maken kreeg met een verhoogde werkdruk door aanvullende taken. Zo was er sprake van een nieuwe teamchef, was de digi-coach gedetacheerd naar een extern digitaal team en werden de twee digitaal wijkagenten die affiniteit met de aanpak van online criminaliteit hadden afwisselend voor perioden van een halfjaar ingezet op andere afdelingen vanwege personeelstekorten. Doordat het mandaat voor samenwerking aan het begin van het ontwerponderzoek niet expliciet was vastgelegd, waren de onderzoekers grotendeels afhankelijk van de *goodwill* van de resterende medewerkers binnen het basisteam. Hierdoor begon de opzet van de cocreatie in dit onderzoek feitelijk weer vanaf het begin.

In totaal zijn door de onderzoekers opvolgend vier pogingen ondernomen om binnen dit basisteam een geschikte ingang en kartrekker te vinden om de samenwerking op gang te brengen. In dit hoofdstuk wordt beschreven hoe deze pogingen zijn verlopen en welke inzichten dit heeft opgeleverd, ondanks het uitblijven van een concrete interventie.

### Voorbereiding

In deze alinea beschrijven we de verschillende pogingen die zijn gedaan om de ontwikkeling en het uitvoeren van een interventie bij Lichtblauwveen van de grond te krijgen.

#### *Oriëntatiegesprek (21 mei 2025)*

De voormalige contactpersoon van het onderzoeksteam binnen basisteam Lichtblauwveen was inmiddels werkzaam als Operationeel Specialist (OS-C) en overgeplaatst buiten het basisteam. Desondanks namen hij en een expert van het team Digitale Transformatie (DiTra) deel aan een oriëntatiegesprek waarin zij reflecteerden op de situatie

binnen het basisteam. Het gesprek startte met een presentatie van de resultaten uit de lokale interviews en de nationale vragenlijst (hoofdstukken 3 en 4). Op basis hiervan identificeerden de respondenten een aantal structurele knelpunten in de lokale aanpak van online criminaliteit.

Het eerste knelpunt betreft de kwaliteit van het intelligencebeeld. De deelnemers benadrukken dat de effectiviteit van opsporing samenhangt met de kwaliteit en volledigheid van gegevensverzameling in het veld. Dit vraagt om gerichtere uitvraag bij slachtoffers en om concrete handvatten voor politiemedewerkers om relevante informatie systematisch vast te leggen in het intelligence-systeem.

*‘Het labeltje is niet interessant – milieu, ondermijning of cyber – het gaat om de maatschappelijke impact. Als de intel en vulling van systeem goed van kwaliteit is, kan je daarmee aan de slag gaan. Ga situaties goed loggen in de uitvoering. Zoals een digi-wijkagent: ga een query draaien die dagelijks op een aantal zaken worden rapporteert, zodat je een informatiestroom op gang brengt.’*

Daarnaast wordt gewezen op de relatief grote discretionaire ruimte in de taakuitvoering, met name binnen de incidentafhandeling, waarmee men in de uitvoering nog veel vrijblijvendheid lijkt te ervaren in de aanpak van online criminaliteit. *‘Het is eigenlijk heel bijzonder dat je ergens werkt en er verandert iets aan je werk en dat er zoveel vrije ruimte is dat je kan zeggen: “ik heb er geen affiniteit mee.”’* In tegenstelling tot de private sector ontbreekt binnen de politie een externe prikkel tot verandering, al signaleren de respondenten wel een geleidelijke verschuiving door instroom van nieuwe generaties medewerkers met een meer nieuwsgierige houding; zij initiëren zelf vaker vragen. De klassieke collega leunt op parate kennis. *‘Daar moeten gewoon een of twee generaties overheen gaan’.*

Ten aanzien van professionalisering achten de deelnemers basisteambrede initiatieven, zoals een ‘digi-dag’ (in lunchvorm), weinig effectief, mede gezien de operationele context met onregelmatige diensten (bijvoorbeeld nacht- en avonddiensten). *‘Er is op het basisteam helemaal geen ruimte om met lunches te werken, dan krijg je er twee van de tweehonderd. Het online aspect moet in het werk. Het moet echt via het werk, hoe ziet een dienst eruit, welke meldingen kom je? Ga een maand lang meldingen meelopen en knal de socials eruit. Overlast van een skatepark kon je zien door wie daarover aan het posten waren, vanuit het Real Time Intelligence Centre.’* Zij pleiten in plaats daarvan voor een de benadering ‘learning by doing’, waarbij ervaring centraal staat in het ontwikkelen van vertrouwen in eigen handelen.

Op organisatieniveau signaleren de deelnemers een gebrek aan structurele borging van de aanpak van online criminaliteit. Hoewel er landelijk een toewijzingskader (2023) bestaat, is dit binnen het basisteam niet formeel geïmplementeerd. Eveneens zijn er op eenheidsniveau KPI's (targets) vastgesteld, maar de huidige registratiewijze beperkt de representativiteit daarvan. *‘Daarnaast worden jammers al registreert als cybercrime, want je hackt het systeem, dan worden er al snel vinken in de systemen gezet. Wat is nu de maatschappelijke impact? Zet je dan via verkeer in op jammers, zodat je er per week*

*er een aantal hebt, of ga je vanuit de bedoeling werken? Met maatschappelijke impact.* Ook wordt er gesteld dat er een beperkt taakbesef is rondom de online criminaliteitsdoelstellingen. *‘In de frontlinie komt het niet tussen de oren dat daar een taak ligt, zo worden fraude in webshops waarin accounts zijn overgenomen afgeboekt op ID-fraude, terwijl dit als hacking geclassificeerd moet worden.’*

Verder blijkt dat bestaande faciliteiten, zoals het digitaal informatiepunt binnen het basisteam, onvoldoende worden benut. De deelnemers relateren dit mede aan negatieve sociale dynamieken, zoals pestgedrag. *‘Bij vijftig-zestig procent van de teams speelt dit, dat flyers weggegooid worden et cetera. Als je wat anders doet dan wat gevestigd is, zul je moeten laten zien wat je komt doen en toegevoegde waarde hebben.’* Wel wijzen ze erop dat vergelijkbare voorzieningen in andere teams wel effectief kunnen zijn. *‘Basis-team [Lichtblauwveen] is anders dan andere basisteams. Daar zit een historie van radicale keuzes, waardoor er echt anders wordt gekeken naar zaken rond digitaal.’*

Tot slot benadrukken de deelnemers dat capaciteitsproblemen structureel van aard zijn. In plaats van uitbreiding van capaciteit zien zij meer potentie in het anders organiseren van het werk, bijvoorbeeld door het versterken van thematische affiniteit binnen het team of het gericht aantrekken van expertise van buitenaf. *‘Als je daarvoor kiest, zegt dat iets over wat je van belang vindt.’*

#### *Briefing (28 mei 2025)*

Na het oriëntatiegesprek ontbrak een duidelijke kartrekker binnen het basisteam. Daarom is een brede uitnodiging verstuurd naar alle afdelingen (I&S, recherche, incidentafhandeling en leiding) van het basisteam. De onderzoekers sloten vervolgens aan bij een briefing waar alle uitgenodigde personen welkom waren om aan te sluiten. Deelname was vrijwillig; uiteindelijk waren er 23 medewerkers (voornamelijk incidentafhandeling) aanwezig. Deze setting fungeerde als het ware als een grote focusgroep. Tijdens de bijeenkomst presenteerden de onderzoekers resultaten uit lokale interviews en de nationale vragenlijst. De interactie was hoog. De groep herkende de toename van online criminaliteit en medewerkers gaven zelfs aan ook zelf slachtoffer te zijn geweest. *‘We zijn allemaal de sjaak geweest met diefstal gegevens tijdens de politie hack.’* Er is echter weinig zicht op opvolging van verdachten door gebrek aan terugkoppeling. Het toewijzingskader (2023) bleek grotendeels onbekend en een e-learning blijkt beperkt. Over het toewijzingskader zei iemand: *‘Omdat het vaak in kantjes en boekjes van zestien pagina’s staat en ik druk ben, dus delete’.* Over e-learnings gaf iemand aan: *‘Deze klikken we gewoon door, “geef toe”’,* wat leidde tot instemmend gelach onder de aanwezigen. Affiniteit met digitale criminaliteit was unaniem afwezig; er werd gepleit voor een gespecialiseerd team. Handelingsverlegenheid speelt volgens de aanwezigen een rol: aangiftes worden soms (deels) bij het slachtoffer neergelegd en verantwoordelijkheden worden doorgeschoven. Ook capaciteitstekort werd daarbij als belangrijke belemmering genoemd.

Op de vraag wie affiniteit had met de aanpak van online criminaliteit kwam een unaniem antwoord: stilte. Er werd aangegeven dat verantwoordelijkheid voor digitale zaken vaak werd doorgeschoven. Er werd suggereerd dat er een apart team moest wor-

den opgericht dat dit oppakt. *‘Voor ons is het een te ver van onze bedshow. Je hoopt dat de melding naar een andere collega gaat, maar het gaat een keer gebeuren dat jij die moet oppakken,’* zei een aanwezige van de incidentafhandeling medewerkers. Een ander zei: *‘Te veel en te moeilijk, ik blijf erbij dat er een apart team moet komen.’* Tot slot gaf iemand aan: *‘Nu schuiven we het af naar een collega, de digi-wijkagent.’* Ook capaciteit werd benoemd als obstakel om aan de slag te gaan met online criminaliteit. Naast obstakels legden sommigen het capaciteitsvraagstuk anders uit. *‘Capaciteitsgebrek is ook keuzes maken, we gaan wel naar winkeldiefstal, dus met OM andere keuzes in maken.’* Iemand uit de opsporing zei: *‘Als we blijven doen wat we nu doen beëindigen we vanuit de opsporing alle zaken waar jullie [Blauw] twee uur aan hebben zitten tikken.’*

Naast doorschuiven werd ook gesproken over samenwerking met andere afdelingen. Hierover werd het volgende gezegd:

*‘We hebben verschillende afdelingen binnen politie met cyber. Best lastig met hen in contact te komen, iedereen zegt wij doen dit en niet dat, er moet een ingangspunt komen in plaats van dat wij moeten leuren met een aangifte, hangt er een verkeerde code aan dan doen ze het niet.’*

Ongeveer de helft van de aanwezigen ervaart naar eigen zeggen een lage motivatie. Daarnaast leeft frustratie over de snelle digitale ontwikkelingen en de aansluiting van de organisatie hierop. *‘Probleem van de politie, is dat we altijd achter de feiten aanlopen. Je hoort altijd bij de politie, waarom wordt dit nu van mij verwacht? Weten het al vijf jaar dus hadden ze moeten aanpakken en nu ben je gewoon te laat.’* Ook ging het over de ervaring van leren: *‘Het is niet iets wat je met een melding geleerd hebt. Ik denk alleen maar zo snel mogelijk op papier zetten.’* En een ander zei: *‘Binnen tweeëneenhalf uur leer ik niet wat phishing is.’* Tot slot gaf een andere aanwezige aan: *‘Ik weet niet eens hoe ik diensttelefoon moet inregelen, daar hebben wij collega’s voor.’*

Het basisteam werd vergeleken met een ‘huisarts’, een eerste aanspreekpunt dat voor specialistische problematiek moet doorverwijzen.

*‘Je moet van alles wat weten en dan doorverwijzen naar specialist. Zolang je die keuze hebt, specialiseer je je ook niet. Vanuit blauw moet je evengoed weten wat je bij reanimatie en met tourniquet moet doen, net als bij woning inbraak en dan forensische opsporing (FO) laten komen.’*

Volgens een leidinggevende, die na de briefing werd gesproken, leidt dit er soms toe dat inspanningen voor verandering als tevergeefs worden ervaren.

*‘Het is nu alles of niets. Maar waar maak je op inhoud keuzes op. Dat willen we wel, maar dat mag nog niet. [...]. Bij winkeldiefstal moet OC zelf al keuzes maken, het gevoel echt iets te kunnen betekenen is nodig. Meemaken en meevoelen. Je moet ze tijd en ruimte geven, vaak is het een gegeven wat op ons afkomt, maar je krijgt ze niet mee. Wij weten als leidinggevend ook niet hoe we het moeten overdragen want we*

*weten het zelf ook niet, dan is het te groot en komt het bij ons terecht en ben je huisarts en specialist in één.'*

#### *Gesprek met team Digitale Transformatie (1 juli 2025)*

Tijdens de bijeenkomst identificeerden de onderzoekers opnieuw *geen* concrete, kansrijke digitale aanjagers voor verdere interventie-ontwikkeling. Daarom hebben de onderzoekers besloten met DiTra in gesprek te gaan, dit keer met twee experts van deze afdeling, onder wie de persoon die ook bij het eerste gesprek aanwezig was. Mogelijk beschikte DiTra over inzichten in manieren waarop dergelijke aanjagers binnen het basisteam bereikt of gecreëerd konden worden, evenals over verklaringen voor de knelpunten die de voortgang van de aanpak van online criminaliteit binnen dit basisteam hebben belemmerd. Dit gesprek leverde een aantal belangrijke inzichten op. Allereerst blijkt dat structurele verandering vraagt om duidelijke organisatorische commitment. Binnen het basisteam is de werkwijze van de leidinggevende sterk autonoom, wat ertoe leidt dat sturing beperkt wordt ervaren ('we moeten niks'). Medewerkers worden bovendien niet aangesproken op het uitblijven van registraties van online criminaliteit, waardoor de aanpak in de praktijk sterk afhankelijk is van individuele motivatie, affiniteit en inspiratie. Ook spelen culturele factoren een rol. Ter illustratie wordt aangegeven dat slachtoffers helpen onder medewerkers niet 'cool', maar daders pakken wel 'gaaf' wordt gevonden. Dit geldt vooral binnen de incidentafhandeling. Daarnaast is er duidelijk sprake van verandermoeheid binnen het team, wat een belangrijke belemmering vormt voor nieuwe initiatieven. De gesprekspartners vroegen zich af hoe je hier goed mee kunt omgaan. Dit hangt samen met een breder patroon binnen het basisteam dat wordt geschetst. Ambities zijn volgens de gesprekspartners vaak mooi, maar worden door personeelsverloop en wisselingen niet volledig gerealiseerd. Dit wijst op het belang van het formuleren van kleinere, concretere en haalbare interventies. Een combinatie van bottom-upinitiatieven, ondersteund door duidelijke top-downsturing en borging, lijkt hierbij kansrijk. Gezamenlijk kwam het idee tot stand om een focusgroep met experts op verschillende functieniveaus en afdelingen (I&S, basisteamrecherche en incidentafhandeling) binnen het basisteam te organiseren waarin de eerder opgehaalde resultaten worden teruggelinkkoppeld. Het doel is om een open dialoog te faciliteren ('wrijving is glans'), waarbij ook ruimte is voor kritische geluiden en emoties. Hiermee kunnen de oorzaken en onderliggende redenen waarom medewerkers bepaalde taken niet bereid zijn op zich te nemen (i.e. weerstand) worden onderzocht. Het betrekken van de teamchef wordt hierbij als belangrijk gezien, om bottom-upinzichten te vertalen naar gedragen en uitvoerbare acties.

#### *Expertgesprek (1 juli 2025)*

Na het gesprek met de twee experts van DiTra werden de onderzoekers doorverwezen naar een expert op het gebied van digitale transformatie en innovatie die kon ondersteunen bij het opzetten van een focusgroep binnen het basisteam. Dit gesprek leverde aanvullende inzichten op.

Binnen het team is formeel een aanjager (OS-C) aanwezig op het thema verandering en operatie, maar deze rol wordt in de praktijk onvoldoende ingevuld. Effectief aanjagen vraagt volgens de expert om een combinatie van inhoudelijke kennis van online criminaliteit én het vermogen om deze kennis toegankelijk en begrijpelijk te vertalen naar het uitvoeringsniveau. Daarbij is een benaderbare houding essentieel ('Ik laat het je wel zien'). De opvatting heerst bij de expert dat het deze persoon momenteel ontbreekt aan concrete handelingsperspectieven, zoals het stellen van de juiste vragen. Zeker als iemand nieuw in het team is kan dit voor kwetsbaarheid zorgen. De expert geeft aan dat bij de politie iemand eerst 'blauw geverfd' moet worden.

Daarnaast kwam naar voren dat historische factoren bijdragen aan de huidige weerstand. In het recente verleden heeft de teamleiding sterk ingezet op het agenderen van online criminaliteit, mede vanuit opdracht van hogere hand. Deze top-downbenadering heeft echter tot een sterke aversie binnen het team geleid, wat nog steeds doorwerkt in de houding ten opzichte van nieuwe initiatieven die hieraan raken.

Als interventie stelde de expert voor om te starten met een kleine intervisiegroep. Het doel hiervan is om gezamenlijk te bepalen welke stappen nodig zijn om weer energie te creëren, en deze direct te koppelen aan een concreet fenomeen. Belangrijk hierbij is een zorgvuldige samenstelling van de groep, met ruimte voor kritische geluiden om 'groupthink' te voorkomen. Echter, de organisatie van deze sessie is uiteindelijk niet van de grond gekomen, mede door planningsproblemen en beperkte beschikbaarheid (mede door de zogenoemde NAVO-top-vakanties).

### **Gevolgtrekking**

Ondanks de verschillende pogingen van de onderzoekers om binnen basisteam Lichtblauw een interventie gericht op de intensivering van de aanpak van online criminaliteit te ontwikkelen, concludeerden de onderzoekers in overleg met vertegenwoordigers van het programma Politie en Wetenschap en de begeleidingscommissie uiteindelijk dat dit binnen de looptijd van het onderzoek niet haalbaar was. Het ontbreken van een duidelijke kartrekker of andere vormen van draagvlak binnen het basisteam, beperkte beschikbaarheid van betrokkenen, capaciteitsdruk en een collectieve en sterke weerstand tegen de aanpak van online criminaliteit op de werkvloer maakten dat het niet lukte om voldoende draagvlak en continuïteit te organiseren voor een concrete interventie. De voorgenomen focusgroep en intervisievorming kwamen daarvoor niet van de grond.

Tegelijkertijd leverden de gesprekken waardevolle inzichten op in de onderliggende mechanismen die de lokale aanpak van online criminaliteit beïnvloeden, zoals handelingsverlegenheid, verandermoeheid, onduidelijkheid over verantwoordelijkheden en de spanning tussen bottom-upmotivatie en top-downsturing. Deze inzichten vormden aanleiding om het vervolg van dit onderzoek te verbreden naar een landelijk perspectief. In het volgende hoofdstuk wordt daarom aan landelijk experts onder andere de vraag voorgelegd of de beperkte ontwikkeling van de aanpak van online criminaliteit primair moet worden begrepen als een cultuurvraagstuk, of dat juist sterkere formele sturing via taken, rollen en verantwoordelijkheden noodzakelijk is.

## 6 Interviewresultaten intensivering

### 6.1 Inleiding

Voor het laatste onderdeel van dit onderzoek zijn er in totaal tien interviews afgenomen met verschillende experts op het gebied van de aanpak van online criminaliteit, binnen (onder anderen een medewerker van het Nationaal Team Digitale Transformatie, de landelijke portefeuille GGP, een senior medewerker Intelligence, een medewerker van het OSC en een cybervrijwilliger) en buiten de politie (onder anderen een organisatieadviseur en een medewerker van het Openbaar Ministerie), zie ook paragraaf 2.5. Zoals in het methodenhoofdstuk beschreven, heeft de analyse van deze resultaten plaatsgevonden via codering. In de uitwerking hierna staan het aantal keer dat de respondenten een onderwerp in de interviews ter sprake brachten tussen haakjes vermeld om de lezer een indruk te geven van het relatieve belang dat door de respondenten aan de elementen van het overkoepelende verhaal werd gehecht. Het aantal uitspraken ligt in sommige gevallen hoger dan het aantal respondenten, omdat één respondent meerdere relevante uitspraken kon doen.

### 6.2 Landelijk en lokaal voorbij de lokale vrijblijvendheid sturen

De respondenten waren tijdens de interviews duidelijk ten aanzien van het landelijke beleid. Wat hen betreft zijn er doelstellingen en KPI's nodig ten aanzien van online criminaliteit (24). Deze doelstellingen op eenheidsniveau moeten vervolgens worden vertaald naar district- en basisteamniveau. Een dergelijk beleid ontbreekt nu echter op landelijk niveau (4). Volgens hen dient de huidige vrijblijvendheid in de aanpak van online criminaliteit door middel van landelijk beleid te worden verminderd (10). Daarbij geldt dat het moeilijke gesprek over wat de politie vervolgens minder of niet meer gaat doen ook moet worden gevoerd, want voor politiewerk geldt volgens de respondenten dat er doorgaans wel taken bijkomen, maar er geen taken vanaf worden gehaald (10). Hierover moeten landelijk, maar ook lokaal, duidelijke afspraken worden gemaakt (9).

Online criminaliteit is volgens de respondenten nog te veel onderbelicht gebleven en daarmee is er een disbalans ontstaan tussen de inzet van de politie ten aanzien van traditionele en online criminaliteit (13), terwijl de aantallen slachtoffers (8) en de impact van slachtofferschap (7) veel meer inzet van de politie zouden rechtvaardigen. Dit zal een verdere druk op de capaciteit van de politieorganisatie – die ook nog te maken

heeft met bezuinigingen – betekenen (12). Maar hierbij merken meerdere respondenten op dat de politie altijd al te maken heeft met een tekort aan capaciteit. Hierop vormen duidelijke keuzes en afspraken de uitweg (5).

Daarbij merken de respondenten op dat het aanpakken van online criminaliteit in hun ogen zowel een specialisatie als algemene politietaken betreft (7). Daarbij is vooral de opsporing van meer complexe en internationale zaken volgens hen een specialisme, maar is het aanpakken van eenvoudigere zaken van online criminaliteit in hun ogen een algemene politietaken (8). Hierbij merken zij op dat lokaal echter de traditionele ‘bloed en spoed’ politietaken nog voorrang krijgen (9), waarmee het lokaal oppakken van deze nieuwe politietaken momenteel vooral een kwestie van affiniteit is (14). Doorgaans wordt door de basisteams nog weinig eigenaarschap ervaren (2). Daarbij vormt ook de geografische focus van de politie een belemmering voor de aanpak van online criminaliteit, omdat politiemedewerkers primair gericht zijn op zaken binnen het eigen verzorgingsgebied, terwijl online criminaliteit zich vaak niet beperkt tot één geografisch gebied (14): daders en slachtoffers zijn immers over heel het land, en zelfs daarbuiten, verspreid.

Om de online criminaliteit door daders vanuit het buitenland aan te kunnen pakken, moet er landelijk worden ingezet op de internationale samenwerking (5), maar ook moet er landelijk worden geïnvesteerd in de informatiepositie van de politie, waarmee grip wordt verkregen op de grote hoeveelheden data rondom zaken van online criminaliteit (12). Hierbij wordt door de respondenten veelal gesproken over een landelijk datacenter voor online criminaliteit (7). Door zaken te koppelen moeten zowel lokale daders (7) als slachtoffers (5) beter inzichtelijk worden gemaakt. Door een landelijke analyse ontstaat daarmee in potentie ook een samenhangende, lokale aanpak (9). Dit gebeurt momenteel vanuit de aanpak die vanuit het Project Centurion is ontwikkeld – dat als vervolg op de werkwijze vanuit het Landelijk Meldpunt Internetoplichting (LMIO) is ingezet (4). De respondenten geven echter aan dat het lokaal oppakken van deze zaken nog te vrijblijvend is, waardoor het voor hen onduidelijk is in welke mate dit ook daadwerkelijk gebeurt (6).

Duidelijk is dat de basisteams, ten aanzien van ‘eenvoudige’ zaken van online criminaliteit, een belangrijke schakel vormen (10). Daarom moet op het niveau van de basisteams volgens de respondenten worden ingezet op het vergroten van de basiskennis over online criminaliteit (11), omdat de kennis en vaardigheden op dit moment onvoldoende zijn om de nieuwe taken op te kunnen pakken (9). Hierbij wordt echter nadrukkelijk opgemerkt dat de basisteams er niet alleen voor staan, maar moeten kunnen rekenen op hun collega's met ervaring en expertise. De aanpak van online criminaliteit drijft dus goeddeels op de kwaliteit van interne samenwerking (7).

De respondenten beschrijven voor de leiding van de basisteams een ‘fikse’ taak om te sturen op het oppakken van taken ten aanzien van online criminaliteit (25). Naast het geven van prioriteit aan zaken van online criminaliteit (23) komt deze taak neer op het vergroten van de basiskennis van personeel (12) en ruimte geven aan personeel voor deskundigheidsbevordering ten aanzien van de lokale aanpak van online criminaliteit (8), omdat routine grotendeels ontbreekt (4). Dit zal per basisteam echter neerkomen

op maatwerk (9). Gezien de impact van deze verandering is het ontstaan van een lage motivatie (5) en weerstand (6) onder personeel volgens de respondenten geen verrassing. Het antwoord op deze weerstand en de lage motivatie om online criminaliteit aan te pakken wordt door de respondenten gevonden in de impact van slachtofferschap van online criminaliteit (6), waarbij het nodig is dat de politie met de tijd meebeweegt met nieuwe vormen van criminaliteit (6). Daarbij kan het helpen om de lokale beelden van daders en slachtoffers als vertrekpunt te nemen, om deze vaak abstract beleefde vormen van criminaliteit concreter en invoelbaarder te maken voor het personeel.

Dat is ook het doel van de unaniem bepleitte verander- en leerstrategie van *learning by doing* (20). Hierbij zou het personeel van basisteams groepsgewijs en in offline bijeenkomsten (5) samen concrete, lokale casuïstiek aan moeten pakken en zich daarbij vooral moeten richten op de eenvoudige vormen van online criminaliteit (14), waarbij ook bijzondere aandacht is voor de online componenten in criminaliteit binnen de relationele sferen. Ook zouden basisteams de restinformatie die uit onderzoeken door cybercrimeteams of andere opsporingsteams naar voren is gekomen kunnen oppakken om de lokaal actieve daders en netwerken beter in kaart te brengen en deze te verstoren. Hierbij kunnen digi-coaches en andere specialisten (16) en *early adopters*<sup>30</sup> in de basisteams (11) hun collega's ondersteunen in het zich eigen maken van de nieuwe politietaken. Daarbij wordt ingespeeld op de primaire leerbehoefte van medewerkers in de basisteams: leren van collega's (16), waarbij kennisoverdracht via e-learningen zo veel mogelijk wordt beperkt vanwege de weerstand die hiertegen bestaat (9). Daarbij is naast groepsgewijs leren ook het samenwerken met specialisten (5) en het hebben van korte lijnen met experts (12) van belang, zoals ook in het project De Digitale Meldkamer in de eenheid Oost-Nederland positief is ervaren (5).

Wel merken de respondenten op dat er onderscheid moet worden gemaakt in wat medewerkers van basisteams, per functie, zouden moeten weten en kunnen ten aanzien van de aanpak van online criminaliteit (13) en wordt dit idealiter een vast onderdeel van deze bestaande functies (6) met bijbehorende kennisstandaard (2). Basisteams zouden volgens de respondenten een externe samenwerking met partners moeten aangaan (11) in het versterken van de weerbaarheid van de lokale samenleving tegen online criminaliteit in de vorm van preventie (6). Ook hebben medewerkers van de basisteams wat de respondenten betreft vooral een signalerende functie (6): zij moeten online criminaliteit kunnen herkennen, weten hoe zij in de basis moeten handelen in acute situaties, digitale sporen kunnen veiligstellen en aangiftes kunnen opnemen. Ook moeten zij slachtoffergericht kunnen optreden (13): slachtoffers kunnen helpen, adviseren en in- en extern doorverwijzen. Ten aanzien van daders kan naast strafrechtelijke aanpak ook nadrukkelijk worden gekeken naar andere, betekenisvolle afdoenin-

30 De term '*early adopters*' komt uit de *Diffusion of Innovations* theorie van Rogers (2003), ook bekend als de Innovatietheorie. Hij beschrijft hierin hoe nieuwe innovaties zich verspreiden binnen een sociale groep. *Early adopters* (pioniers) zijn volgens de theorie een groep mensen die relatief vroeg een innovatie omarmen. Ze volgen de zogeheten *innovators* en spelen een belangrijke rol doordat zij vaak invloedrijk zijn binnen hun netwerk. Hun acceptatie helpt om anderen te overtuigen en versnelt de verdere verspreiding van een innovatie binnen een groep.

gen (3). Ten aanzien van de opsporing kan worden nagedacht over een *dedicated* team (4) op eenheidsniveau waar in Oost-Nederland ook al is geëxperimenteerd met een samenwerking met het Openbaar Ministerie in de HUB (6).

### 6.3 Conclusies en principes voor landelijke opschaling

De respondenten benadrukken dat landelijk beleid nodig is om de vrijblijvendheid in de aanpak van online criminaliteit door basisteams te doorbreken. Momenteel ontbreekt een heldere vertaling van landelijke doelstellingen naar het lokale niveau, wat binnen de basisteams leidt tot een disbalans tussen de inzet voor traditionele en online criminaliteit. Ondanks bezuinigingen en capaciteitstekorten moet de politie volgens de respondenten duidelijke keuzes maken en prioriteit geven aan online criminaliteit, getiteld op het hoog aantal slachtoffers en de impact ervan. Daarbij merken de respondenten op dat de aanpak van eenvoudige zaken van online criminaliteit een algemene politietask voor de basisteams is. De meer complexe en internationale zaken zijn wat hen betreft voor experts elders in de organisatie.

Lokale basisteams hebben momenteel echter onvoldoende kennis, vaardigheden en eigenaarschap voor de aanpak van online criminaliteit, mede door de geografische focus van de politie. Landelijke samenwerking (bijvoorbeeld een landelijk datacenter voor online criminaliteit) en investeringen in de informatiepositie zijn noodzakelijk om grip te krijgen op data en lokale daders en slachtoffers beter in kaart te brengen. Basisteams spelen volgens de respondenten een cruciale rol in de aanpak van eenvoudige online criminaliteit, maar hebben ondersteuning nodig van specialisten (bijvoorbeeld digi-coaches, digitale opsporing, cybercrimeteams) en ruimte om te leren (bijvoorbeeld via *learning by doing* en groepsgewijs leren). Leidinggevendenden moeten hier prioriteit aan geven, sturen op verandering en weerstand begeleiden, waarbij korte lijnen met experts en duidelijke afspraken essentieel zijn.

De respondenten benadrukten concluderend dat de aanpak van online criminaliteit niet vrijblijvend mag zijn en dat landelijk beleid, duidelijke prioriteiten en leiderschap essentieel zijn in de opschaling van taken van de basisteams in de aanpak van online criminaliteit. Lokale basisteams moeten worden ondersteund met kennis, praktische handvatten en ruimte om te leren, waarbij samenwerking (intern en extern) en slachtoffergericht handelen centraal staan. De reacties van de respondenten hebben geleid tot een nadere aanscherping van de door de onderzoekers ontwikkelde principes voor de landelijke opschaling van taken in de lokale aanpak van online criminaliteit (zie bijlage VI). De aangepaste principes worden hieronder weergegeven.

#### *Principe #1 – Urgentie van online criminaliteit voelbaar maken*

De urgentie voor de aanpak van online criminaliteit moet zichtbaar en voelbaar zijn voor alle medewerkers van de basisteams, door lokale casuïstiek te gebruiken (bijvoorbeeld verhalen van slachtoffers en daders uit het eigen werkgebied) om de impact te illustreren. Daarbij kunnen data worden ingezet om de omvang (aantallen slachtoffers, schadebedragen) en kwalitatieve impact (bijvoorbeeld emotionele gevolgen voor

slachtoffers) in kaart te brengen. Leidinggevendenden moeten prioriteit geven en sturen op de aanpak, waarbij slachtoffergericht optreden (bijvoorbeeld tegengaan van *victim blaming*) en het opnemen van aangiftes de urgentie versterken. Daarbij is het raadzaam om het rechtvaardigheidsgevoel van medewerkers aan te spreken. Medewerkers moeten inzien dat online criminaliteit net zo serieus is als traditionele criminaliteit. Een respondent benadrukte treffend dat door digitalisering tijd en plaats fluide zijn geworden, waardoor landelijke analyse en coördinatie nodig zijn om lokaal effectief te kunnen handelen in de aanpak van online criminaliteit.

*Principe #2 – Motivatie voor de lokale aanpak van online criminaliteit verhogen*

De lage motivatie onder medewerkers van de basisteams om online criminaliteit aan te pakken, kan worden verhoogd door succesverhalen over de aanpak van online criminaliteit door medewerkers van basisteams te delen (bijvoorbeeld concrete casuïstiek waar basisteams resultaat boeken). Hiertoe leent de *learning by doing*-strategie zich omdat de basisteams in kleine stappen zich deze nieuwe stappen eigen maken. Tussendoor kunnen collega's van het eigen en andere basisteams worden meegenomen in de successen. Zo ervaren medewerkers in de breedte dat zij daadwerkelijk verschil kunnen maken (bijvoorbeeld stopgesprekken bij *first offenders*, hulpverlening aan slachtoffers). Hierbij staat samenwerking met collega's (bijvoorbeeld *early adopters*, *digi-coaches*) en korte lijnen met experts (bijvoorbeeld via het Cybercrimeteam) centraal. Daarbij wordt idealiter ingezet op fysieke bijeenkomsten en groepsgewijs leren. E-learnings dienen volgens de respondenten te worden voorkomen omdat de weerstand hiertegen groot is. Overall moeten leidinggevendenden ruimte en prioriteit aan de aanpak van online criminaliteit geven en weerstand begeleiden. Medewerkers van de basisteams dienen het hybride karakter van de hedendaagse criminaliteit te omarmen: online en offline criminaliteit zijn vaak verbonden.

*Principe #3 – Intensiveren is maatwerk per basisteam*

De intensivering van de aanpak moet maatwerk zijn, afgestemd op capaciteit (fte's) en affiniteit van medewerkers. Hierbij kan het inzetten op een gemotiveerde groep *early adopters* bijdragen aan een breder enthousiasme onder medewerkers van de basisteams. Bij het eigen maken van nieuwe kennis en vaardigheden moet rekening worden gehouden met functiespecifieke kennis. Niet iedereen hoeft hetzelfde te weten. I&S, basisteamrecherche, incidentafhandeling en leiding hebben immers verschillende behoeften. Daarbij ligt in de aanpak door de basisteams de focus op eenvoudige vormen van online criminaliteit en wordt in de verandering idealiter een gebalanceerd tempo aangehouden (geen radicale omslag). Daarbij kunnen de nieuwe taken worden *geframed* als een thematische taak (net als georganiseerde misdaad) in plaats van een specialistische taak. De respondenten merken daarbij op dat het aanpakken van online criminaliteit door de basisteams niet vrijblijvend zou moeten zijn. Een groep respondenten vindt dat de aanpak verplicht moet zijn voor alle basisteams, gelet op de omvang en impact van online criminaliteit. Dit vergt zowel op landelijk als lokaal niveau dat er heldere keuzes worden gemaakt: leidinggevendenden moeten afspraken maken over

wat minder of niet meer wordt gedaan om capaciteit vrij te maken om zich de nieuwe taken in de aanpak van online criminaliteit eigen te maken. Momenteel staan de medewerkers van basisteams die online criminaliteit willen en aanpakken er nog redelijk vaak alleen voor. Zij zouden binnen hun basisteams kunnen fungeren als gidsen voor hun collega's, zonder dat zij de last van eventuele weerstand op zich zouden moeten krijgen. Het is immers aan het lokale leiderschapsteam om deze weerstand te herkennen en te begeleiden.

*Principe #4 – Heldere leerstrategie voor basisteams*

De leerstrategie wordt idealiter ingericht langs de leerstrategie van *learning by doing* in fysieke omgevingen, gericht op lokale casuïstiek (lokale slachtoffers of daders) en samenwerking met collega's binnen het basisteam, de eenheid en experts. Hierbij dient vooral in te worden gezet op groepsgewijs leren (geen e-learning of individueel leren) waarbij digi-coaches ondersteunen en medewerkers korte lijnen met experts (bijvoorbeeld digi-hulplijn) hebben. Leidinggevenden moeten ruimte geven om tijdens werktijd te leren en duidelijke afspraken maken. Een respondent wees hierbij op het praktijkgerichte opleidingsniveau en een verondersteld gebrek aan nieuwsgierigheid bij sommige medewerkers in de basisteams, wat extra begeleiding vanuit de teamchef en het kader vereist.

*Principe #5 – Rol van teamchefs en het kader: prioriteren, sturen en afdwingende macht*

Teamchefs en het kader van de basisteams moeten prioriteit geven aan de aanpak van online criminaliteit en sturen op daadwerkelijke uitvoering. Daarbij moeten zij medewerkers de ruimte bieden voor verandering en leren en eventuele weerstand tegen verandering begeleiden. Daarbij moeten met medewerkers en teams duidelijke afspraken worden gemaakt over taken die minder of niet meer worden gedaan. Het is daarbij van belang om tussendoor succes te vieren om medewerkers gemotiveerd te houden. Het is tevens van belang dat teamchefs en het kader informele processen in het team herkennen en hierop inspelen. Daarbij kunnen zij samenwerken met OpCo's, OSA's en experts van buiten het basisteam om deze transitie te ondersteunen. Dit doet volgens de respondenten een beroep op de veranderkundige vaardigheden van teamchefs en het kader: leidinggevenden moeten verleiden in plaats van dwingen, en effectief omgaan met weerstand.

*Principe #6 – De rol van de lokale cultuur: weerstand aanpakken*

Eerst een cultuurverandering doorvoeren voordat men met een basisteam inzet op de aanpak van online criminaliteit is volgens de respondenten niet altijd nodig. In plaats daarvan kan worden ingezet op het enthousiasmeren van een groep *early adopters* in basisteams die de lokale aanpak van online criminaliteit oppakken en hun collega's daarin – onder begeleiding en met steun van de teamchef en het kader – meenemen. Eventuele weerstand moet daarbij collectief worden aangepakt (niet individueel), waarbij teamchefs en het kader de informele processen in het team herkennen en daar – wanneer nodig – effectief op inspelen. Daarbij moet men voorbij de huidige vrijblij-

vendheid in de aanpak van online criminaliteit sturen. Leidinggevend en moeten prioriteit geven en sturen op de noodzaak hier vanuit de bestaande functies op te acteren. Deze aanpak kent echter een nadrukkelijke, geleidelijke opbouw. Medewerkers van basisteams moeten immers niet worden overspoeld met nieuwe taken, maar men moet hen hier stapsgewijs en in groepsverband aan laten wennen (bijvoorbeeld via *learning by doing* met ondersteuning van digi-coaches).



## 7 Conclusies, discussie, beperkingen en aanbevelingen

In dit hoofdstuk maken wij de balans op van het onderzoek. Allereerst komen de conclusie en discussie aan bod (paragraaf 7.1). Vervolgens beschrijven wij de beperkingen van het onderzoek (paragraaf 7.2). Tot slot presenteren we de aanbevelingen voor de praktijk en vervolgonderzoek (paragraaf 7.3).

### 7.1 Conclusie en discussie

Zoals in de inleiding van dit rapport is beschreven, is het doel van dit onderzoek om inzicht te bieden in hoe basisteams hun personeel effectief kunnen voorbereiden op de intensivering van de lokale aanpak van online criminaliteit, en handvatten te ontwikkelen voor toepassing in de politiepraktijk. Om dit doel te bereiken, is de volgende hoofdvraag geformuleerd: *Hoe kunnen basisteams van de politie hun personeel effectief voorbereiden op een intensivering van de lokale aanpak van online criminaliteit?* Deze hoofdvraag beantwoorden we in paragraaf 7.1.6 op basis van de antwoorden van de deelvragen (paragraaf 7.1.1-7.1.5).

**Deelvraag 1: Hoe percipiëren politiemensen van de basisteams de lokale taak, waar liggen wat hen betreft de zwaartepunten in de aanpak van online criminaliteit en wat hebben zij aan kennis en vaardigheden nodig om invulling aan deze taak te geven?**

Uit de interviews en vragenlijsten met medewerkers van basisteams komt naar voren de ideale, lokale aanpak zich volgens hen zou moeten focussen op het opnemen van betrouwbare aangiften, nazorg en preventie voor slachtoffers, en opsporing van kleinere online criminaliteitszaken. Respondenten benadrukken ook het belang van het verstoren van online criminaliteit en alternatieve interventies. Basisteams zouden zich volgens geïnterviewden moeten richten op gedigitaliseerde criminaliteit in plaats van cybercrime. Uitdagingen waar basisteams tegenaan lopen, zijn capaciteitsproblemen, lage motivatie en tekorten aan kennis en vaardigheden. Er zijn grote verschillen in expertise en interesse: van medewerkers die niets met online criminaliteit willen doen tot 'hobbyisten' die zich de materie zelfstandig eigen maken. Deze kennis neemt toe met ervaring, met name bij de vier Centurion-delicten (telefonische helpdeskfraude, aan- en verkoopfraude, hulpvraagfraude en phishing). Cybercrimezaken komen lokaal echter zelden voor, wat de onzekerheid onder personeel vergroot. Hoewel de meeste respondenten enige kennis en ontwikkelbehoefte aangeven, is er variatie in interesse.

Momenteel ligt de focus in de basisteams vooral op nazorg, terwijl respondenten alle vier de pijlers in de aanpak van online criminaliteit – opsporing, nazorg, verstoring en preventie – even belangrijk vinden. Cruciaal voor verbetering zijn het herkennen en veiligstellen van digitale sporen en het verhogen van kennis over juridische bevoegdheden, om zo de opsporingskansen te vergroten.

Uit de interviews met een dwarsdoorsnede van medewerkers van twee basisteams blijkt dat deze medewerkers een toename van online criminaliteit in de samenleving opmerken, maar dat zij minder zicht hebben op de omvang van online criminaliteit in hun eigen werkgebied. Het is onvoldoende duidelijk welke vormen van online criminaliteit veelvuldig voorkomen en welke (typen) daders hierbij betrokken zijn. Daarentegen hebben de geïnterviewden beter zicht op het slachtofferschap van online criminaliteit in het eigen verzorgingsgebied.

Eerder onderzoek (Akkermans et al., 2024; Arends et al., 2025; Borwell et al., 2024) laat zien dat slachtofferschap van online criminaliteit in alle lagen van de samenleving voorkomt en dat de impact heftig kan zijn op zowel financieel, emotioneel als psychisch vlak. De impact van slachtofferschap van online criminaliteit wordt ook door de meeste geïnterviewden (sterk) gevoeld en de meerderheid van vragenlijstrespondenten geeft aan dat online criminaliteit een grote impact heeft op de samenleving, waarbij niemand aangeeft dat deze impact klein wordt ingeschat. De geïnterviewden steunen de plannen uit het Toewijzingskader Cybercrime en Digitalisering (2023), die de lokale aanpak van online criminaliteit prioriteert, maar uiten tegelijkertijd aanzienlijke twijfels over de praktische uitvoerbaarheid ervan. Hierna gaan wij daar nader op in.

Uit zowel de interviews als de vragenlijst komt naar voren dat de focus van de lokale aanpak – in een ideaal scenario – moet liggen op I) het opnemen van correcte en betrouwbare aangiften, II) het helpen van slachtoffers in nazorg en preventie van (herhaald) slachtofferschap en III) het uitvoeren van opsporingsonderzoeken voor kleinere en minder complexe online criminaliteitszaken. Het opnemen van aangiften komt alleen naar voren in de interviews en is niet bevraagd in de vragenlijst. In de vragenlijst wordt door de respondenten ook het verstoren van online criminaliteit en alternatieve interventies belangrijk gevonden.

De vragenlijstrespondenten geven aan dat naar hun beeld andere afdelingen primair verantwoordelijk moeten zijn voor de aanpak van online criminaliteit, maar ook dat er een belangrijke rol is weggelegd voor (een deel van) het basisteam in samenwerking met andere afdelingen binnen de politie of externe organisaties. Volgens de geïnterviewden moeten basisteams zich wel richten op zaken van gedigitaliseerde criminaliteit en niet op cybercrime, die voor specialistische teams bestemd zouden moeten zijn. Dit is een afwijking van het Toewijzingskader (2023) dat niet alleen gedigitaliseerde criminaliteit maar ook ‘eenvoudige’ cybercrimezaken aan het basisteam toeschrijft.

Uit de interview- en vragenlijstresultaten blijkt dat medewerkers in de basisteams tegen de volgende punten aanlopen: I) capaciteitsproblemen, II) een lage motivatie om online criminaliteit aan te pakken en III) tekorten aan kennis en vaardigheden in de aanpak van online criminaliteit. Daarnaast is er een groot verschil in de interesse in online criminaliteit (zie ook Van Steden et al., 2025). Dit loopt uiteen van politiemensen

sen die expliciet ‘niets’ willen doen met online criminaliteit tot zogenaamde ‘hobbyisten’ die zich de materie zelfstandig eigen maken. De geïnterviewden signaleren dat geïnteresseerden binnen basisteams, die meer kennis over deze materie hebben, vaak snel doorstromen of naar een ander team overstappen, waardoor hun expertise verloren gaat. Deze uitdagingen voor de politie worden al meerdere jaren beschreven in de literatuur (onder andere in Jansen et al., 2020; Ruiter et al., 2023; Spithoven & Leukfeldt, 2023, Stol et al., 1999, Toutenhoofd-Visser et al., 2009).

Over het algemeen lijkt de basiskennis om online criminaliteit te bestrijden bij de meeste vragenlijstrespondenten in enige mate aanwezig. Hoe vaker politiemensen te maken krijgen met online misdrijven hoe beter ze weten hoe ze ermee om moeten gaan. Dit is vooral zichtbaar bij misdrijven die vanuit het Project Centurion naar de basisteams worden aangeleverd, waarbij relatief veel vragenlijstrespondenten aangeven te weten hoe zij deze zaken moeten aanpakken. Het is aannemelijk dat politiemensen weten hoe zij deze vier ‘Centurion-delicten’ – telefonische helpdeskfraude, aan- en verkoopfraude, hulpvraagfraude en phishing – kunnen aanpakken doordat zij hier relatief vaker mee te maken hebben gehad. Ervaring met cybercrimezaken komt echter zelden op lokaal niveau voor, waardoor de vragenlijstrespondenten waarschijnlijk aangeven minder goed weten hoe zij dergelijke zaken moeten aanpakken.

Uit alle resultaten blijkt dat er grote verschillen zijn in de gerapporteerde kennis en kunde van politiemensen op de basisteams. In de interviewresultaten kon een duidelijk onderscheid worden gemaakt tussen medewerkers met veel expertise en medewerkers met een lage motivatie. Dit verschil komt ook naar voren in de vragenlijstdata, waaruit wij observeren dat het gerapporteerde kennisniveau op dit thema sterk uiteenloopt. Over het algemeen geven de meeste vragenlijstrespondenten zelf aan enige kennis en kunde te hebben om online criminaliteit aan te pakken. Tegelijkertijd heeft het merendeel minimaal enige interesse om zichzelf hierin verder te ontwikkelen, waarbij iets minder dan de helft zelfs veel tot zeer veel interesse toont. Bij het interpreteren van deze resultaten moet rekening worden gehouden met zelfselectiebias (zie paragraaf 7.2). Politiemensen met meer interesse in online criminaliteit kunnen immers eerder geneigd zijn geweest om de vragenlijst in te vullen.

Als naar de gemiddelde antwoorden wordt gekeken, dan valt op dat de I&S-medewerkers verschillen van de andere groepen. De I&S-groep rapporteert het vaakst in aanraking te komen met online criminaliteit en geeft ook – naar eigen zeggen – het vaakst aan te weten hoe zij hiermee moeten omgaan. Of dit in de praktijk ook zo uitpakt, is de vraag. Van Steden en collega’s (2025) rapporteerden bijvoorbeeld diverse klachten van andere afdelingen binnen de basisteams over de kwaliteit van door I&S opgenomen aangiften van online criminaliteit. De I&S-groep scoort ook relatief hoog op aspecten zoals nazorg en preventieve taken, wat suggereert dat deze elementen als kernverantwoordelijkheden binnen hun functie worden beschouwd. Andere groepen, zoals de incidentafhandeling en de basisteamrecherche, leggen mogelijk andere accenten in hun werkzaamheden.

Uit de vragenlijstresultaten blijkt dat de behoefte aan verdere ontwikkeling onder respondenten varieert. Een klein aantal respondenten heeft ‘geen’ interesse in het uitbrei-

den van hun kennis en vaardigheden op het gebied van online criminaliteit. Daarentegen is er ook een kleine groep met een sterke ontwikkelbehoefte. De meeste respondenten tonen 'enige' tot 'veel' interesse in verdere scholing ten aanzien van de aanpak van online criminaliteit. Hoewel er geen significante verschillen tussen de functiegroepen zijn gevonden, wordt over het algemeen door de respondenten aangegeven dat er ruimte is voor verbetering van hun kennis en vaardigheden op dit gebied. Momenteel wordt binnen basisteams vooral ingezet op nazorg van slachtoffers, terwijl er relatief weinig aandacht is voor opsporing, verstoring en preventie. Dit wijkt af van de prioriteiten van de respondenten, die aangeven alle vier de pijlers (opsporing, nazorg, verstoring en preventie) even belangrijk te vinden. Daarnaast wordt door de respondenten in de interviews benadrukt dat het correct opnemen van aangiften wat hen betreft prioriteit verdient.

Dit sluit aan bij de bredere uitdagingen in de lokale aanpak van online criminaliteit. Zo zijn het herkennen en in kaart brengen van digitale sporen cruciaal voor effectieve opsporing. Meer kennis en kunde op dit vlak zou met name de I&S-medewerkers, alsook de incidentafhandeling, in staat stellen om aangevers beter te adviseren over het veiligstellen van digitale sporen. Betere aangiften met hogere opsporingsindicaties verhogen immers de kans op succesvolle opsporing. Daarnaast is het ontwikkelen van kennis over juridische bevoegdheden voor het gebruik van digitale informatie essentieel, aangezien hier relatief weinig kennis over aanwezig is onder medewerkers van de basisteams.

## **Deelvraag 2: Hoe pakken basisteammedewerkers online criminaliteit momenteel in de praktijk aan?**

Uit de vragenlijstresultaten blijkt dat er weinig tot geen uitvoering wordt gegeven aan de aanpak van online criminaliteit door de medewerkers van de basisteams. Er blijkt dat er vooral nazorg wordt geleverd aan slachtoffers van online criminaliteit. Dit kan vorm krijgen door hen te adviseren in het voorkomen van herhaald slachtofferschap. Een kleine groep medewerkers van de basisteams voert ook alternatieve interventies uit, zoals stopgesprekken met geldezels. Door basisteam Postenveld en Lichtblauwveen zijn verschillende stopgesprekken gevoerd met geldezels, in sommige gevallen samen met jongerenwerkers. Er is een kleinere groep medewerkers die online criminaliteit heeft opgespoord en een nog kleinere groep die aan preventie van online slachtofferschap heeft gewerkt. Er is niet tot nauwelijks ingezet op het verstoren van online criminaliteit en preventie van daderschap, en dit gebeurde enkel door respondenten die werkzaam zijn in de incidentafhandeling.

Deze bevindingen staan in groot contrast met de aangegeven, geprioriteerde taken van de basisteams. De meerderheid van de medewerkers is het (helemaal) eens dat de opsporing, nazorg, verstoring, alternatieve interventies en preventie van slachtofferschap en daderschap belangrijke taken van hun basisteam zijn. De opsporing en nazorg aan slachtoffers vinden de meeste respondenten belangrijk. Preventie van slachtofferschap staat daarbij op de laatste plaats. Er zijn enkelingen die deze taken (helemaal) geen belangrijk taak vinden voor hun basisteam.

**Deelvraag 3: Wat kan er middels interventies worden gedaan om de lokale aanpak van online criminaliteit te intensiveren (of hierop voor te bereiden), en op welke wijze kan dat effectief?**

In de laatste jaren hebben basisteams van de politie zich ontwikkeld op het gebied van online criminaliteit. Verschillende interventies die bewust of onbewust zijn toegepast om online criminaliteit beter door medewerkers van de basisteams aan te laten pakken, worden als positief ervaren. Vooral het werken aan een ‘echte’ online criminaliteitszaak, idealiter samen met een meer ervaren collega, ook wel *learning by doing* genoemd, is volgens de medewerkers zelf een positieve manier van kennisontwikkeling. Andere positieve voorbeelden van interventies die door hen werden genoemd waren triage en de digitale hulplijn. Het – overigens veel toegepaste – delen van informatie via e-mail of het volgen van een e-learning over de aanpak van online criminaliteit, worden door de medewerkers *niet* als effectieve methoden voor de ontwikkeling van kennis en vaardigheden gezien.

Er is behoefte aan het vergroten van de motivatie om online criminaliteit aan te pakken en kennis en vaardigheden om dit beter aan te kunnen pakken. Geïnterviewden vinden het belangrijk om verschillende vormen van online criminaliteit te kennen en zowel online als offline signalen daarvan te herkennen. Ze vinden dat ze digitale sporen moeten herkennen en interpreteren om opsporingsindicaties vast te stellen voor collega's van het basisteam of andere opsporingsteams binnen de politie. Er wordt ook gewezen op het belang van het melden van online criminaliteit (aangiften) om opsporingsindicaties te identificeren. Overkoepelend is het van belang om de juridische kaders die van toepassing zijn op online criminaliteit goed te kennen voor de opsporing en aangiftebehandeling. Tot slot is de juiste omgang met slachtoffers van belang in het kader van dienstverlening en preventie van herhaald slachtofferschap. Deze behoeften komen grotendeels overeen met eerder vastgestelde normen van kennis en vaardigheden voor politiemensen in basisteams (Jansen et al., 2020; POR, 2020).

Samenvattend erkennen politiemensen de ernst van online criminaliteit en het belang van een lokale aanpak. Tegelijkertijd ontbreekt het hen aan motivatie en de benodigde kennis en vaardigheden (naast een beperkte capaciteit). Tot op heden zijn nauwelijks trainingen of opleidingen gevolgd en worden dergelijke ontwikkelmogelijkheden bovendien weinig aangeboden. De medewerkers van de basisteams zijn daarmee grotendeels op zichzelf aangewezen om zich deze nieuw materie eigen te maken en dit is lastig gezien de beperkte tijd en de soms aanwezige lage motivatie om online criminaliteit aan te pakken.

Om de aanpak van online criminaliteit op lokaal niveau te versterken, is het volgens de vragenlijstrespondenten cruciaal dat interventies worden ontwikkeld die plaatsvinden in een fysieke setting en ondersteund worden door een goed leeraanbod en de juiste hulpmiddelen, zoals laptops en telefoons. Leren van ervaren politiecollega's binnen en buiten het basisteam (zoals team Cybercrime, ECDO et cetera) speelt volgens de vragenlijstrespondenten hierin een belangrijke rol. Uit de vragenlijstresultaten blijkt dat vrijwel alle respondenten aangeven hulp te durven vragen over online criminaliteit. Specifiek, de basisteamrechercheurs geven over het algemeen aan te weten bij wie ze

terecht kunnen met vragen over online criminaliteit. Ook leidinggevend scoren relatief hoog op het vermogen om intern samen te werken binnen dit thema.<sup>31</sup> Dit biedt een waardevol uitgangspunt om onderlinge kennisuitwisseling en samenwerking binnen en buiten het basisteam te stimuleren.

Op basis van het Toewijzingskader (2023) en op basis van wat vragenlijstrespondenten als belangrijk beschouwden, kunnen de taken van basisteams op het gebied van online criminaliteit worden herzien. Er blijkt immers een groot verschil te zijn tussen de prioriteiten die vragenlijstrespondenten aangeven en de taken die daadwerkelijk door hen worden uitgevoerd. Daarom is het zinvol om bij interventies rekening te houden met de prioriteiten van het basisteam, zowel formeel vastgelegde prioriteiten als gepercipieerde prioriteiten per afdeling. Dit draagt bij aan een praktijkgerichte, realistische aanpak die gedragen wordt door de medewerkers.

Voor medewerkers I&S en de incidentafhandeling ligt de nadruk in de praktijk op nazorg aan slachtoffers van online criminaliteit. Om slachtoffers beter te ondersteunen, is het belangrijk dat medewerkers meer kennis opdoen over slachtofferadvies. Dit omvat onder andere: welke vervolgstappen kunnen slachtoffers nemen, welke instanties hen kunnen helpen en hoe zij digitale sporen kunnen veiligstellen. Daarnaast is een goede begeleiding cruciaal om slachtoffers van online criminaliteit de juiste nazorg te bieden. Momenteel weten niet alle politiemensen naar welke organisaties zij slachtoffers kunnen doorverwijzen, terwijl een integrale samenwerking tussen deze partijen de nazorg aanzienlijk zou kunnen verbeteren.

De incidentafhandeling is de enige groep die aangeeft in te zetten op zowel preventie, verstoring, alternatieve interventies, nazorg als opsporing van online criminaliteit. Het is zelfs de enige groep die iets heeft gedaan aan het verstoren en preventie van daderchap van online criminaliteit, ook al betrof dit een enkeling. Als we kijken naar de gerapporteerde kennis en vaardigheden, dan lijken de meeste medewerkers in deze groep een bepaalde basiskennis te hebben en is er onder hen ook behoefte aan verdere ontwikkeling. Zo geeft meer dan de helft aan goed online te kunnen communiceren met burgers. Het laagst gerapporteerde kennisniveau betreft het juridische kader voor het opsporen van online criminaliteit en de taken die op een plaats delict kunnen worden uitgevoerd. Omdat deze functiegroep op verschillende manieren online criminaliteit kan aanpakken (van preventie tot verstoring en opsporing), is het voor een effectieve interventie belangrijk om alle kennis en vaardigheden verder te ontwikkelen en hiermee rekening te houden met individuele behoeften binnen een basisteam.

De basisteamrecherche richt zich primair op de opsporing, die grotendeels afhankelijk is van de opsporingsindicaties die in de aangiften worden opgenomen. Hierdoor zijn eerdere verbeterpunten, zoals het correct opnemen van aangiften en het veiligstellen van digitale sporen door collega's van binnen en buiten het basisteam, van directe invloed op hun werk. Uit de vragenlijstdata blijkt dat rechercheurs op basisteams goed op de hoogte zijn van welke collega's of afdelingen zij moeten benaderen bij vragen over online criminaliteit. Ook beschikken zij over redelijke kennis met betrekking tot het

31 Bij de andere functiegroepen was een specifiek item over interne samenwerking niet opgenomen.

opstellen van vorderingen om online gegevens van verdachten te achterhalen. Toch blijven er uitdagingen bestaan op het gebied van interceptiemogelijkheden en het correct analyseren en duiden van de onderzoeksbevindingen. Voor een effectieve interventie is het daarom belangrijk om te benadrukken wat al goed gaat – zoals het weten bij wie men met vragen terecht kan – en dit als basis te gebruiken om verdere expertise te ontwikkelen.

Binnen de groep leidinggevendenden lijkt de (gepercipieerde) betrokkenheid bij online criminaliteit nog opvallend beperkt. Ongeveer een op de acht respondenten geeft aan door hun leidinggevendenden te worden gemotiveerd om zich met dit thema bezig te houden. Slechts een derde van de bevroagde leidinggevendenden vindt dat zij voldoende basiskennis hebben om hun team effectief aan te sturen, terwijl minder dan een derde aangeeft daadwerkelijk richting te kunnen geven aan de aanpak van online criminaliteit. Dit wijst op een duidelijke uitdaging onder leidinggevendenden van de basisteams: zij dienen meer kennis te ontwikkelen om hun teams beter te kunnen ondersteunen en aansturen in de aanpak van online criminaliteit. Daarbij is het noodzakelijk om nader te onderzoeken welke specifieke kennis hiervoor ontbreekt, hoe deze effectief kan worden overgebracht en welke ondersteuningsbehoefte zij mogelijk hebben in het begeleiden van de lokale, digitale transitie.

#### **Deelvraag 4: Hoe wordt de ontwikkelde interventie door deelnemers ervaren en wat zijn de effecten ervan in de praktijk?**

Bij basisteam Postenveld zijn twee interventies uitgevoerd, een HINT-oefening en een kennislunch. De evaluatie van beide interventies laat zien dat deelnemers deze overwegend positief hebben ervaren, met name vanwege de combinatie van praktische toepasbaarheid en laagdrempelige kennisoverdracht. De oefening werd gewaardeerd om de actieve werkvorm en het oefenen met realistische casuïstiek, wat bijdroeg aan een beter begrip van online criminaliteit en de herkenning van digitale sporen. De kennislunch bleek toegankelijk en activerend, mede door het spelelement en de informele setting, waardoor deelname werd gestimuleerd en de drempel om met het onderwerp bezig te zijn werd verlaagd.

De impact van de interventies ligt vooral op het vergroten van bewustwording en kennis onder medewerkers van het basisteam. Deelnemers geven na de interventies aan beter zicht te hebben op vormen van online criminaliteit en het belang van zorgvuldig handelen, terwijl de kennislunch bij hen de basiskennis versterkte en hun interesse voor de aanpak van online criminaliteit aanwakkerde. Tegelijkertijd blijft de impact van de interventies op zelfvertrouwen (houding) en zelfstandig handelen (gedrag) gematigd. Een deel van de deelnemers voelt zich beter toegerust, maar een aanzienlijke groep blijft terughoudend, met name door onzekerheid over de praktische toepassing in *reallife* zaken en bevoegdheden.

Daarnaast maken de resultaten duidelijk dat leren effectief lijkt te zijn wanneer het praktijkgericht en herhaald wordt aangeboden. De oefening wordt als waardevoller ervaren dan passieve leervormen, terwijl de kennislunch juist een goede aanvulling vormt voor bewustwording en basiskennis. Beide interventies onderstrepen echter dat

een eenmalige investering onvoldoende is voor duurzame gedragsverandering ten aanzien van de aanpak van online criminaliteit in het basisteam. Er blijft, althans bij diverse deelnemers, behoefte aan verdieping, herhaling en betere aansluiting op taakspecifieke werkzaamheden.

Tot slot tonen de interventies aan dat ontwikkeling op het thema online criminaliteit samenhangt met organisatorische randvoorwaarden. Ervaren tekorten in tijd, capaciteit, samenwerking en duidelijkheid over rollen vormen voor de deelnemers belemmeringen voor de vertaalslag van de nieuwe inzichten naar de dagelijkse praktijk. Hoewel de interventies bijdragen aan een positieve beweging, is structurele borging in het basisteam noodzakelijk om het opgebouwde bewustzijn en de toegenomen kennis daadwerkelijk om te zetten in effectief handelen.

### **Deelvraag 5: Hoe kan de aanpak van online criminaliteit door medewerkers van de basisteams worden geïntensiveerd?**

De geïnterviewde experts benadrukken in de interviews over de intensivering van taken van de basisteams in de aanpak van online criminaliteit de noodzaak van landelijk beleid om de vrijblijvendheid in de aanpak van online criminaliteit door basisteams te doorbreken. Momenteel ontbreekt een heldere vertaling van landelijke doelstellingen naar lokaal niveau volgens hen. Dit zorgt voor een disbalans in de inzet van basisteams in de aanpak van traditionele en online criminaliteit. Ondanks bezuinigingen en capaciteitstekorten moet de politie volgens deze respondenten prioriteit geven aan online criminaliteit, gelet op het hoog aantal slachtoffers en de impact. Basisteams hebben hiertoe op dit moment echter onvoldoende kennis en vaardigheden en hebben behoefte aan ondersteuning van specialisten, ruimte om te leren, en landelijke samenwerking en investeringen in data.

Voor een eventuele opschaling van de aanpak van online criminaliteit door medewerkers van de basisteams zijn door de onderzoekers – en met aanscherping van de respondenten – principes geformuleerd die als volgt kunnen worden samengevat:

- allereerst moet de urgentie van online criminaliteit voelbaar zijn, bijvoorbeeld via lokale casuïstiek en data, te beginnen bij het vergroten van de betrokkenheid van de lokaal leidinggevendenden bij de aanpak van online criminaliteit;
- daarnaast kan de lage motivatie om online criminaliteit aan te pakken worden verhoogd door succesverhalen en *learning by doing* in groepsverband, met ondersteuning van experts; en
- ten slotte, moet de intensivering maatwerk zijn, afgestemd op capaciteit en affiniteit, met focus op eenvoudige vormen van online criminaliteit.

Een heldere leerstrategie (fysiek en groepsgewijs) en sterk leiderschap van teamchefs en het lokale kader van leidinggevendenden zijn volgens de respondenten essentieel bij deze verandering. Zij moeten prioriteren, sturen, weerstand begeleiden en succes vieren. Daartoe moet echter eerst hun kennis over en betrokkenheid bij de aanpak van online criminaliteit worden vergroot. Cultuurverandering is in de beleving van de respondenten in de verandering naar meer taken in de aanpak van online criminaliteit

door de basisteams niet altijd nodig. In plaats daarvan kunnen *early adopters* hun collega's meenemen in een geleidelijke opbouw van deze taken. Volgens de respondenten is het cruciaal dat de aanpak van online criminaliteit door de basisteams verplicht wordt gesteld. Dit raakt de politieorganisatie in de volle breedte en dit vraagt om een duidelijke verschuiving in leiderschap en sturing.

## 7.2 Reflectie op de rol van de onderzoekers

De rol van de onderzoekers speelt in dit onderzoek een wat complexere rol. Voor de literatuurstudie (hoofdstuk 1), de interviews met de medewerkers van Lichtblauwveen en Postenveld (hoofdstuk 3) en de vragenlijsten onder medewerkers van de basisteams in Nederland (hoofdstuk 4) geldt dat er sprake is van een klassieke, meer beschouwende rol van de onderzoekers. Voor het onderdeel waarin werd overgegaan tot de ontwikkeling van interventies (hoofdstuk 5) was de eerste auteur niet alleen betrokken als onderzoeker, maar ook als praktijkgerichte veranderaar binnen basisteam Postenveld. In Lichtblauwveen was deze rol in het projectplan voorgenomen voor twee andere auteurs, maar is deze niet van de grond gekomen. De actieve betrokkenheid van de onderzoeker in Postenveld droeg bij aan de vooruitgang van het basisteam op het thema, maar roept vragen op over de onafhankelijkheid van het onderzoek en de mate waarin de onderzoeker het proces heeft beïnvloed. Hoewel de voortgang binnen het basisteam zonder deze medewerking waarschijnlijk beperkter zou zijn geweest, benadrukt deze situatie het belang van duidelijke professionele grenzen en heldere rolverdeling, zoals deze eerder rond actieonderzoek zijn opgeworpen (Spithoven & Walberg, 2025). Voor toekomstig onderzoek is het daarom essentieel om vooraf duidelijke afspraken te maken over de rol van de onderzoeker en kritisch te reflecteren op de eigen invloed op de onderzochte praktijk.

Voor het onderdeel waarin interviews met interne en externe experts zijn gevoerd over een mogelijke opschaling van taken van basisteams in de aanpak van online criminaliteit (hoofdstuk 6), hebben de onderzoekers vooraf een eerste, inhoudelijke aanzet voor de principes voor opschaling geformuleerd op basis van de bevindingen uit de eerdere onderzoeksfasen. Deze vorm van cocreatie droeg bij aan de inhoudelijke aansluiting op de eerdere onderzoeksbevinding. Tegelijkertijd bracht deze werkwijze het risico met zich mee dat onderzoekers mogelijk minder kritisch zouden reflecteren op de uitkomsten van deze onderzoeksfase. Om dit risico te beperken, zijn de interviewverslagen onafhankelijk gecodeerd en geïnterpreteerd door een andere onderzoeker. Vervolgens zijn deze analyses gecontroleerd door een tweede onderzoeker. Daarna hebben de onderzoekers die de principes opstelden en de interviews met de experts afnamen de resultaten beoordeeld en waar nodig aangescherpt. Op deze wijze is getracht de betrouwbaarheid van de interpretaties te versterken.

### 7.3 Beperkingen

Dit onderzoek biedt waardevolle inzichten en praktische handvatten voor de lokale aanpak van online criminaliteit door basisteams, maar de resultaten vragen – in het verlengde van onze voorgaande reflectie op de rol van de onderzoekers – om een genuanceerde interpretatie door diverse methodologische beperkingen.

Allereerst kan *interviewerbias* zijn ontstaan doordat zes verschillende onderzoekers semigestructureerde interviews afnamen, met ruimte voor follow-upvragen. Hoewel de coderingen redelijk gelijkmatig over de basisteams zijn verdeeld, zijn er verschillen zichtbaar, zoals een hoger aantal coderingen voor het thema ‘behoeften aanpak online criminaliteit’ in Postenveld dan in Lichtblauwveen.

Daarnaast speelt *intercoderbetrouwbaarheid* een rol: twee onderzoekers codeerden de interviews, wat tot kleine verschillen in interpretatie kan leiden. Hoewel de codes en citaten met elkaar zijn vergeleken en voldoende overeenstemming toonden, ontbrak een externe intercoder-betrouwbaarheidsanalyse. Ook de variatie in interviewers en de mate van follow-upvragen kunnen de context en het aantal codes per transcriptie beïnvloeden.

De mogelijke *sociale wenselijkheidsbias* is aangepakt door anonimiteit te garanderen en deelnemers te benadrukken dat er geen goede of foute antwoorden zijn. Toch blijft het risico bestaan dat respondenten antwoorden gaven die maatschappelijk wenselijk waren.

Een andere beperking is *zelfrapportagebias*: de resultaten zijn gebaseerd op wat respondenten zelf aangeven over hun kennis en vaardigheden, zonder objectieve meting. Dit kan leiden tot een overschatting van hun competenties.

Een mogelijke *selectiebias* kan optreden doordat vooral medewerkers met affiniteit voor digitalisering deelnamen, waardoor andere perspectieven ondervertegenwoordigd kunnen zijn. Dit kan de representativiteit van de uitkomsten beperken en leiden tot een enigszins eenzijdig beeld van digitalisering binnen de politieorganisatie. Hoewel de sample niet sterk afwijkt van de populatie, is geen non-respons onderzoek uitgevoerd om dit nader te verifiëren. Ook sampling bias speelt een rol: verschillen in steekproefgroottes tussen functiegroepen beïnvloeden de betrouwbaarheid van de statistische analyses, ondanks het toepassen van een Bootstrap-analyse.

Het *ontbreken van een systematische effectmeting* (zoals een voormeting) maakt het moeilijk om empirisch vast te stellen of de interventies daadwerkelijk leidden tot een toename in kennis en vaardigheden. Wel bieden observaties, focusgroepen en een online vragenlijst inzicht in de werkzame principes.

Ten slotte hebben wij onze respondenten niet uitgevraagd op hun kennis en vaardigheden ten aanzien van AI en de door hen veronderstelde rol van AI in online criminaliteit, omdat onze dataverzameling plaatsvond voordat dit zijn algemene, grootschalige intrede in de samenleving deed. Ondanks deze beperkingen leveren de bevindingen waardevolle inzichten op in de perspectieven van basisteammedewerkers en hun behoeften bij de aanpak van online criminaliteit. Wel kan de afhankelijkheid van de on-

derzoeker in de praktijk leiden tot een ‘gat’ op dit thema zodra de onderzoeker het team verlaat.

## 7.4 Aanbevelingen voor de praktijk

Op basis van onze bevindingen doen wij de volgende aanbevelingen aan de praktijk ten aanzien van de noodzakelijke verandering waarbij medewerkers van basisteams eenvoudige zaken van online criminaliteit gaan aanpakken:

1. Maak met **landelijk beleid** de aanpak van eenvoudige online criminaliteitszaken (met opsporingsindicatie en een lage politieke gevoeligheid) door basisteams minder vrijblijvend. Kader deze taak als een thematische, algemene politietaak (net als de aanpak van georganiseerde misdaad of ondermijning) in plaats van een specialistische taak. Geef daarbij – ondanks bezuinigingen en capaciteitstekorten – met duidelijke keuzes prioriteit aan online criminaliteit en vertaal landelijke doelstellingen ten aanzien van de lokale aanpak van online criminaliteit middels duidelijke beleidskeuzes op het lokale niveau (Black et al., 2019; Bossler & Holt, 2012; Brunner, 2020; Burns et al., 2004; Forouzan et al., 2018; Hadlington et al., 2018; Holt et al., 2010; Holt & Bossler, 2012; Hull et al., 2018; Kort & Spithoven, 2021; 2022; Lee et al., 2025; Leukfeldt et al., 2020; McNealey et al., 2025; Politie, 2023; Shandler & Gomez, 2023; Spithoven et al., 2022; Spithoven & Leukfeldt, 2023; Stambaugh et al., 2001; Terpstra et al., 2021; Terpstra, 2024). De empirische data in dit onderzoek laten zien dat het aanpakken van online criminaliteit binnen basisteams nog sterk afhankelijk is van individuele affiniteit en expertise, en dat ontwikkeling hierin op lokaal niveau nog ondermaats wordt gestimuleerd vanuit de leiding. De betrokkenheid van de lokaal leidinggevenden bij de aanpak van online criminaliteit moet duidelijk worden vergroot. Het is belangrijk om in de algehele veranderstrategie de nadruk te leggen op ‘verleiding in plaats van dwingen’ en effectief om te gaan met weerstand vanuit politiemedewerkers en de visie en urgentie op het gebied van de intensivering van de aanpak van online criminaliteit heldere wijze top-down naar de basisteams te communiceren.
2. **Vergroot de betrokkenheid onder de leidinggevenden van de basisteams bij de aanpak van online criminaliteit.** Ongeveer een op de acht respondenten uit de landelijke vragenlijst onder medewerkers van de basisteams geeft aan door hun leidinggevenden te worden gemotiveerd om zich met dit thema bezig te houden. Laat **leidinggevenden binnen de basisteams** prioriteit geven aan aanpak van online criminaliteit geven, **sturen op verandering en weerstand begeleiden** en geef hen waar nodig daarbij extra ondersteuning. Ook is het nodig dat er ruimte in roosters wordt gemaakt om zich tijdens werktijd *on the job* de nieuwe kennis en vaardigheden rondom de aanpak van online criminaliteit eigen te maken. Het is van belang dat teamchefs en het kader informele processen in het team herkennen en hierop inspelen. Eventuele weerstand in het basisteam moet collectief worden aangepakt. Daarbij kunnen teamchefs samenwerken met OPCO's, OSA's en experts

van buiten het basisteam om deze verandering te ondersteunen (Black et al., 2019; Bossler & Holt, 2012; Bossler et al., 2020; Cockcroft et al., 2021; Hitchcock et al., 2017; Hinduja, 2004; Holt & Bossler, 2012; Johnson et al., 2020; Lee et al., 2025; Stambaugh et al. 2001; Wall, 2007; Wilson et al., 2022).

3. Maak de **urgentie voor de aanpak van online criminaliteit zichtbaar en voelbaar** voor alle medewerkers van de basisteams, door lokale casuïstiek te gebruiken om de impact te illustreren. Gebruik bijvoorbeeld verhalen van slachtoffers en verhalen over daders uit het eigen werkgebied. Ook kan naast deze verhalen gebruik worden gemaakt van lokale cijfers over aantallen daders, slachtoffers en schadebedragen. Naast politiecijfers is het ook raadzaam om met lokale veiligheidspartners informatie uit te wisselen. Denk hierbij bijvoorbeeld aan gemeenten, RIEC's, en zorg- en veiligheidshuizen. Sta daarbij ook stil bij de vele facetten van de impact van slachtofferschap. Hierbij kan worden ingespeeld op het rechtvaardigheidsgevoel van medewerkers als motivatie om online criminaliteit aan te pakken en slachtoffers te helpen.
4. **Verhelder de taken rondom de aanpak van online criminaliteit door medewerkers van de basisteams**, die vooral gaan om het bewustzijn van de aard en omvang van online criminaliteit en het kennen, weten te herkennen en benoemen van de strafbaarstelling van specifieke delicten. Daarnaast moet men weten hoe te handelen op een plaats delict en met online sporen, adequaat kunnen omgaan met aangedragen informatie en een opsporingsonderzoek naar online criminaliteit kunnen starten op basis van de daarvoor geldende eisen. In sommige eenheden wordt de 'incidentafhandeling' ook belast met het opnemen van meldingen en aangiften op het bureau, maar deze taak ligt in beginsel bij medewerkers van I&S (Boekhoorn, 2020; Huisman et al., 2016; Jansen et al., 2020; Kort & Spithoven, 2021; Leukfeldt et al., 2012; 2013; POR, 2020; Ruiter et al., 2023; Schiks et al., 2022; Toutenhoofd-Visser et al., 2009; Zuurveen & Stol, 2020). Meer concreet zijn de volgende contouren van de lokale, digitale politietaak in dit onderzoek houdbaar gebleken (Kort & Spithoven, 2022, p. 115):

Tabel 7.1 Contouren van de lokale, digitale politietaak (Kort &amp; Spithoven, 2022, p. 115).

| I&S                                              | Wijkwerk                                                                                                                               | Interventie                                                                                                                        | Veelvoor-<br>komende<br>criminaliteit                                       | Ondersteunen opsporing                                                                                                                                                                 |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Signaleren van lokaal slachtoffer- en daderschap | Signaleren van lokaal actieve daders, dadergroepen en criminele netwerken. Lokaal agenderen en tot integrale, preventieve aanpak komen | Samenwerken met partnerorganisaties bij preventieve activiteiten. Gezamenlijk voeren van stopgesprekken met <i>first offenders</i> | Opsporen van lokaal actieve daders en eenvoudig te onderkennen dadergroepen | Andere organisatieonderdelen ondersteunen met advies en lokale kennis ten aanzien van lokale daders, dadergroepen of criminele netwerken en ondersteunen bij het aanhouden en verhoren |

De internationale literatuur over de lokale aanpak van online criminaliteit legt daarbij meer de nadruk op de rol van *first responder* voor slachtoffers door de incidentafhandeling. Hierbij ligt de nadruk op de volgende taken: slachtoffers opvangen, slachtoffers van advies voorzien, slachtoffers doorverwijzen naar andere hulpverlenende instanties, aangiftes opnemen en digitaal bewijs veiligstellen (Black et al., 2018; Bossler & Holt, 2012; Chudasama et al., 2020; Cross, 2018; 2020; Cross & Blackshaw, 2015; Cross et al., 2021; Forouzan et al., 2018; Hadlington et al., 2021; Holt & Bossler, 2012; Lee et al., 2025; Schreuders et al., 2020; Wilson et al., 2022). Het uitvoeren van opsporing ligt volgens de internationale literatuur doorgaans omwille van de complexiteit buiten de lokale politietaak (Black et al., 2019; Broadhurst, 2006; Cockcroft et al., 2021; Cross et al., 2021; Forouzan et al., 2018; Hadlington et al., 2021; Hitchcock et al., 2017; Wall, 2007). In Nederland geldt dat opsporing van eenvoudige online criminaliteitszaken ligt bij medewerkers van VVC. In de eenheid Oost-Nederland worden iets grotere en complexere zaken echter toebedeeld aan een eenheid-brede HUB waarin rondom opsporing nauw wordt samengewerkt met zaaksofficieren van het Openbaar Ministerie. Hierbij moet binnen de politie een keuze over deze inrichtingsvraag rondom opsporing worden gemaakt.

5. Zet in op een verandering waarbij lokale politiemedewerkers **steeds meer kennis, vaardigheden en eigenaarschap voor de aanpak van online criminaliteit krijgen**. Daarin schieten lokale politieteam al langere tijd tekort (Black et al., 2019; Boekhoorn, 2020; Bossler & Holt, 2012; Broadhurst, 2006; Chudasama et al., 2020; Cockcroft et al., 2021; Cross et al., 2021; Forouzan et al., 2018; Hadlington et al., 2021; Hitchcock et al., 2017; Holt & Bossler, 2012; Huisman et al., 2016; Jansen et al., 2020; Johnson et al., 2020; Kort & Spithoven, 2021; Lee et al., 2025; Leukfeldt et al., 2012; McNealey et al., 2025; Nowacki & Willits, 2020; POR, 2020; Schiks et al., 2022; Stol et al., 1999; 2013; Wall, 2007). Het tekort aan kennis en vaardigheden is terug te zien in de nationale vragenlijstdata onder medewerkers van basisteams, waarin zichtbaar wordt dat de mate van kennis en kunde sterk varieert per functiegroep en per onderdeel van de aanpak van online criminaliteit. Hoewel de meerderheid van de respondenten aangeeft in algemene zin over enige tot voldoende

kennis en vaardigheden te beschikken, blijkt deze vooral te liggen op basisaspecten, zoals het durven vragen om hulp en het weten waar binnen de organisatie informatie kan worden verkregen. Tegelijkertijd blijven meer inhoudelijke, digitale kennis en vaardigheden achter, met name op het gebied van het herkennen en veiligstellen van digitale sporen, het verzamelen van online informatie en het toepassen van juridische bevoegdheden. Deze resultaten wijzen erop dat basiskennis over online criminaliteitsvormen wel aanwezig is, maar vaak nog onvoldoende is doorontwikkeld richting operationele handelingsbekwaamheid voor de aanpak van deze vormen van criminaliteit. Dit onderstreept de noodzaak van structurele opleiding en training om de aanwezige basiskennis te versterken naar handelingsbekwaamheid. Daarmee wordt de algemeen heersende insteek van *learning by doing* in de aanpak van online criminaliteit wat ons betreft idealiter gefundeerd door een meer gestructureerde en meer onderbouwde aanpak.

6. Zet in op **ondersteuning van de basisteams door specialisten** (bijvoorbeeld digi-coaches, cybercrimeteams) en geef basisteams de ruimte om zich nieuwe kennis en vaardigheden eigen te maken en in de aanpak van online criminaliteit routine te ontwikkelen (Black et al., 2019; Button et al., 2015; Cross et al., 2021; Cockcroft et al., 2021; Forouzan et al., 2018; Hadlington et al., 2021; McNealey et al., 2025; Martin et al., 2018; Nowacki & Willits, 2020; Wall, 2007). Leren van specialisten met vakinhoudelijke expertise op het gebied van de aanpak van online criminaliteit wordt in zowel de interviews als de vragenlijst door respondenten als wenselijk en waardevol beschouwd. Daarnaast bleek uit de oefeningen tijdens het ontwerponderzoek in basisteam Postenveld dat de prestaties zichtbaar verbeterden wanneer een digitaal specialist aanwezig was. De deelnemers kregen gerichte feedback tijdens en na de oefening waardoor zij beter inzicht kregen in digitale opsporingsmogelijkheden, het veiligstellen van sporen en het gebruik van hulpmiddelen (zoals de digi-koffer). De feedback droeg bij aan meer bewust en doelgericht handelen. Deze feedback bestond onder andere uit het verstrekken van informatie, stellen van vragen, maar ook door aan te geven wat goed gaat en wat er eventueel gemist is. Dit is een voorbeeld waarbij het inbedden van samenwerking tussen specialisten en generalisten binnen het basisteam kan bijdragen aan de ontwikkeling van de handelingsbekwaamheid op het gebied van de aanpak van online criminaliteit.
7. **Zet in op de leerstrategie van *learning by doing*** via verplichte, offline bijeenkomsten waar groepsgewijs wordt geleerd op basis van concrete, recente en lokale casuïstiek van slachtoffers en daders van online criminaliteit. Houd daarbij rekening met functie-specifieke kennis (bijvoorbeeld verschil tussen I&S, recherche, incidentafhandeling en leiding). Daarbij moet de aanpak van online criminaliteit eveneens onderdeel worden van de basis politieopleidingen (Holt & Bossler, 2012; Stol et al., 2013; Hitchcock et al., 2017; Jahankhani & McCarthy, 2018; Forouzan et al., 2018; Chudasama et al., 2020; Cockcroft et al., 2021; Hadlington et al., 2021). Learning by doing helpt **de lage motivatie voor de aanpak van online criminali-**

- teit verhogen** doordat het onbekende gezamenlijk concreet en beheersbaar wordt gemaakt en vertrouwen groeit door praktijkervaring. Dit kan, naast zelf actief aan de slag gaan, bijvoorbeeld ook door succesverhalen over de aanpak van online criminaliteit binnen het eigen basisteam en andere basisteams met elkaar te delen (Ruiter et al., 2023; Spithoven & Leukfeldt, 2023).
8. **Bied maatwerk voor deze verandering**, afgestemd op capaciteit (fte's) en affiniteit van medewerkers. Formeer een groep *early adopters* binnen de basisteams die hun collega's meenemen in de noodzaak en werkwijze van de lokale aanpak van online criminaliteit. Daarbij kunnen experts als digi-coaches en collega's van het cybercrimeteam ondersteunen. Leidinggevend en moeten verleiden in plaats van dwingen, en effectief omgaan met weerstand. Zorg daarbij dat het tempo van de verandering gebalanceerd is. Er dient in elk geval *geen* radicale omslag plaats te vinden – of door leidinggevend worden geforceerd –, maar er dient een geleidelijke verandering plaats te vinden. Medewerkers van basisteams moeten immers niet worden overspoeld met nieuwe taken, maar men moet hen hier stapsgewijs en in groepsverband aan laten wennen (Terpstra et al., 2021; Van Steden et al., 2025).

## 7.5 Aanbevelingen voor vervolgonderzoek

Naast onze aanbevelingen voor de praktijk zien wij verschillende mogelijkheden voor vervolgonderzoek naar de verandering waarbij medewerkers van de basisteams van de politie meer taken gaan vervullen in de aanpak van online criminaliteit. Allereerst I) zou er onderzoek uitgevoerd kunnen worden naar de rol van leidinggevend (teamchefs, OSA's, OPCO's et cetera) en experts (digi-coaches, cybercrimeteam et cetera) in de aanpak van deze verandering en wat daarin werkende en belemmerende factoren zijn. Daarnaast II) zou onderzoek uitgevoerd kunnen worden naar de landelijke verandering over de tijd waarbij longitudinaal wordt gevolgd hoe de basisteams zich in de aanpak van online criminaliteit ontwikkelen en wat daarin eveneens helpende en beperkende factoren zijn.

Ook zien wij III) een noodzaak om vanuit de landelijke politieorganisatie gestructureerd te werken aan ontwerponderzoek, waarin de lokale aanpak van online criminaliteit en de verandering van medewerkers om deze aanpak te omarmen en eigen te maken, wordt ondersteund en waarbij *best practices* landelijk worden gedeeld om de basisteams in deze verandering te ondersteunen. Daarbij zou IV) op basis van onze bevindingen over de beleving en behoefte van basisteammedewerkers middels ontwerponderzoek een gedegen zelftest voor basisteams kunnen worden ontworpen waarbij teamchefs inzichtelijk krijgen waar in de verandering de aandachtspunten zitten en waarbij een *toolbox* met interventies wordt ontwikkeld die passend elke veranderingsfase kunnen worden ingezet. Deze gedachte sluit aan op een intern politieproject genaamd 'DigiKarakters' waarbij teamchefs een 'gespreksstarter' in de vorm van een fy-

sieke waaier krijgen aangereikt die hen helpt om met basisteammedewerkers het gesprek aan te gaan over de omgang met digitale veranderingen.<sup>32</sup>

Ten slotte V) zien wij kansen voor internationaal vergelijkend onderzoek naar het beleid en de aanpak van de implementatie van lokale taken rondom online criminaliteit, omdat politiekorpsen in de hele wereld duidelijk een noodzaak hebben tot een functionele aanpassing op de radicaal veranderde omgeving, waarbij internationaal leren en gezamenlijk daarin optrekken inspiratie en houvast kunnen geven. Daarbij hebben wij als onderzoekers niet de indruk dat er momenteel een politiekorps is dat zich volledig heeft aangepast aan de veranderde criminaliteit. Wel kunnen de strategieën waarmee korpsen wereldwijd deze transitie vormgeven en implementeren, inspiratie bieden voor de Nederlandse politie bij het ontwikkelen en bijstellen van de eigen strategie.

---

32 <https://www.politieacademie.nl/over-ons/nieuws/digitale-vaardigheid-de-noodzaak-groeit-de-ruimte-knelt>.

## 8 **Epiloog: online doorpakken is geen keuze maar een noodzaak!**

Na het afronden van dit onderzoek blijven wij als onderzoekers met een onbehaaglijk gevoel zitten. Wij troffen namelijk een duidelijke spanning tussen de ambities die de politie formuleert ten aanzien van de aanpak van online criminaliteit en de feitelijke praktijk op lokaal niveau (zie tabel 4.8), evenals de percepties en ervaringen van medewerkers in de basisteams. Daarmee lijkt het discours in de strategische top van de Nationale Politie weliswaar te zijn veranderd, maar vertaalt dit zich vooralsnog slechts zeer beperkt naar veranderingen in het operationele handelen binnen de basisteams. Een dergelijke trend is ook zichtbaar in de internationale literatuur (zie ook Black et al., 2019; Cockcroft et al., 2021; Johnson et al., 2020; Terpstra, 2023).

In basisteam Lichtblauwveen is ondanks herhaalde pogingen, vanwege een tekort aan draagvlak op de werkvloer, de beoogde interventieaanpak niet van de grond gekomen. Wij hebben als onderzoekers in dit basisteam de weerstand tegen het aanpakken van online criminaliteit onder medewerkers van basisteams 'aan den lijve ondervonden'. Dit kwam bijvoorbeeld tot uiting in de interviews en de groepsgewijze terugkoppelingen van onze bevindingen. Dat was terugkijkend een intense ervaring: er werd ons in stevige, zij het correcte, communicatie te kennen gegeven dat deze groep medewerkers de aanpak van online criminaliteit pertinent niet als een taak voor zichzelf zag en niet te motiveren was om hierover verder met ons in gesprek te gaan, laat staan om zich in de toekomst taken op dit terrein eigen te maken. Duidelijk werd dat lang niet iedere medewerker van de basisteams vanzelfsprekend mee zal willen gaan in de benodigde transitie.

Ondanks dat er al ruim dertig jaar onderzoek wordt gedaan naar digitalisering en politiewerk (onder anderen Stol, 1996; Stol et al., 1999), zien we nog steeds een vergelijkbaar beeld optreden als in de eerste onderzoeken: de meeste politiemedewerkers in basisteams erkennen weliswaar de impact van de digitalisering op hun werk, maar willen er zelf liever niet mee aan de slag of weigeren dit zelfs categorisch. De weinige medewerkers die deze nieuwe politietaken wel oppakken, moeten vaak vechten tegen de stroom – en soms zelfs tegen de hoon van collega's en leidinggevendenden – om slachtoffers van online criminaliteit te helpen en lokale daders en dadergroepen op te sporen en hun werk te verstoren. Dit duidt op een grote weerstand tegen de digitale transformatie bij een deel van de politiemensen (Black et al., 2019; Cockcroft et al., 2021; Johnson et al., 2020; Terpstra, 2023) en een stevige, remmende impact van de politiecultuur op een noodzakelijke, functionele aanpassing aan het veranderde criminaliteitsbeeld (zie ook Johnson et al., 2020; Spithoven et al., 2026).

Uit ons onderzoek blijkt dat er binnen de basisteams van de politie nog steeds een grote vrijblijvendheid heerst voor individuele medewerkers en basisteams om zich al dan niet met de aanpak van deze nieuwe criminaliteitsvormen bezig te houden (zie ook Spithoven et al., 2026; Terpstra, 2023). In sommige gevallen, zoals in basisteam Lichtblauwveen, komen teams zelfs collectief in verzet als de leiding hen hiertoe aanzet of voornemens is aan te zetten. Dit staat in schril contrast met de boodschappen van de korps- en eenheidsleiding, die nu al geruime tijd benadrukken dat de aanpak van online criminaliteit prioriteit verdient. Er zijn doelstellingen gesteld, er is beleid gemaakt en er zijn verschillende initiatieven gelanceerd, maar de échte lokale transformatie blijft vooralsnog uit.

Medewerkers van de basisteams noemen hiervoor verschillende redenen: ervaren capaciteitsgebrek, weinig affiniteit met digitale zaken en onzekerheid in de uitvoering (zie ook Van Steden et al., 2025). Maar tussen deze verhalen klinkt toch vooral een voorkeur voor traditioneel politiewerk – actie, bloed en spoed. Ook de werving speelt hierbij naar ons beeld een rol: de politie zoekt anno 2026 nog steeds vooral de fysiek en mentaal sterke medewerkers die niet terugdeinzen, maar een stap vooruitzetten voor actie, terwijl de aanpak van online criminaliteit een heel andere aanpak en het nodige zitvlees vereist. Deze zaken kenmerken zich immers door grote hoeveelheden data, complexe vorderingshandelingen en de noodzaak om digitaal bewijsmateriaal veilig te stellen. Dit is wellicht voor velen ‘nieuw’, maar naar ons beeld evengoed ‘echt’ politiewerk. Gelukkig worden in de opsporing werkzame initiatieven opgeschaald, zoals landelijke analyse van losse aangiften om tot bundeling van zaken op het M.O. te komen (Centurion) en op de opsporing en verstoring van online criminaliteit gerichte samenwerkingen tussen politie en Openbaar Ministerie op regionaal niveau (HUB's). Hier moet simpelweg meer capaciteit naartoe. Dat is geen keuze, maar een noodzaak.

Omdat de opsporing bij online criminaliteit doorgaans complexer is geworden en over alle eenheidsgrenzen heen gaat, kan deze beter op een hoger geografisch niveau worden uitgevoerd. Daarmee komen de HUB's voor de aanpak van gedigitaliseerde criminaliteit naast de Cybercrimeteams te staan die zich daarmee vooral op de meer complexere zaken en aanpak van cybercriminaliteit kunnen richten. Deze noodzakelijke verschuivingen in de opsporing maken dat de lokale aanpak van online criminaliteit door de basisteams vooral is gericht op hulpverlening aan slachtoffers: hen voorzien van eerste noodhulp, emotionele en praktische steun, advies om de impact te beperken en herhaling te voorkomen. Dit is wat ons betreft zeker *geen* 'optioneel', laat staan 'minder echt' politiewerk: hulpverlening betreft naast handhaven van de rechtsorde immers een *volwaardige kerntaak van de politie*. En de politie beweegt in de westerse landen al langer van traditionele *'crime fighting'* naar een bredere, publieke dienstverlening (Rowe, 2018; Spithoven et al., 2026).

Sinds 2012 is duidelijk dat jaarlijks tussen de 2 en 2,5 miljoen Nederlanders van vijftien jaar en ouder slachtoffer worden van online criminaliteit (Arends et al., 2025). Onderzoek toont aan dat de impact hiervan vergelijkbaar – of zelfs groter – is dan die van traditionele delicten (Borwell et al., 2021a, b; Borwell, 2025; Jansen & Leukfeldt, 2018; Leukfeldt et al., 2020). En werkelijk iedereen kan slachtoffer van online criminaliteit

worden. De slachtoffers van online criminaliteit verdienen evengoed aandacht, hulp en zorg. En de lokale politie vervult hierin – ook in andere landen – vaak de rol van *first responder* (Bossler & Holt, 2012; Cross, 2020, 2018; Cross et al., 2021; Hadlington et al., 2021; Lee et al., 2025; Schreuders et al., 2020; Spithoven et al., 2026; Wilson et al., 2022).

Ondanks de herhaalde oproepen van de korps- en eenheidsleiding kunnen medewerkers van de basisteams in Nederland er blijkbaar nog steeds voor kiezen om deze nieuwe politietaken naast zich neer te leggen en zich te richten op wat zij als ‘echt politiewerk’ zien (zie ook Terpstra, 2023). Al dan niet met steun van het lokale leiderschap. De politiecultuur en de wijze waarop medewerkers worden geworven en gesocialiseerd, belemmeren zo de hoognodige digitale transformatie. Samenvattend signaleren wij, in lijn met Johnson en collega’s (2020) en Terpstra (2023), dat de functionele aanpassing van de politie op de radicaal veranderde criminaliteit wordt tegengehouden door institutionele en culturele barrières (zie ook Spithoven et al., 2026). Maar als de politie online in de nabije toekomst geen grotere rol van betekenis pakt, dan verliest zij een deel van haar legitimiteit (Bradford et al., 2022). Nagenoeg de helft van de hedendaagse criminaliteit vindt intussen immers online plaats en nagenoeg elk delict heeft een digitale component.

De politie moet daarmee in onze ogen, niet alleen in woorden, maar vooral in daden prioriteit stellen aan de aanpak van online criminaliteit. Dit vergt duidelijke keuzes maken en een noodzakelijke, fundamentele herverdeling van middelen en taken binnen de Nationale Politie. Er is behoefte aan meer personeel met kennis van online criminaliteit: dit zijn niet per se fysiek sterke medewerkers, maar specifiek opgeleide professionals die complexe, digitale puzzels kunnen oplossen. Hoeveel broeken zij in basispolitiezorg hebben versleten, is in onze ogen hierbij volstrekt irrelevant. Zij zouden met open armen moeten worden ontvangen, ook op de basisteams. De criminaliteit is immers fundamenteel veranderd – de politie, teams en de individuele medewerker moeten meebewegen. Dat is geen keuze, maar dat is de politie en de individuele medewerker in onze ogen aan de samenleving – en vooral de slachtoffers van online criminaliteit – *verplicht* (zie ook Terpstra, 2023).

Historisch gezien heeft de politie zich eerder met succes weten aan te passen aan maatschappelijke veranderingen, zoals de toename van mobiliteit en nieuwe communicatiemiddelen. Technologie was hierin vaak zowel oorzaak als oplossing: de techniek leidde tot nieuwe criminaliteit, maar de toepassing van nieuwe techniek hielp bij de aanpak. Met de grootschalige komst van auto’s en de toegenomen criminaliteit waarbij van auto’s gebruik werd gemaakt, paste de politie zich aan, ging zich in dienstauto’s verplaatsen en kreeg zelfs een verkeerspolitie. Ook bij online criminaliteit speelt technologie een dubbelrol, want bij de analyse van digitale sporen wordt intensief gebruik gemaakt van inzichten uit de *data science*. Verandering van de politie en het politiewerk gaat historisch gezien vaak gepaard met weerstand vanaf de werkvloer. Zo verzetten agenten en onderzoekers zich in de jaren twintig van de vorige eeuw tegen de introductie van vingerafdruktechnieken en hielden liever vast aan de bekende werkwijzen (Meershoek, *in press*). Ook wisten dienders bij de eerste meldingen van wonin-

ginbraken waar zij aan werden gekoppeld vaak niet goed hoe op te treden op de plaats delict en om te gaan met de slachtoffers. Maar dit is, net als het afnemen van vingerafdrukken, intussen al jaren gemeengoed in de lokale politiepraktijk.

Hoewel discretionaire bevoegdheid een charme is van het politiewerk, pleiten wij rondom de lokale aanpak van online criminaliteit voor steviger beleid, voorbij de vrijblijvendheid (zie ook Terpstra, 2023). Hiertoe dienen het landelijke en lokale bevoegde gezag de politie ruimte te geven. Want ook het bevoegd gezag moet de oude kaders, gebaseerd op oude criminaliteitsbeelden loslaten en meebewegen met de fundamentele verandering van de criminaliteit. Men moet – ook lokaal – een gelijkwaardig aan wijk en web verbonden politie faciliteren en toejuichen in plaats van willen vasthouden aan mantra's van 'meer blauw op straat'. De criminaliteit vindt, zoals eerder gesteld, anno 2026 voor een belangrijk deel op de digitale snelweg plaats. Daarom zou er naast de vraag om meer blauw op straat ook vanzelfsprekend de vraag om meer blauw online moeten zijn. De politie moet immers daar zijn waar zij nodig is.

De functionele adaptatie van politietaken in de aanpak van online criminaliteit ligt in onze ogen nu vooral bij de politieorganisatie en de individuele medewerker. Hoewel deze verandering ingrijpend is voor het dagelijks werk, geldt dat verder uitstel deze transformatie alleen maar complexer maakt. De digitalisering denderd immer ongeremd voort. Zo is intussen ook artificiële intelligentie, voor iedereen beschikbaar – ook voor criminelen. De politie *moet* meebewegen met wat leeft en speelt in de samenleving. Haar wettelijke taak is om de rechtsorde te handhaven en hulp te bieden. Wat ons betreft, geldt dat dus evengoed online als in de traditionele, offline setting.

De samenleving heeft een fundamenteel andere dienstverlening van de politie nodig. Ook de korpschef en de hoogste leidinggevende van het OM hebben hier al noodsignalen over afgegeven. Een regeringscommissie, zoals in de jaren tachtig, die zij recent opperden (Politie, 2026), is in onze ogen echter *niet* wat nu nodig is: de contouren van een effectieve aanpak van online criminaliteit zijn immers al bekend. De politieorganisatie en individuele medewerkers moeten naar ons beeld nu vooral zelf online de stap naar voren zetten, met steun van experts en de *early adopters* die nu nog vaak opvallend alleen staan in de eigen organisatie. Waarom zou een regeringscommissie de politie naar deze bekende weg moeten wijzen? De tijd van zoeken is wat ons betreft echt voorbij. Deze tijd vraagt om doorpakken en dit kan niet langer wachten. Laat een regeringscommissie te zijner tijd de noodzaak van deze ingezette beweging desnoods verder onderstrepen en inhoudelijk aanscherpen.

De politie en individuele medewerkers hebben hierin wat ons betreft geen keuze: zij moeten vandaag nog beginnen met online doorpakken. Daartoe zullen de lokaal leidinggevendenden als eerste overstag moeten gaan en zich meer met de aanpak van online criminaliteit moeten verbinden. Dit betekent dat ander werk minder prioriteit krijgt. Maar ook dat is niets nieuws: er is bij de politie altijd meer werk dan beschikbare capaciteit. Dat is altijd zo geweest en zal altijd zo zijn. Dit is een kwestie van duidelijke keuzes maken.

*Online doorpakken* begint daarom in onze ogen met heldere prioriteiten en moeilijke keuzes van de korpsleiding, die de eenheidsleiding hier vervolgens op afrekenen: welk

werk doen we minder of zelfs helemaal niet meer? Vervolgens moeten eenheids- en districtsleidingen hun lagere leidinggevende lagen hierin sturen en begeleiden, zonder hen nog enige ruimte voor online doormodderen te geven. In basisteams is vervolgens een mix nodig van duidelijkheid en verleiding: opleidingen, coaching en hulp op maat voor leidinggevers bij een aanpak die weerstand omzet in betrokkenheid. Specialisten en *early adopters* binnen de organisatie kunnen hierin een gidsende rol spelen, mits ze de nodige steun van het lokale leiderschap krijgen, wat zelf de verantwoordelijkheid voor de transitie en omgang met eventuele weerstand op zich neemt. Medewerkers in de basisteams *moeten* wat ons betreft uiteindelijk mee in deze digitale transformatie. Liefst na enige aanmoediging, maar in het uiterste geval met meer hiërarchische dwang. De hiërarchische lijn van de nationale politieorganisatie moet daadwerkelijk gaan sturen.

De politie als geheel en individuele medewerkers staan in onze ogen voor een kruispunt tussen online doorpakken en doormodderen. Onze oproep aan hen is om het voorbeeld van vele collega's te volgen en ook online de stap naar voren te zetten. Het dagelijks leven en werk vindt voor een groot deel online plaats en het is daar allesbehalve veilig. De politie is hard nodig om online criminaliteit een halt toe te roepen en hulp te verlenen aan slachtoffers van online criminaliteit, juist vanuit de kracht van lokale verbinding. Van betekenis zijn waar je nodig bent, dat wil toch elke diender?



## Referenties

Akkermans, M., Derksen, E., Kennis M., Kloosterman, R. & Moons, E. (2024). *Veiligheidsmonitor 2023*. Centraal Bureau voor de Statistiek (CBS).

Arends, J., Derksen, E. & Morren, M., (2025). *Online Veiligheid en Criminaliteit 2024*. Centraal Bureau voor de Statistiek (CBS).

Bærenholdt, J.O., Büscher, M., Scheuer, J.D. & Simonsen, J. (2010). *Perspectives on design research*. In: J. Simonsen, J.O. Bærenholdt, M. Buscher & J.D. Scheuer (Eds.). *Design Research: Synergies from Interdisciplinary Perspectives*. London/New York, Routledge.

Black, A., Lumsden, K. & Hadlington, L. (2019). 'Why don't you block them?' Police officers' constructions of the ideal victim when responding to reports of interpersonal cybercrime. In K. Lumsden & E. Harmer (Eds.), *Online othering: Exploring digital violence and discrimination on the web* (p. 355-378). Springer.

Boekhoorn, P. (2020). *De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging*. Politie & Wetenschap.

Borwell, J. (2025). *Unravelling the impact of cybercrime: Understanding victim experiences and implications for police practice*. Open Universiteit (proefschrift).

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

Borwell, J., Jansen, J. & Stol, W. Ph. (2021b). 'The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory'. *Social Science Computer Review*, 40(1), 933-954. doi: <https://doi.org/10.1177/0894439320983828>.

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

- Bossler, A.M. & Holt, T.J. (2012). 'Patrol officers' perceived role in responding to cyber-crime'. *Policing*, 35, p. 165-181. <https://doi.org/10.1108/13639511211215504>.
- Bossler, A. M., Holt, T. J., Cross, C. & Burruss, G. W. (2020). 'Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness'. *Security Journal*, 33, p. 311-328.
- Bradford, B., Aston, E., O'Neill, M. & Wells, H. (2022). "Virtual policing", trust and legitimacy'. In: J. Terpstra, R. Salet & N.R. Fyfe (Eds.), *The abstract police. Critical reflections on temporary change in police organisations*, p. 213-238.
- Broadhurst, R.G. (2006). 'Developments in the global law enforcement of cyber-crime. *Policing: an International Journal of Police Strategies and Management*', 29(3), p. 408-433.
- Brunner, M. (2020). 'Challenges and opportunities in state and local cybercrime enforcement'. *Journal of National Security Law & Policy*, 10, p. 563-582.
- Bryman, A. (2012). *Social research methods* (4th ed.). Oxford University Press.
- Burns, R.G., Whitworth, K.H., Thompson, C.Y. (2004). 'Assessing law enforcement preparedness to address Internet fraud'. *Journal of Criminal Justice*, 32(5), p. 477-493. [doi.org/10.1016/j.jcrimjus.2004.06.008](https://doi.org/10.1016/j.jcrimjus.2004.06.008)
- Burruss, G. W., Howell, C. J., Bossler, A. M. & Holt, T. J. (2020). 'Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class analysis'. *Policing: An International Journal*, 43(1), p. 105-119. <https://doi.org/10.1108/PIJPSM-08-2019-0142>.
- Button, M. (2021). 'Hiding behind the veil of action fraud: The police response to economic crime in England and Wales and evaluating the case for regionalization or a national economic crime agency'. *Policing: A Journal of Policy and Practice*, 15(3), p. 1758-1772. <https://doi.org/10.1093/police/paab022>.
- Button, M., Blackburn, D. & Tunley, M. (2015). "The not so thin blue line after all?" investigative resources dedicated to fighting fraud/economic crime in the United Kingdom'. *Policing: A Journal of Policy and Practice*, 9(2), p. 129-142. <https://doi.org/10.1093/police/pau037>.
- Chudasama, D., Patel, D., Shah, A. & Shaikh, N. (2020). 'Research on Cybercrime and its Policing'. *American Journal of Computer Science and Engineering Survey*, 8(3), p. 14.

---

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z. C. & Trevorrow, P. (2021). 'Police cybercrime training: Perceptions, pedagogy, and policy'. *Policing: A Journal of Policy and Practice*, 15(1), p. 15-33.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Lawrence Erlbaum Associates.

Collier, B., Horgan, S., Jones, R. & Shepherd, L.A. (2020). *The implications of the covid-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations*. Scottish Institute for Policing Research.

Cross C. (2018). 'Expectations vs reality: Responding to online fraud across the fraud justice network'. *International Journal of Law, Crime and Justice*, 55, p. 1-12. doi: 10.1016/j.ijlcj.2018.08.001.

Cross, C. (2020). "'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims'. *Criminology & Criminal Justice*, 20(3), p. 358-375. <https://doi.org/10.1177/1748895819835910>.

Cross, C. & Blackshaw, D. (2015). 'Improving the police response to online fraud'. *Policing: A Journal of Policy and Practice*, 9(2), p. 119-128. doi: 10.1093/policing/pau044.

Cross, C., Holt, T., Powell, A. & Wilson, M. (2021). 'Responding to cybercrime: Results of a comparison between community members and police personnel'. *Trends and Issues in Crime and Criminal Justice*, 635, p. 1-20.

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, p. 1-14. <https://doi.org/10.52922/til48355>.

Dodge, C. & Burruss, G. W. (2019). 'Policing cybercrime: Responding to the growing problem and considering future solutions'. In R. Leukfeldt & T. Holt (Eds.), *The human factor of cybercrime* (p. 339-358). Routledge.

Forouzan, H., Jahankhani, H. & McCarthy, J. (2018). 'An examination into the level of training, education and awareness among frontline police officers in tackling cybercrime within the Metropolitan Police Service'. In H. Jahankhani (Ed.), *Cyber Criminology. Advanced Sciences and Technologies for Security Applications* (p. 307-323). Springer.

Friese, S. (2014). *Qualitative data analysis with ATLAS.ti*. Sage.

- Hadlington, L., Lumsden, K., Black, A. & Ferra, F. (2021). 'A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime'. *Policing: A Journal of Policy and Practice*, 15(1), p. 34-43.
- Hinduja, S. (2004). 'Perceptions of local and state law enforcement concerning the role of computer crime investigative teams'. *Policing: An International Journal of Police Strategies & Management*, 27(3), p. 341-357. <https://doi.org/10.1108/13639510410553103>.
- Hitchcock, A., Holmes, R. & Sundorph, E. (2017). *Bobbies on the net: A police workforce for the digital age*. Reform August.
- Holt, T. J. & Bossler, A.M. (2012). 'Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments'. *Cyberpsychology, Behavior, and Social Networking*, 15(9), p. 464-472. <https://doi.org/10.1089/cyber.2011.0625>.
- Holt, T.J., Bossler, A.M. & Fitzgerald S. (2010). 'Examining State and Local Law Enforcement Perceptions of Computer Crime'. In T.J. Holt (Ed.), *Crime online: Correlates, Causes, and Context* (p. 221-246). Carolina Academic Press.
- Huisman, S., Princen, M., Klerks, P. & Kop, N. (2016). *Handelen naar waarheid. Sterkte- en zwakteanalyse van de opsporing*. Politieacademie.
- Hull, M., Eze, T. & Speakman, L. (2018). 'Policing the cyber threat: Exploring the threat from cyber crime and the ability of local law enforcement to respond'. In *Proceedings of the European Intelligence and Security Informatics Conference* (p. 15-22). IEEE. <http://dx.doi.org/10.1109/EISIC.2018.00011>.
- Jansen, J. (2025). *Samen sterker in een digitaliserende samenleving: Van en met elkaar leren*. Boom.
- 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), p. 205-228.
- Jansen, J., van Valkengoed, T., Veenstra, S. & Stol, W. Ph. (2020). *Level-Up! Kennis voor politiewerk in een digitale samenleving*. NHL Stenden Hogeschool/Politieacademie.
- Johnson, D., Faulkner, E., Meredith, G. & Wilson, T. J. (2020). 'Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts'. *The Journal of Criminal Law*, 84(5), p. 427-450.

---

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

Kort, J. & Spithoven, R. (2022). Uit de praktijk. Lokale stappen in de aanpak van gedigitaliseerde criminaliteit. *Tijdschrift voor Veiligheid*, 21(3/4), p. 109-119.

Lee, J. R., Nam, Y., Lee, W. G., Holt, T. J. & Bossler, A. M. (2025). 'Police capacity for cybercrime response: Assessing the impact of officers' perceptions and agency-level factors on England and Wales constables' capability responding to computer hacking offenses'. *Journal of Criminal Justice*, 101, 102541. <https://doi.org/10.1016/j.crimjus.2025.102541>.

Leukfeldt, E. R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Eleven International Publishers.

Leukfeldt, E. R., Notté, R. J. & Malsch, M. (2020). 'Exploring the needs of victims of cyber-dependent and cyber-enabled crimes'. *Victims & Offenders*, 15(1), p. 60-77.

Leukfeldt, E. R., Spithoven, R. & Misana-ter Huurne, E.F.J. (2020). 'De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk'. *Cahiers Politiestudies*, 2020(3), p. 203-223.

Leukfeldt, E. R., Veenstra, S., Domenie, M.M.L. & Stol, W.P. (2012). *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime*. Lectoraat Cybersafety, NHL Stenden Hogeschool.

Leukfeldt, E. R., Veenstra S. & Stol W.Ph. (2013). 'High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands'. *International Journal of Cyber Criminology*, 7(1), p. 1-17.

McNealey, R. L., Figueroa, C. I. & Maher, C. A. (2025). "Police can't help you": Exploring influences on perceptions of policing cybercrime'. *Journal of Criminal Justice*, 101, 102542. <https://doi.org/10.1016/j.crimjus.2025.102542>.

Meershoek, G. (In Press). 'Intelligence in the Dutch police 1880-1940. New technologies and stubborn detectives'. In A. Renglet (ed.), *Police intelligence*. Palgrave, nog te verschijnen.

Nowacki, J. & Willits, D. (2020). 'An organizational approach to understanding police response to cybercrime'. *Policing: An international journal*, 43(1), p. 63-76.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y. & Podsakoff, N. P. (2003). 'Common method biases in behavioral research: A critical review of the literature and recommended remedies'. *Journal of Applied Psychology*, 88(5), p. 879-903.

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

Politie (2023). *Toewijzingskader cybercrime (concept)*. Agenda (Portefeuille) Digitalisering & Cybercrime, Nationale Politie.

Politie (2026). *Jaarcijfers: Nieuwe oplossingen nodig voor veranderende criminaliteit*. Geraadpleegd op: <https://www.politie.nl/nieuws/2026/januari/13/jaarcijfers-nieuwe-oplossingen-nodig-voor-veranderende-criminaliteit.html>.

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

Rogers, E.M. (2003). *Diffusion of innovations (5th edition)*. Free Press.

Ruiter, S., van Leuken, M., van Ruitenburch, T., Schiks, J. & Leukfeldt, R. (2023). *In- en doorstroom van online criminaliteit in de strafrechtketen*. NSCR.

Saldaña, J. (2012). *The coding manual for qualitative researchers*. Sage.

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

Schreuders, C., Cockcroft, T., Butterfield, E., John, E., Ahmad Ryad, S. & Mohammad, S. A. (2020). 'Needs assessment of cybercrime and digital evidence in a UK police force'. *International Journal of Cyber Criminology*, 14(1), p. 316-340. <https://doi.org/10.5281/zenodo.3757271>.

Shandler, R. & Gomez, M. A. (2023). 'The hidden threat of cyber-attacks—undermining public confidence in government'. *Journal of Information Technology & Politics*, 20(4), p. 359-374. doi.org/10.1080/19331681.2022.2112796.

Skidmore, M., Goldstraw-White, J. & Gill, M. (2020). 'Vulnerability as a driver of the police response to fraud'. *Journal of Criminological Research, Policy and Practice*, 6(1), p. 49-64.

---

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

Spithoven, R., Jansen, J., Drenth, A.R. & Leukfeldt, E.R. (2022). 'Redactioneel. Wijk + web. De noodzaak van een lokale aanpak van cybercriminaliteit'. *Tijdschrift voor Veiligheid*, 21(3/4), p. 3-12.

Spithoven, R. & Leukfeldt, E.R. (2023). 'Gemeenten lijden aan digitale koudwatervrees. Waarom Nederlandse gemeenten verder op cybercriminaliteit verder in beweging moeten komen'. In *SECONDANT*, via: <https://ccv-secondant.nl/platform/article/gemeenten-lijden-aan-digitale-koudwatervrees>.

Spithoven, R. & Walberg, A. (2026). 'Uitdagingen in het doen van actieonderzoek. Reflecties op onze eerste pogingen samen met de politie en lokale partners'. In R. van Steden, G. Schuiling & S. J. Mulder (Red.), *Impact met actieonderzoek*. Boom.

Spithoven, R., van Amersfoort, C.W., Klopman, J. & Land, E (2026). 'Local police emergency assistance for victims of online crime: Qualitative reflections on first experiences from emergency response shifts in the Netherlands'. *Policing: An International Journal*. <https://doi.org/10.1108/PIJPSM-03-2026-0080>.

Stambaugh H., Beaupre D.S., Icove D.J., et al. (2001). *Electronic crime needs assessment for state and local law enforcement*. Washington, DC: National Institute of Justice.

Steden, R. van, Woerds, S. ter, Merk, A., Schuppers, K., Willekers, M., Valk-van Waarde, D., Jansen, R. & Ruiter, S. (2025). *Online Blauw. Een onderzoek naar de rol van basisteams in de aanpak van digitale criminaliteit en ervaringen van slachtoffers met de politie*. Politiekunde, 130.

Stol, W. P. (1996). *Politieoptreden en informatietechnologie*. Vrije Universiteit Amsterdam (academisch proefschrift).

Stol, W. P., Leukfeldt, E. R. & Klap, H. (2013). 'Policing a digitized society. The state of affairs in the Netherlands in 2013'. In W. Ph Stol & J. Jansen (Eds.), *Cyber Criminology* (p. 61-74). Springer.

Stol, W.P., Treeck, R.J. van & Ven, A.E.B.M. van der (1999). *Criminaliteit in cyberspace: Een praktijkonderzoek naar aard, ernst en aanpak in Nederland*. Elsevier.

Terpstra, J.B. (2023). 'Gebiedsgebonden politiewerk. Ambivalentie, continuïteit en voortgaande ontwikkeling'. In: J. van Hoorn & M. van Bavel (Eds.), *Onze politie in een kwetsbare rechtsstaat*. Gompel & Svacina, p. 15-38.

Terpstra, J.B. (2024). 'Eenheid en breuklijnen. De opdracht van de politie tegen de achtergrond van interne ontwikkelingen'. *Tijdschrift voor Veiligheid*, 23(1/2), p. 71-85.

Terpstra J.B., Salet., R., Duijneveldt, I.M. van, Havinga, T. (2021). *Gebiedsgebonden Politiewerk in Ontwikkeling. Onderzoek naar Basisteams in een digitale superdiverse samenleving*. Politie en Wetenschap, 124.

Toutenhoofd-Visser, M.H., Veenstra S., Domenie M.M.L., Leukfeldt E.R. & Stol W.Ph. (2009). *Politie en Cybercrime. Intake en eerste opvolging. Een onderzoek naar de intake van het werkaanbod cybercrime door de politie*. NHL Hogeschool.

Van Amersfoort, C.W., Klopman, J., Walberg, A.W., Land, E. & Spithoven, R. (2025). *#DigiTP – Ter plaatse bij online slachtofferschap. Een theoriegestuurde, ex-durante beleidsevaluatie van De Digitale Meldkamer van de politie Oost-Nederland*. Hogeschool Saxion.

Van den Berg, E. & Kouwenhoven, W. (2008). Ontwerponderzoek in vogelvlucht. *Tijdschrift voor lerarenopleiders*, 29(4), p. 20-26.

Van Turnhout, K., Andriessen, D. & Cremers, P. (2023). *Handboek ontwerpgericht wetenschappelijk onderzoek*. Boom.

Wall, D. S. (2007). 'Policing cybercrimes: Situating the public police in networks of security within cyberspace'. *Police Practice and Research*, 8(2), p. 183-205. <https://doi.org/10.1080/15614260701377729>.

Wilson, M., Cross, C., Holt, T. & Powell, A. (2022). 'Police preparedness to respond to cybercrime in Australia: An analysis of individual and organizational capabilities'. *Journal of Criminology*, 55(4), p. 468-494.

Yar, M. (2005). 'The novelty of "cybercrime": an assessment in light of Routine Activity Theory'. *European Journal of Criminology*, 2(4), p. 407-427.

Zuurveen, R. & Stol, W.Ph. (2020). *Benutten van digitale sporen*. Politiekunde, 107.

## **Bijlagen**



## Bijlage 1 Beschrijving basisteams

### Beschrijving basisteam Postenveld

Het basisteam Postenveld<sup>33</sup> is gevestigd in de regionale eenheid Noord-Nederland. De regionale eenheid Noord-Nederland bestaat uit drie districten waaronder district Groningen, Fryslân en Drenthe. De beschrijving van dit basisteam is gebaseerd op een gesprek met de Operationeel Specialist C (OS-C) van het team. De OS-C'er is verantwoordelijk voor het verbeteren van de processen van het basisteam (het 'hoe'). De teamchef van het basisteam is verantwoordelijk voor het leidinggeven en dagelijks functioneren van het basisteam (het 'wat').

Het basisteam Postenveld is opgebouwd uit verschillende functionele eenheden, waaronder GGP, I&S en VVC. Binnen de GGP zijn verschillende clusters actief, verdeeld over meerdere locaties. Elk cluster bestaat uit ongeveer vijftien personen, voornamelijk medewerkers en senioren GGP. Elk cluster heeft twee OE's: één Wijk en één Leiding en Sturing (OE-LS). Een OE-LS kan verschillende rollen hebben, zoals Operationeel Coördinator (OpCo; voor de dagelijkse aansturing op het basisteam), Hulpofficier van justitie (HOvJ) en Officier van Dienst Politie (OvD-P) voor aansturing bij incidenten. Een OE Wijk heeft verschillende thema's aan zich verbonden en is op inhoud bij de wijkagenten betrokken, maar heeft geen leidinggevende functie. Er is één digitale wijkagent in basisteam Postenveld. Er is ook een kwaliteitshulpofficier van justitie, die onder andere verantwoordelijk is voor het bewaken van de kwaliteit van opsporing en de intake (dienstverlening).

Het cluster I&S is essentieel voor de dienstverlening van basisteam Postenveld. Medewerkers van dit cluster zijn verantwoordelijk voor het eerste contact met de burger, het vastleggen en beoordelen van meldingen en het doorgeleiden van zaken naar de juiste clusters of specialismen. De senior medewerkers I&S screenen binnenkomende zaken binnen het verzorgingsgebied en selecteert op basis van prioritering en op basis van opsporingsmogelijkheden.

Binnen VVC werken gespecialiseerde medewerkers aan opsporing en onderzoek. Naast deze medewerkers is er een leidinggevende (operationeel expert) en zijn er drie medewerkers Senior Tactische Opsporing (STO). De STO'er heeft een cruciale rol. Hij of zij screent nieuwe zaken en bepaalt welke dossiers binnen VVC worden opgepakt. Dit selectieproces is echter niet enkel een interne afweging; het gebeurt in samenspraak met de officier van justitie tijdens het zogenoemde 'zicht op zaken'-overleg. Zo wordt

33 Deze beschrijving van basisteam Postenveld is beschreven per februari 2024, met een update in december 2024.

gewaarborgd dat de gekozen zaken niet alleen strategisch en efficiënt zijn afgestemd op de capaciteit en expertise van VVC maar ook op de prioriteiten van het Openbaar Ministerie.

Naast de eerdergenoemde teams en functies spelen drie Operationeel Specialisten A (OS-A) een belangrijke rol binnen het basisteam. Deze OS-A's werken nauw samen met de clusters op het gebied van veiligheidsproblemen en processen. Vanwege hun brede inzetbaarheid functioneren zij als een soort 'vliegende kiep', die ook op uiteenlopende operationele uitdagingen kan worden ingezet. Ook is er een secretariael medewerker ter ondersteuning van de teamleider en een gespecialiseerd medewerker B voor alle regelzaken.

Binnen het basisteam is er tevens een portefeuillehouder online criminaliteit en een jeugdagent (die bijvoorbeeld een vinger aan de pols houdt op scholen in het kader van online criminaliteit). 'Buiten' het basisteam zijn er verschillende groepen waarmee nauw wordt samengewerkt. Ten eerste, de districtsrecherche (DR), die houdt zich bezig met High Impact Crime (HIC) en ondersteuning van het basisteam. Ten tweede, het flexteam van vijftien personen die worden gevraagd bij acties of ondersteuning en draaien zelf ook diensten in het district. Tot slot wordt samengewerkt met de DRIO (Dienst Regionale Intelligence Organisatie).

### **Beschrijving basisteam Lichtblauwveen**

Het basisteam Lichtblauwveen<sup>34</sup> is gevestigd in de regionale eenheid Oost-Nederland. De regionale eenheid Oost-Nederland bestaat uit de vijf districten. Basisteam Lichtblauwveen bestaat uit GGP, I&S, BR, OCP en leiding.

De GGP bestaat uit vier clusters met daarin een mix van ongeveer 25 (hoofd)agenten en wijkagenten. Het basisteam bestaat uit meerdere clusters. Elk cluster heeft een OE en een OE Wijk. Tijdens elke dienst is er een OpCo aanwezig voor de dagelijkse sturing. De OE's kunnen per dienst een verschillende rol uitvoeren, zoals de OpCo-rol of de OvD-P-rol of werkzaam zijn als HOvJ. De leiding van een cluster bestaat uit een OE en een Wijkagent Operationeel Expert (WOE). Een WOE heeft een wijkoverstijgende rol in dit basisteam. Er zijn twee wijkagenten met een focus op online criminaliteit. Er is ook een kwaliteitshulpofficier van justitie, verantwoordelijk voor het bewaken van de kwaliteit van opsporing. Meerdere Senioren tactische opsporing zijn werkzaam binnen het basisteam.

De BR behandelt de complexere zaken, maar screent zelf geen zaken. Deze taak ligt binnen dit basisteam bij de OCP. Zij screenen en coördineren de verschillende zaken. Op het basisteam zijn ook een aantal specialisten OS-A werkzaam, die ontwikkelvraagstukken behandelen, ondersteunen bij het inrichten van processen en zich bezighouden met thema's zoals ondermijning en de digitale transformatie. Deze specialisten hebben ook de rol van HOvJ. Binnen het basisteam werken de collega's samen met een digitaal informatiepunt met daarin een OS-A, digitaal wijkagent(en) en een ICT-coach, en meerdere jeugdagenten (die zich bezighouden met jeugdgroepen). De organisatie-

34 Deze beschrijving van basisteam Lichtblauwveen is beschreven per oktober 2024.

---

onderdelen waar basisteam Lichtblauwveen mee samenwerkt zijn talrijk. Zij werken bijvoorbeeld zelf aan High Impact Crime zaken. ‘Buiten’ het basisteam zijn er afdelingen waarmee nauw wordt samengewerkt. Bijvoorbeeld het Cybercrimeteam, Forensische Opsporing (FO), Team Digitale Opsporing (TDO) en de DR, die zich bezighouden met High Impact Crime en het flexteam.



## Bijlage 2 Interviewprotocol basisteams

### Inleiding

Allereerst bedankt dat u mee wilt werken met dit onderzoek. NHL Stenden Hogeschool, Hogeschool Saxion en de Haagse Hogeschool voeren een onderzoek uit naar de lokale aanpak van gedigitaliseerde criminaliteit. Dit doen wij in samenwerking met de politie waaronder twee basisteams, een Cybercrimeteam en een digitaal platform.

### *Doel van interview*

In dit interview willen wij focussen op hoe politiemensen de lokale taak in de aanpak van gedigitaliseerde criminaliteit zien, welke kennis en vaardigheden ze denken nodig te hebben en welke ze al in huis hebben. Tevens zijn wij benieuwd naar manieren om deze kennis en vaardigheden verder te stimuleren om de lokale aanpak van gedigitaliseerde criminaliteit te intensiveren.

### *Belangrijke informatie vooraf*

- Alle input wordt in principe anoniem verwerkt in een eindrapport.
- Het verslag van dit interview wordt desgewenst ter verificatie voorgelegd. De geïnterviewde heeft, indien relevant, de mogelijkheid om de eerder gegeven toestemming in te trekken. Ook mag de geïnterviewde deelname aan het onderzoek op elk moment stoppen, zonder opgave reden.
- Toestemming tot opname? Dit wordt alleen gebruikt voor uitwerkingsdoeleinden en vernietigd na eventuele verificatie van het verslag door de geïnterviewde én het vaststellen ervan. Het geanonimiseerde verslag wordt op veilige wijze bewaard door Saxion Hogeschool en u kunt op verzoek inzage krijgen in de wijze waarop gegevens worden verwerkt en bewaard.
- Geïnterviewde gelegenheid bieden tot het stellen van vragen over het onderzoek.
- 'Informed consent'-formulier digitaal laten tekenen.

### *Introductie*

1. Kunt u vertellen over uw functie en welke rol(len) u heeft binnen het basisteam?
2. In hoeverre bent u bekend met het begrip 'online criminaliteit', en wat verstaat u daaronder?

We vragen in de rest van dit interview naar uw visie op en ervaringen met **online criminaliteit**. Hieronder verstaan wij zowel 'gedigitaliseerde criminaliteit' als 'cybercrime'. Onder **gedigitaliseerde criminaliteit** verstaan wij klassieke vormen van crimina-

liteit in een nieuwe digitale jas, zoals WhatsApp-fraude, phishing, verkoopfraude, online bedreiging, stalking en discriminatie. Onder **cybercrime** verstaan wij vormen van criminaliteit die gepleegd worden met een ICT-middel en zijn gericht op ICT. Denk hierbij aan ransomware aanvallen, DDoS-aanvallen, hacking en malware. In het interview vragen wij naar online criminaliteit en willen wij een beeld vormen van zowel gedigitaliseerde criminaliteit als cybercrime.

3. Hoe kijkt u naar online criminaliteit in de samenleving?

*Instructie; vraag door op vormen van cybercrime of gedigitaliseerde criminaliteit indien niet spontaan benoemd.*

- a. Wat is uw beeld van de omvang van het slachtofferschap van online criminaliteit in de samenleving? En hier lokaal in [basisteam]?
- b. Wat is uw beeld van de impact van het slachtofferschap van online criminaliteit in de samenleving? En hier lokaal in [basisteam]?
- c. Wat is uw beeld van de daders van online criminaliteit in de samenleving? En hier lokaal in [basisteam]?
- d. Heeft u affiniteit met het aanpakken en/of voorkomen van online criminaliteit? Waarom wel/niet?

4. Heeft u ooit een opleiding/cursus gevolgd op het gebied van online criminaliteit?

*Instructie: indien niet duidelijk, vraag door of cursus ging over gedigitaliseerde criminaliteit en/of cybercrime en/of IT in algemene zin (opleiding, tooling et cetera).*

*Werkzaamheden*

5. Bent u in het afgelopen jaar in aanraking gekomen met online criminaliteit in uw werk?

- a. Zo ja, wat deed zich voor? (*instructie; eventueel afbakenen tot twee voorbeelden; meest recent of tot de verbeelding sprekend.*) Welke rol speelt online criminaliteit in uw werk?
  - i. Welke rol speelt gedigitaliseerde criminaliteit in uw werk?
  - ii. Welke rol speelt cybercrime in uw werk?

*Rol*

6. Wat is of zijn volgens u de taak of taken van het basisteam in de lokale aanpak van online criminaliteit?

- a. Hoe verhoudt deze taak (of verhouden deze taken) van het basisteam in de lokale aanpak van online criminaliteit zich tot de taken van andere onderdelen van het district, de eenheid en de Nationale Politie?
- b. In hoeverre verschilt dit tussen gedigitaliseerde criminaliteit of cybercrime?

7. Waar zou hier binnen het basisteam het zwaartepunt moeten liggen in de aanpak van online criminaliteit? Waarom?

- a. In hoeverre verschilt dit tussen gedigitaliseerde criminaliteit of cybercrime?

---

Volgens het **toewijzingskader** van de Agenda Digitalisering & Cybercrime zouden basisteams zich in de nabije toekomst moeten gaan richten op online criminaliteitszaken waarbij de dader bekend is en er sprake is van een lage complexiteit in combinatie met veel opsporingsindicaties. Denk hierbij aan het afhandelen en oppakken van geldezels, sextortion-zaken waarbij de dader bekend is en zonder letsel voor (of de dood van) het slachtoffer en cyberpesten in de relationele of lokale sfeer. En bijvoorbeeld aan hacken in de relationele sfeer (onrechtmatig inloggen of in mailboxen of social media van een ander kijken); DDoS-aanvallen met bekendheid van de dader (een doelbewuste overbelasting van de digitale infrastructuur van een organisatie om deze uit de lucht te halen) en diefstal van gegevens door medewerkers van een bedrijf.

8. Wat vindt u van dit toewijzingskader?
  - a. In hoeverre is uw BT al actief op deze delicten?
    - i. *Notitie: vraag voorbeelden uit van gedigitaliseerde criminaliteit en cybercrime.*
  - b. Wanneer zal uw BT deze toewijzing waar kunnen maken en wat is daarvoor nodig denkt u?
  - c. In hoeverre is er verschil in activiteit op het gebied van gedigitaliseerde criminaliteit en cybercrime? Waar ligt dat volgens u aan?

### **Kennis en vaardigheden**

*In deze paragraaf vragen wij naar de benodigde kennis en vaardigheden om online criminaliteit aan te pakken. Wij starten met vragen over uw afdeling en uw rollen en stellen later vragen over het hele basisteam.*

9. Welke belangrijkste **kennis** is nodig bij de afdeling (waar geïnterviewde werkt)/uw functie om online criminaliteit lokaal aan te pakken?
  - a. *Instructie: indien niet spontaan benoemd, bijvoorbeeld juridische kaders, kennis over typen cybercrime, kennis over opsporingsmogelijkheden zoals digitale sporen veiligstellen, strafbaarstelling van cyberdelicten, verbanden tussen delict en juiste vragen bij aangifte, kennen van tools, bewijswaarde inschatten (evidential evaluation) et cetera.*
10. In hoeverre is deze **kennis** voldoende beschikbaar binnen de afdeling? Welke wel en welke niet?
  - a. Welke kennis zou nog ontwikkeld moeten worden? Welke heeft/hebben prioriteit?
  - b. Geldt dit ook voor de rest van het basisteam (andere afdelingen), of gelden daarvoor andere prioriteiten in kennis?
  - c. In hoeverre is deze kennis voldoende beschikbaar op platformen van de politie? Welke platformen zijn dit? In hoeverre kijkt u naar die platformen? Waarom wel/niet?
  - d. Weet u waar u kennis en vaardigheden kunt halen? Hoe doet u dit?

11. Welke specifieke **vaardigheden** zijn nodig bij de afdeling (*waar geïnterviewde werkt*)/uw functie om online criminaliteit lokaal aan te pakken?
  - a. *Indien niet spontaan benoemd, bijvoorbeeld digitale sporen kunnen veiligstellen, juiste vragen kunnen stellen bij intake, relevante digitale gegevensdragers herkennen, gegevens kunnen duiden, gebruiken van opsporingstools (iRN).*
12. In hoeverre zijn deze **vaardigheden** voldoende beschikbaar binnen de afdeling? Welke wel en welke niet?
  - a. In welke vaardigheden zouden nog ontwikkeld moeten worden?
  - b. Geldt dit ook voor de rest van het basisteam (andere afdelingen), of gelden daarvoor andere prioriteiten in vaardigheden?

#### *Lokale aanpak intensiveren*

13. Hoe zou u in uw werk zien dat er vooruitgang is geboekt op digitaal gebied?
14. Welke kennis en/of vaardigheid zou u graag willen ontwikkelen om online criminaliteit beter aan te kunnen pakken?
15. In hoeverre heeft het basisteam zich de laatste twee jaren ontwikkeld in de aanpak van gedigitaliseerde criminaliteit en cybercrime?
  - a. Indien ontwikkeld, hoe is die ontwikkeling tot stand gekomen?
  - i. Workshops, trainingen, presentaties, mails, serious gaming, learning by doing et cetera.
  - ii. Wat gaat goed, wat kan beter? Waar blijkt dat volgens u uit?
    - b. Indien niet ontwikkeld, wat is daarvoor de oorzaak? Wat kan gedaan worden om daarin toch stappen te maken?
16. Hoe zouden politiemensen vanuit het basisteam volgens u het best gestimuleerd kunnen worden in de aanpak van gedigitaliseerde criminaliteit en cybercrime?
  - a. Wat heeft hiervoor gewerkt bij kennisontwikkeling en vaardighedenontwikkeling voor u? (*instructie; hierbij ook de ruimte geven voor ontwikkeling op andere gebieden; naast online criminaliteit*)
  - b. Wat heeft hiervoor gewerkt bij kennisontwikkeling en vaardighedenontwikkeling voor het basisteam? (*instructie; hierbij ook de ruimte geven voor ontwikkeling op andere gebieden; naast online criminaliteit*)
  - c. Waarin kan of moet het basisteam volgens u faciliteren/ondersteunen?
  - d. Zijn er anderen die u kunnen faciliteren/ondersteunen? (*instructie; bij geen spontane reactie: denk aan andere eenheden, organisatieonderdelen, landelijk, externen (zoals kennisinstellingen)*)

---

**Afsluiting**

Wij zijn hiermee aan het einde gekomen van het interview. Tot slot willen we u graag nog een praktische vraag stellen omtrent het onderwerp.

17. Heeft u nog suggesties of anderszins opmerkingen omtrent dit onderwerp die we niet hebben besproken in het interview, maar die u wel graag wilt delen?



## Bijlage 3 Codering van de basisteams- interviews

In deze bijlage wordt uitgebreider verslag gedaan van het coderingsproces van de transcripten, waarvan de resultaten zijn opgenomen in hoofdstuk 3. Tabel 3.1 geeft een overzicht van alle hoofdcodes en subcodes per thema, gebaseerd op de codering. Hieruit blijkt dat het aantal coderingen per hoofdthema redelijk gelijk verdeeld is tussen beide basisteams.

Tabel 3.1 Overzicht van alle hoofdcodes, geordend per thema

| Thema                                                      | Hoofdcode                              | Basisteam<br>Postenveld | Basisteam<br>Lichtblauwveen |
|------------------------------------------------------------|----------------------------------------|-------------------------|-----------------------------|
| <b>Behoeften aanpak OC</b><br>(Totaal 396 codes)           | Belemmerende/succesfactoren            | 105                     | 87                          |
|                                                            | Benodigde kennis                       | 15                      | 21                          |
|                                                            | Benodigde vaardigheden                 | 6                       | 14                          |
|                                                            | Interventies                           | 43                      | 105                         |
|                                                            | <b>Totaal Behoeften aanpak OC</b>      | <b>169</b>              | <b>227</b>                  |
| <b>Huidige status aanpak OC</b><br>(Totaal 272 codes)      | Effectiviteit aanpak OC                | 1                       | 0                           |
|                                                            | Huidige aanpak OC                      | 34                      | 34                          |
|                                                            | Huidige kennis                         | 31                      | 32                          |
|                                                            | Huidige vaardigheden                   | 4                       | 6                           |
|                                                            | Prevalentie OC basisteam               | 24                      | 28                          |
|                                                            | Teamontwikkeling                       | 47                      | 31                          |
|                                                            | <b>Totaal Huidige status aanpak OC</b> | <b>141</b>              | <b>131</b>                  |
| <b>Persoonlijke factoren</b><br>(Totaal 81 codes)          | Affiniteit                             | 12                      | 7                           |
|                                                            | Functie/rollen                         | 18                      | 19                          |
|                                                            | Opleiding/politie-ervaring             | 8                       | 13                          |
|                                                            | Ervaring OC privésituatie              | 2                       | 2                           |
|                                                            | <b>Totaal Persoonlijke factoren</b>    | <b>40</b>               | <b>41</b>                   |
| <b>Perspectief</b><br>(Totaal 270 codes)                   | Ideaalbeeld lokale aanpak              | 16                      | 15                          |
|                                                            | Visie op OC                            | 71                      | 52                          |
|                                                            | Visie op toewijzingskader              | 19                      | 10                          |
|                                                            | Visie rol BT                           | 31                      | 56                          |
|                                                            | <b>Totaal Perspectief</b>              | <b>137</b>              | <b>133</b>                  |
| <i>Notitie. OC = Online criminaliteit, BT = Basisteam.</i> |                                        |                         |                             |

Om de resultaten van Basisteam Postenveld en Lichtblauwveen te bundelen, hebben twee coderende onderzoekers elke variatie tijdens een fysiek overleg opgeschreven op een post-it, en op een muur per thema samengevoegd (zie figuur 3.1). Op deze wijze konden de onderzoekers in één oogopslag zien waar de overeenkomsten en verschillen tussen de coderingen van de interviews met medewerkers van de twee basisteams lagen. In figuur 3.2 staat een voorbeeld van het digitale coderingsproces en figuur 3.3 toont het uiteindelijke uitgewerkte codeboek in ATLAS.ti.



Figuur 3.1 Fysiek codeerproces; vergelijking resultaten Basisteams Postenveld en Lichtblauwveen



Figuur 3.2 Voorbeeld gecodeerde quotatie (JK09, BT B)

| Search Entities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                       |                                                                                                                 |        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------|
| Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Grounded                                                                                                                              | Density                                                                                                         | Groups |
| <ul style="list-style-type: none"> <li>Behoeften aanpak OC               <ul style="list-style-type: none"> <li>Belemmerend/succesfactoren</li> <li>Benodigde kennis</li> <li>Benodigde vaardigheden</li> <li>Interventies</li> </ul> </li> <li>Huidige status aanpak OC               <ul style="list-style-type: none"> <li>Effectiviteit aanpak OC</li> <li>Huidige aanpak OC</li> <li>Huidige kennis</li> <li>Huidige vaardigheden</li> <li>Prevalentie OC basisteam</li> <li>Teamontwikkeling tot nu toe</li> </ul> </li> <li>Niet relevant</li> <li>Persoonlijke factoren               <ul style="list-style-type: none"> <li>Affiniteit</li> <li>Functie / rollen</li> <li>Opleiding / Politie-ervaring</li> <li>Privé ervaring OC</li> </ul> </li> <li>Perspectief               <ul style="list-style-type: none"> <li>Ideaal beeld lokale aanpak</li> <li>Visie op OC</li> <li>Visie op toewijzingskader</li> <li>Visie rol BT</li> </ul> </li> </ul> | 169<br>105<br>15<br>6<br>43<br>141<br>1<br>34<br>31<br>4<br>24<br>47<br>47<br>40<br>12<br>18<br>8<br>2<br>137<br>16<br>71<br>19<br>31 | 0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0 |        |

Figuur 3.3 Voorbeeld codeboek (BT B)



## Bijlage 4 Vragenlijst politiebasisteams

### **Toestemming**

Bedankt voor uw interesse in dit onderzoek. Dit onderzoek is voor politiemensen die in een basisteam werken. Nadat u het toestemmingsformulier hierna heeft gelezen, kunt u op 'Ik ga akkoord' klikken als u wilt deelnemen.

### **Doel van het onderzoek**

Dit onderzoek wordt uitgevoerd door NHL Stenden en Saxion, in opdracht van Politie en Wetenschap. We brengen in kaart hoe mensen in basisteams online criminaliteit (kunnen) aanpakken, wat kan leiden tot verbeteringen in het politiewerk en beleid. Uw antwoorden zijn hierbij erg belangrijk.

### **Invullen vragenlijst**

Het invullen van deze vragenlijst duurt ongeveer vijftien minuten. Het is mogelijk om een deel van de vragenlijst in te vullen en het op een later tijdstip af te maken (via dezelfde URL-link).

### **Uw rechten**

U hoeft niet deel te nemen en mag op elk moment stoppen met het invullen van de vragenlijst. Dit heeft geen nadelige gevolgen.

### **Risico's van deelname**

Naar verwachting brengt het invullen van de vragenlijst geen fysieke of emotionele risico's met zich mee.

### **Vertrouwelijkheid en privacy van uw gegevens**

Deelname is vertrouwelijk. We vragen *geen* persoonlijk identificeerbare gegevens. Als u toch persoonlijke informatie geeft dan wordt deze verwijderd, zodat uw antwoorden niet te herleiden zijn. Uw antwoorden worden alleen gebruikt voor wetenschappelijke en praktijkgerichte publicaties en worden na tien jaar verwijderd.

### **Contactgegevens voor vragen**

Als u vragen heeft, dan kunt u contact opnemen met Saskia Westers en Nick van der Klok, via e-mail: [e-mailadres].

**Toestemming om deel te nemen**

Uw deelname aan dit onderzoek is geheel vrijwillig.

1. Ik heb voorgaande informatie gelezen en begrepen. Ik ga akkoord met deelname aan dit onderzoek door hierna op 'Ik ga akkoord' te klikken.

☐ Ik ga akkoord (naar vragenlijst)

☐ Ik ga niet akkoord (naar exit pagina)

*Exit: U geeft aan niet akkoord te gaan met deelname aan dit onderzoek. Bedankt voor uw reactie.*

2. Bent u werkzaam voor een politiebasis-team? (screen-out vraag #1)

|                       |                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------|
| <input type="radio"/> | Ja, ik ben werkzaam in een politiebasis-team                                                      |
| <input type="radio"/> | Nee, ik ben niet werkzaam in een politiebasis-team (BT), maar werk met BT('s) samen (exit)        |
| <input type="radio"/> | Nee, ik ben niet werkzaam in een politiebasis-team (BT), en werk ook niet met BT('s) samen (exit) |

*Exit: De doelgroep van dit onderzoek zijn politiemensen die werkzaam zijn op een basis-team. U behoort niet tot deze doelgroep en kunt de vragenlijst daarom niet verder invullen. Bedankt voor uw interesse in dit onderzoek.*

3. Welke functieomschrijving past het beste bij uw werkzaamheden? (meerdere antwoorden mogelijk)

|                       |                                    |
|-----------------------|------------------------------------|
| <input type="radio"/> | Generalist GGP                     |
| <input type="radio"/> | Medewerker VVC/opsporing/crimeteam |
| <input type="radio"/> | Senior GGP - Wijkagent             |
| <input type="radio"/> | Senior GGP - Overig                |
| <input type="radio"/> | Medewerker I&S                     |
| <input type="radio"/> | Senior Tactische Opsporing         |
| <input type="radio"/> | Operationeel Specialist            |
| <input type="radio"/> | Operationeel Expert                |
| <input type="radio"/> | Operationeel coördinator           |
| <input type="radio"/> | Teamchef                           |
| <input type="radio"/> | Aspirant/stagiaire                 |
| <input type="radio"/> | Anders, namelijk ...               |

4. Welke omschrijving past het beste bij uw dagelijkse werkzaamheden binnen het basisteam? (meerdere antwoorden zijn NIET mogelijk)

|                       |                                                                            |
|-----------------------|----------------------------------------------------------------------------|
| <input type="radio"/> | I&S (algemeen + deel I&S)                                                  |
| <input type="radio"/> | Incidentafhandeling (algemeen + deel blauw)                                |
| <input type="radio"/> | Basisteamrecherche/opsporing (VVC/crime team) (algemeen + deel opsporing)  |
| <input type="radio"/> | Leidinggevende of operationeel specialist (algemeen + deel leidinggevende) |
| <input type="radio"/> | Anders .... (routing: alleen algemeen)                                     |

### Online criminaliteit

Volgens ontwikkelingen binnen de Nationale Politie zouden basisteams zich in de nabije toekomst moeten gaan richten op online criminaliteitszaken. Denk hierbij aan geldezels en eenvoudige zaken van sextortion, cyberpesten, hacken en DDoS-aanvallen. In deze vragenlijst gaat het om online criminaliteitszaken waarbij de **dader bekend** is en er sprake is van een **lage complexiteit** in combinatie met **veel opsporingsindicaties**.

5. Geef voor u het meest passende antwoord: In hoeverre weet u wat [*online criminaliteitsvorm*] is? [Let op: Er zijn geen goede of foute antwoorden]. [routing: indien antwoord 'ik weet niet wat dit is' wordt gekozen, vraag 6 ook niet dat item laten zien]

*Let op: het gaat het om online criminaliteitszaken waarbij de dader bekend is en er sprake is van een lage complexiteit in combinatie met veel opsporingsindicaties.*

| Code                 | Item                                                  | Ik ken dit<br><i>niet</i> | Ik ken dit<br><i>enigszins</i> | Ik ken dit<br><i>goed</i> |
|----------------------|-------------------------------------------------------|---------------------------|--------------------------------|---------------------------|
| GC lage complexiteit | Werken als een geldezel/katvanger                     | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| GC lage complexiteit | Sextortion                                            | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| GC lage complexiteit | Cyberpesten                                           | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| CC lage complexiteit | Hacking                                               | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| CC lage complexiteit | DDoS-aanvallen                                        | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| CC lage complexiteit | Diefstal van persoonlijke gegevens                    | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| Centurion            | Telefonische helpdeskfraude (Bank-/helpdeskfraude)    | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| Centurion            | Aan- en verkoopfraude                                 | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| Centurion            | Hulpvraagfraude (Vriend-in-noodfraude/WhatsAppfraude) | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |
| Centurion            | Phishing                                              | <input type="radio"/>     | <input type="radio"/>          | <input type="radio"/>     |

6. Hoe vaak bent u in de afgelopen twaalf maanden in uw werk binnen het basisteam betrokken geweest bij zaken over online criminaliteit?

| <i>Code</i>          | <i>Item</i>                                                 | <i>Dage-<br/>lijks</i> | <i>Weke-<br/>lijks</i> | <i>Maan-<br/>delijks</i> | <i>Elk<br/>kwar-<br/>taal</i> | <i>Eén of<br/>enkele<br/>keren</i> | <i>Nooit</i> |
|----------------------|-------------------------------------------------------------|------------------------|------------------------|--------------------------|-------------------------------|------------------------------------|--------------|
| GC lage complexiteit | Een zaak waarbij een geldezel/katvanger betrokken is        | O                      | O                      | O                        | O                             | O                                  | O            |
| GC lage complexiteit | Sextortion                                                  | O                      | O                      | O                        | O                             | O                                  | O            |
| GC lage complexiteit | Cyberpesten                                                 | O                      | O                      | O                        | O                             | O                                  | O            |
| CC lage complexiteit | Eenvoudige hacking (waarbij dader(s) bekend is/zijn)        | O                      | O                      | O                        | O                             | O                                  | O            |
| CC lage complexiteit | Eenvoudige DDoS-aanvallen (waarbij dader(s) bekend is/zijn) | O                      | O                      | O                        | O                             | O                                  | O            |
| CC lage complexiteit | Diefstal van gegevens                                       | O                      | O                      | O                        | O                             | O                                  | O            |
| Centurion            | Telefonische helpdeskfraude (Bank-/helpdeskfraude)          | O                      | O                      | O                        | O                             | O                                  | O            |
| Centurion            | Aan- en verkoopfraude                                       | O                      | O                      | O                        | O                             | O                                  | O            |
| Centurion            | Hulpvraagfraude (Vriend-in-noodfraude/ WhatsAppfraude)      | O                      | O                      | O                        | O                             | O                                  | O            |
| Centurion            | Phishing                                                    | O                      | O                      | O                        | O                             | O                                  | O            |

### Werkzaamheden

De volgende vragen gaan over de aanpak van online criminaliteit. Met ‘aanpakken’ bedoelen we alle werkzaamheden in relatie tot online criminaliteit die uitgevoerd kunnen worden op een basisteam, zoals aangiften opnemen/screenen, opsporen, herkennen van digitale sporen et cetera.

7. Hoe goed weet u hoe u de hiernavolgende vormen van online criminaliteit kunt aanpakken in uw werk? [Let op: Er zijn geen goede of foute antwoorden]

| Code                 | Item                                                  | Ik weet <b>niet</b> hoe ik het moet aanpakken | Ik weet <b>enigszins</b> hoe ik het moet aanpakken | Ik weet hoe ik het <b>wel</b> moet aanpakken |
|----------------------|-------------------------------------------------------|-----------------------------------------------|----------------------------------------------------|----------------------------------------------|
| GC lage complexiteit | Een zaak met een geldezel/katvanger                   | O                                             | O                                                  | O                                            |
| GC lage complexiteit | Sextortion                                            | O                                             | O                                                  | O                                            |
| GC lage complexiteit | Cyberpesten                                           | O                                             | O                                                  | O                                            |
| CC lage complexiteit | Eenvoudige hacking                                    | O                                             | O                                                  | O                                            |
| CC lage complexiteit | DDoS-aanvallen                                        | O                                             | O                                                  | O                                            |
| CC lage complexiteit | Diefstal van gegevens                                 | O                                             | O                                                  | O                                            |
| Centurion            | Telefonische helpdeskfraude (Bank-/helpdeskfraude)    | O                                             | O                                                  | O                                            |
| Centurion            | Aan- en verkoopfraude                                 | O                                             | O                                                  | O                                            |
| Centurion            | Hulpvraagfraude (Vriend-in-noodfraude/WhatsAppfraude) | O                                             | O                                                  | O                                            |
| Centurion            | Phishing                                              | O                                             | O                                                  | O                                            |

### Kennis/vaardigheden

De volgende vragen gaan over kennis en vaardigheden in relatie tot online criminaliteit en de behoefte om daarin te ontwikkelen.

8. Geef aan in hoeverre u deze kennis bezit of vaardigheid hebt. [Let op: Er zijn geen goede of foute antwoorden]

|                                                                                       | Ik ken/kan het <b>niet</b> (1) | Ik ken/kan het <b>enigszins</b> (2) | Ik ken/kan het <b>wel</b> (3) | Weet ik niet (4) |
|---------------------------------------------------------------------------------------|--------------------------------|-------------------------------------|-------------------------------|------------------|
| Ik ken digitale platformen en socialmediakanalen (3)                                  | O                              | O                                   | O                             | O                |
| Ik kan digitale sporen herkennen (telefoon, internet et cetera) (4)                   | O                              | O                                   | O                             | O                |
| Ik weet hoe ik als politiemedewerker online informatie kan verzamelen (5)             | O                              | O                                   | O                             | O                |
| Ik ken de juridische bevoegdheden voor het gebruik van digitale informatie (6)        | O                              | O                                   | O                             | O                |
| Ik weet waar ik binnen de politie informatie kan vinden over online criminaliteit (7) | O                              | O                                   | O                             | O                |
| Ik weet waar ik binnen de politie vragen kan stellen over online criminaliteit (8)    | O                              | O                                   | O                             | O                |
| Ik durf in mijn werk te vragen om hulp over online criminaliteit (9)                  | O                              | O                                   | O                             | O                |

9. In welke mate wilt u zich verder ontwikkelen op de hiervoor genoemde punten?

- ☐ Helemaal geen interesse
- ☐ Weinig interesse
- ☐ Enige interesse
- ☐ Veel interesse
- ☐ Zeer veel interesse

10. Geef aan in hoeverre u deze kennis bezit of vaardigheid hebt. Alleen I&S [Let op: Er zijn geen goede of foute antwoorden]

|                                                                                                                                                                                                            | Ik ken/kan het<br><b>niet</b> (1) | Ik ken/kan het<br><b>enigszins</b> (2) | Ik ken/kan het<br><b>wel</b> (3) | Weet ik niet<br>(4)   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|----------------------------------------|----------------------------------|-----------------------|
| Ik ken de procedure voor het opnemen van aangifte van online criminaliteit (1)                                                                                                                             | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik ken vormen van online criminaliteit bij het opnemen van meldingen en aangiften (2)                                                                                                                      | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik kan op de juiste wijze een aangifte registreren in de politiesystemen (3)                                                                                                                               | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik weet welk gedrag op het internet strafbaar is (4)                                                                                                                                                       | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik weet hoe ik digitale sporen die voor de opsporing van belang zijn in kaart moet brengen bij het opnemen van aangifte (5)                                                                                | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik weet hoe ik aangevers moet adviseren om digitale sporen veilig te stellen (6)                                                                                                                           | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik ben bekend met informatieproducten die zijn ontwikkeld voor de intake van online criminaliteit (bijvoorbeeld factsheets, hulpmiddelen aangever, handreikingen, webapp cybercrime) (7)                   | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik kan slachtoffers van online criminaliteit adviseren in hun vervolgstappen (8)                                                                                                                           | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik weet naar welke partijen ik slachtoffers van online criminaliteit kan doorverwijzen (bijvoorbeeld Slachtofferhulp Nederland, banken, verzekeringsmaatschappijen, Offlimits. Stop it Now! et cetera) (9) | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik kan aangevers adviseren om (herhaald) slachtofferschap van online criminaliteit te voorkomen (10)                                                                                                       | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |

11. In welke mate wilt u zich verder ontwikkelen op de hiervoor genoemde punten?

- ☐ Helemaal geen interesse
- ☐ Weinig interesse
- ☐ Enige interesse
- ☐ Veel interesse
- ☐ Zeer veel interesse

12. Geef aan in hoeverre u deze kennis bezit of vaardigheid hebt. Alleen indicentaafhandeling. [Let op: Er zijn geen goede of foute antwoorden]

|                                                                                                                                                      | Ik ken/kan het <b>niet</b> (1) | Ik ken/kan het <b>enigszins</b> (2) | Ik ken/kan het <b>wel</b> (3) | Weet ik niet (4)      |
|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-------------------------------------|-------------------------------|-----------------------|
| Ik weet hoe ik met burgers via internet en social media kan communiceren (1)                                                                         | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik ben op de hoogte van mijn taken op een plaats delict bij online criminaliteit (2)                                                                 | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik weet hoe ik relevante digitale gegevensdragers kan herkennen op een plaats delict (3)                                                             | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik ken het juridisch kader voor mijn werk op een plaats delict ten aanzien van online criminaliteit (4)                                              | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik kan aangevers adviseren om (herhaald) slachtofferschap van online criminaliteit te voorkomen (5)                                                  | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik heb kennis over hoe ik aangevers kan adviseren om vervolgstappen te zetten wanneer zij het slachtoffer van online criminaliteit zijn geworden (6) | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik weet hoe ik met burgers via internet en social media kan communiceren (1)                                                                         | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik ben op de hoogte van mijn taken op een plaats delict bij online criminaliteit (2)                                                                 | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik weet hoe ik relevante digitale gegevensdragers kan herkennen op een plaats delict (3)                                                             | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik ken het juridisch kader voor mijn werk op een plaats delict ten aanzien van online criminaliteit (4)                                              | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |

13. In welke mate wilt u zich verder ontwikkelen op de hiervoor genoemde punten?

- ☐ Helemaal geen interesse
- ☐ Weinig interesse
- ☐ Enige interesse
- ☐ Veel interesse
- ☐ Zeer veel interesse

14. Geef aan in hoeverre u deze kennis bezit of vaardigheid hebt. Alleen basisteamrecherche/opsporing (VVC/crime team). [Let op: Er zijn geen goede of foute antwoorden]

|                                                                                                      | Ik ken/kan het <b>niet</b> (1) | Ik ken/kan het <b>enigszins</b> (2) | Ik ken/kan het <b>wel</b> (3) | Weet ik niet (4)      |
|------------------------------------------------------------------------------------------------------|--------------------------------|-------------------------------------|-------------------------------|-----------------------|
| Ik kan digitale sporen veiligstellen (1)                                                             | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik weet wie ik moet benaderen als ik vragen heb op het gebied van online criminaliteit (2)           | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik weet welke online sporen (mogelijk) te vorderen zijn (3)                                          | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik kan een vordering opmaken om online gegevens van een dader te achterhalen (zoals IP-adressen) (4) | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik ken de interceptiemogelijkheden bij online criminaliteit (5)                                      | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik kan een proces-verbaal opmaken voor vormen van online criminaliteit (6)                           | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |
| Ik weet hoe ik onderzoeksbevindingen van online criminaliteit moet analyseren en duiden (7)          | <input type="radio"/>          | <input type="radio"/>               | <input type="radio"/>         | <input type="radio"/> |

15. In welke mate wilt u zich verder ontwikkelen op de hiervoor genoemde punten?

- ☐ Helemaal geen interesse
- ☐ Weinig interesse
- ☐ Enige interesse
- ☐ Veel interesse
- ☐ Zeer veel interesse

16. Geef aan in hoeverre u deze kennis bezit of vaardigheid hebt. Alleen leidinggeven-  
de of operationeel specialisten. [Let op: Er zijn geen goede of foute antwoorden]

|                                                                                                                                         | Ik ken/kan het<br><b>niet</b> (1) | Ik ken/kan het<br><b>enigszins</b> (2) | Ik ken/kan het<br><b>wel</b> (3) | Weet ik niet<br>(4)   |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|----------------------------------------|----------------------------------|-----------------------|
| Ik heb kennis over slachtofferschap van online criminaliteit in het werkgebied van het basisteam (1)                                    | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik heb kennis over daderschap van online criminaliteit in het werkgebied van het basisteam (2)                                          | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik heb voldoende basiskennis over de inhoud van en ontwikkelingen rondom online criminaliteit om mijn team hierop aan te sturen (3)     | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik kan richting geven aan de aanpak van online criminaliteit (4)                                                                        | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik kan medewerkers faciliteren en stimuleren om hun kennis en vaardigheden voor het aanpakken van online criminaliteit te vergroten (5) | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik kan intern samenwerken op het gebied van online criminaliteit (6)                                                                    | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |
| Ik kan extern samenwerken op het gebied van online criminaliteit (7)                                                                    | <input type="radio"/>             | <input type="radio"/>                  | <input type="radio"/>            | <input type="radio"/> |

17. In welke mate wilt u zich verder ontwikkelen op de hiervoor genoemde punten?

- ☐ Helemaal geen interesse
- ☐ Weinig interesse
- ☐ Enige interesse
- ☐ Veel interesse
- ☐ Zeer veel interesse

18. Wat is volgens u de impact van online criminaliteit op de samenleving?

- ☐ Klein
- ☐ Gemiddeld
- ☐ Groot

## Motivatatie

19. In hoeverre bent u het met de volgende stellingen eens?

| <i>Item:</i><br>Ik ... om online criminaliteit aan te pakken in mijn werk binnen het basisteam. | <i>Mee oneens</i>     | <i>Niet mee oneens/niet mee eens</i> | <i>Mee eens</i>       |
|-------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|-----------------------|
| ben gemotiveerd                                                                                 | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> |
| word gemotiveerd door collega's                                                                 | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> |
| word gemotiveerd door de leiding                                                                | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> |
| heb zelfvertrouwen                                                                              | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> |
| ervaar belemmeringen                                                                            | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> |
| werk nauw samen met collega's                                                                   | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> |
| motiveer mijn collega's                                                                         | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> |

## Taken basisteam

20. Welke taken met betrekking tot online criminaliteit hebben u en/of uw collega's het afgelopen jaar uitgevoerd binnen uw basisteam? [meerdere antwoorden mogelijk]

In hoeverre bent u het eens met de volgende stellingen? 'Ik vind ... een belangrijke taak van mijn basisteam.'

| <i>Stelling</i>                                                                                                                                                           | <i>Sterk mee oneens</i> | <i>Mee oneens</i>     | <i>Niet mee oneens/niet mee eens</i> | <i>Mee eens</i>       | <i>Helemaal mee eens</i> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------------|--------------------------------------|-----------------------|--------------------------|
| Preventie van <b>daderschap</b> van online criminaliteit                                                                                                                  | <input type="radio"/>   | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> | <input type="radio"/>    |
| Preventie van <b>slachtofferschap</b> van online criminaliteit                                                                                                            | <input type="radio"/>   | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> | <input type="radio"/>    |
| Verstoren van online criminaliteit                                                                                                                                        | <input type="radio"/>   | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> | <input type="radio"/>    |
| Opsporing van online criminaliteit                                                                                                                                        | <input type="radio"/>   | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> | <input type="radio"/>    |
| Alternatieve interventies<br>I: zoals de waarschuwingsbrief, een stopgesprek met geldezels, Hack_Right of een directe aansprakelijkstelling met bijvoorbeeld deurwaarders | <input type="radio"/>   | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> | <input type="radio"/>    |
| Nazorg aan slachtoffers (bijvoorbeeld adviezen geven aan aangevers om herhaald slachtofferschap te voorkomen)                                                             | <input type="radio"/>   | <input type="radio"/> | <input type="radio"/>                | <input type="radio"/> | <input type="radio"/>    |

---

### Aanpak online criminaliteit

22. Wie zou volgens u online criminaliteit in uw werkgebied moeten aanpakken? (U kunt de blokjes verslepen tot ze voor u in de juiste volgorde staan. Daarbij is 1 de groep die de grootste rol moet spelen in de aanpak) [ranking vraag en randomisatie van antwoorden]

|   |                                       |
|---|---------------------------------------|
| O | Alle collega's van mijn basisteam     |
| O | Een deel van mijn basisteam           |
| O | Andere afdelingen van de politie      |
| O | Andere organisaties buiten de politie |

### Interventies

Tot slot willen we u nog vragen op welke manier u het liefst leert over nieuwe onderwerpen die relevant zijn voor uw politietaak.

23. Welke factoren zijn volgens u belangrijk in het ontwikkelen van kennis/vaardigheden voor de aanpak van online criminaliteit? [ranking vraag] (U kunt de blokjes verslepen tot ze voor u in de juiste volgorde staan. Daarbij is 1 de grootste prioriteit.) [randomisatie van antwoorden]

|   |                                                                                   |
|---|-----------------------------------------------------------------------------------|
| 1 | Tijd krijgen van de werkgever                                                     |
| 2 | Prioritering van thema online criminaliteit (actief gestuurd vanuit de werkgever) |
| 3 | Beschikbaarheid van goed leeraanbod                                               |
| 4 | Eigen motivatie                                                                   |
| 5 | Beloning vanuit werkgever                                                         |
| 6 | Goede hulpmiddelen (laptops, telefoons et cetera)                                 |
| 7 | Leren van enthousiaste collega's                                                  |
| 8 | Ik wil helemaal niets leren over online criminaliteit                             |

24. Ik leer het beste (door) ... (1 = niet belangrijk, 2 = enigszins belangrijk, 3 = wel belangrijk)

| <i>Item</i>                                                                                               | <b>Niet belangrijk<br/>(1)</b> | <b>Enigszins belang-<br/>rijk (2)</b> | <b>Wel belangrijk<br/>(3)</b> |
|-----------------------------------------------------------------------------------------------------------|--------------------------------|---------------------------------------|-------------------------------|
| In een fysieke setting (1)                                                                                | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Alleen (2)                                                                                                | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Tijdens reguliere werkzaamheden (meedraaien met onderzoek met ervaren collega's) (3)                      | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Zelf informatie op te zoeken/lezen (handboek/ intranet/ mailing) (4)                                      | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Leren van politiecollega's binnen basisteam (6)                                                           | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Leren van politiecollega's buiten het basisteam (team cybercrime, ECDO, digitaal platform et cetera) (17) | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Leren van externen (buiten de politie) (16)                                                               | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Technologisch hulpmiddel (bijvoorbeeld webapp cybercrime, chatbot) (10)                                   | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| In een online setting (11)                                                                                | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| In een team (12)                                                                                          | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Buiten reguliere werkzaamheden (bijvoorbeeld clusterdagen, trainingsdagen) (13)                           | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Informatie die wordt aangeboden (cursus, training, escaperoom) (14)                                       | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |
| Fysiek hulpmiddel (handleiding/handboek) (20)                                                             | <input type="radio"/>          | <input type="radio"/>                 | <input type="radio"/>         |

25. Wilt u iets toelichten over het leren over de aanpak van online criminaliteit binnen basisteams? (voor uzelf en/of voor uw basisteam)

#### *Demografische gegevens*

Voor de afronding van de vragenlijst stellen wij u graag nog een aantal algemene vragen over uw positie binnen de politie. Deze vragenlijst is vanzelfsprekend anoniem en de gegevens worden nooit herleidbaar tot een persoon verwerkt.

26. In welke eenheid bent u werkzaam? *Drop down menu met alle eenheden*

- ☐ Amsterdam
- ☐ Den Haag
- ☐ Limburg
- ☐ Midden-Nederland
- ☐ Noord-Holland
- ☐ Noord-Nederland
- ☐ Oost-Brabant
- ☐ Oost-Nederland
- ☐ Rotterdam
- ☐ Zeeland- West-Brabant

27. Heeft u bij de politie specifieke taken of rollen met betrekking tot online criminaliteit? [meerdere antwoorden mogelijk, bij 'nee' worden de andere antwoordopties uitgezet]

|                       |                                                                                  |
|-----------------------|----------------------------------------------------------------------------------|
| <input type="radio"/> | Nee                                                                              |
| <input type="radio"/> | Ja, digi-coach                                                                   |
| <input type="radio"/> | Ja, digitaal wijkagent                                                           |
| <input type="radio"/> | Ja, portefeuillehouder/taakaccenthouder online criminaliteit (of vergelijkbaars) |
| <input type="radio"/> | Ja, namelijk ...                                                                 |

28. Hoe lang bent u in dienst bij de politie?

|                       |                                     |
|-----------------------|-------------------------------------|
| <input type="radio"/> | [jaar zelf invullen, hele getallen] |
|-----------------------|-------------------------------------|

29. Wat is uw leeftijd?

|                       |                      |
|-----------------------|----------------------|
| <input type="radio"/> | [jaar zelf invullen] |
| <input type="radio"/> | Zeg ik liever niet   |

30. Hoe identificeert u zich qua gender?

|                       |                                         |
|-----------------------|-----------------------------------------|
| <input type="radio"/> | Man                                     |
| <input type="radio"/> | Vrouw                                   |
| <input type="radio"/> | Ik beschrijf het liever als [invulveld] |
| <input type="radio"/> | Dat zeg ik liever niet                  |

31. Heeft u een opleiding of cursus gevolgd op het gebied van online criminaliteit? (meerdere antwoorden mogelijk) [bij 'nee, maar ...' of 'nee' worden de andere antwoordopties uitgezet]

|                       |                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------|
| <input type="radio"/> | Ja, op het gebied van cybercrime                                                    |
| <input type="radio"/> | Ja, op het gebied van gedigitaliseerde criminaliteit                                |
| <input type="radio"/> | Ja, maar ik weet niet of het ging over cybercrime of gedigitaliseerde criminaliteit |
| <input type="radio"/> | Nee, maar ik heb een aparte opleiding gevolgd op het gebied van IT                  |
| <input type="radio"/> | Nee                                                                                 |

32. Heeft u nog een opmerking of suggestie over de aanpak van online criminaliteit door politie basisteams en/of de vragenlijst?

|                       |                  |
|-----------------------|------------------|
| <input type="radio"/> | Nee              |
| <input type="radio"/> | Ja, namelijk ... |

33. Zou u bereid zijn om aanvullende toelichting te geven op basis van de algemene resultaten van deze vragenlijst? Indien ja, mogen wij dan contact met u opnemen? Uw e-mailadres wordt niet gekoppeld aan de door u ingevulde vragenlijst.

|                       |                                         |
|-----------------------|-----------------------------------------|
| <input type="radio"/> | Ja, dit is mijn e-mailadres [invulveld] |
| <input type="radio"/> | Nee                                     |

*Bedankt voor de tijd die u heeft genomen om deze vragenlijst in te vullen. Bij vragen kunt u terecht bij [e-mailadres hoofdonderzoeker]*

## Bijlage 5 Interviewprotocol landelijke opschaling

### *Inleiding*

Allereerst bedankt dat u mee wilt werken aan dit onderzoek. Afgelopen anderhalf jaar hebben wij gewerkt met twee basisteams waarbij wij interviews hebben afgenomen ( $n = 19$ ). En daarnaast hebben wij een vragenlijst uitgezet ( $n = 275$ ) onder een representatieve steekproef van alle basisteammedewerkers in Nederland. Uit deze data hebben wij een aantal inzichten (principes voor intensivering) gedestilleerd over hoe op landelijk niveau de lokale aanpak van online criminaliteit kan worden opgeschaald.

### *Doel van interview*

Het doel van het onderzoek is om inzicht te verkrijgen in welke zaken nodig zijn om basisteams effectief voor te bereiden op een intensievere aanpak van online criminaliteit op lokaal niveau. In dit interview verkennen wij graag inzichten om deze verandering te realiseren en hierin zouden wij met u graag op verschillende niveaus willen in- en uitzoomen (van landelijk naar eenheid naar lokaal).

### *Belangrijk.*

- Vooraf interview toestemmingsformulier opgestuurd.
- Gelukt met *informed consent* formulier in te vullen?
- Checken of respondent aanvullende info nodig heeft over onderzoek (vragen?).
- Alle input wordt in principe anoniem verwerkt in een eindrapport, tenzij u anders heeft aangegeven in het toestemmingsformulier. U heeft als het goed is aangegeven welke informatie wel en niet gebruikt mag worden? (naam en functie)

**Naam interview-deelnemer:**

**Functie:**

**Respondentnummer:**

**Datum:**

### *Korte toelichting*

- Interviews ( $n = 20$ ) en landelijke vragenlijst onder basisteams ( $n = 275$ )
- Structuur van interview toelichten (drie thema's: *uitzoomen*, *inzoomen*, *principes*)

### Intro

1. Allereerst, kunt u iets vertellen over uw **functie/rol binnen de politie**?
2. In welke mate **heeft u binnen uw functie te maken met online criminaliteit**?
3. Heeft u **affiniteit** met het onderwerp online criminaliteit?

### Uitzoomen (landelijk en eenheidsniveau)

Voordat wij het gaan hebben over de lokale aanpak van online criminaliteit binnen basisteams, willen wij graag eerst wat vragen stellen op meer landelijk en structureel niveau binnen de politie.

4. Als we even *uitzoomen* en kijken naar de **aanpak van online criminaliteit op landelijk niveau**, hoe vindt u dit gaan?
  - a. Wat gaat er al goed?
  - b. Wat moet er veranderen, denkt u? Waar liggen de kansen?
  - c. Wat zijn de ambities voor de politie voor de komende jaren?
5. Bent u bekend met **specifieke doelstellingen** omtrent het aanpakken van online criminaliteit? (denk aan KPI's, targets, aantal zaken et cetera)
  - a. Op landelijk niveau?
  - b. Op eenheidsniveau?
  - c. Op basisteamniveau?
6. Worden die doelstellingen **behaald**?
  - a. Zo niet, waar ligt dat denkt u aan?
7. Wat is daarvoor nodig, om dat te bereiken? [in een ideale wereld]

### Inzoomen (lokaal niveau)

Nu willen wij graag *inzoomen* op de lokale aanpak van online criminaliteit binnen de basisteams.

8. Wat vindt u van het idee dat basisteams **op lokaal niveau meedoen** in de aanpak van online criminaliteit?
  - a. Hoe ziet u dit binnen de **politietaat**? (kijkend naar: I&S, recherche, incidentafhandeling)
  - b. Op **welk niveau** moeten ze bijdragen? (eenvoudige vormen van online criminaliteit versus complexe vormen) En waar ligt de prioriteit?

- 
9. Waar ligt de **grens** van een basisteam en Cybercrimeteam op het gebied van online criminaliteitszaken? En moeten ze meer **samenwerken**?
- a. Zijn er nog **andere samenwerkingen** op het gebied van de aanpak van online criminaliteit die belangrijk zijn voor het basisteam om op te pakken? (zoals tussen basisteams door het land?)
10. Als u kijkt naar het **kennis- en vaardigheidsniveau** in de aanpak van online criminaliteit, zijn basisteams hier op dit moment al **klaar** voor? (kijkend naar: I&S, recherche, incidentafhandeling)
- a. Waar liggen de **sterke punten**?
- b. Waar liggen de **zwakke punten**?
11. Als u **één kernprobleem** zou moeten aanwijzen in de huidige lokale aanpak van online criminaliteit binnen de basisteams, welke zou dat zijn? (en waarom?)
12. Wat hebben die basisteams denkt u **nodig** om de aanpak van online criminaliteit intensiever uit te voeren?
- a. Denkt u meer aan een **specialistische aanpak** of **politietak breed**?
- b. [mening over digi-dagen, actiedagen, workshops, et cetera uitvragen]

### Principes voor intensivering

Tijdens ons onderzoek hebben wij uit de interviewdata meerdere **principes voor intensivering** gedestilleerd. Dit zijn principes waarvan wij denken dat ze belangrijk zijn voor de intensivering van de lokale aanpak van online criminaliteit op politiebasis-teams. Wij horen graag uw kijk op deze principes.

**PRINCIPE 1:** Om te intensiveren moet de **perceptie** van de basisteampolitiemedewerker veranderen naar een paradigma waarin **urgentie** wordt gevoeld.

*Hoe?*

Slachtofferschap en daderschap moet zichtbaar zijn in het lokale werkgebied, zodat de **impact** op de samenleving duidelijk is.

**urgentie/omvang** = aantal online criminaliteitsvormen en slachtoffers in werkgebied, met schade indicatie (bijvoorbeeld aantal euro's aan oplichting).

**rechtvaardigheidsgevoel/onrechtgevoel** = lokale casuïstiek slachtoffers/daders.

13. **Herkent u zich in deze bevindingen?**
- a. Zo ja, kunt u dit verder toelichten?
- b. Zo niet, wat herkent u niet?
- c. Mist er nog iets?

**PRINCIPE 2:** De **lage motivatie** voor de aanpak van online criminaliteit kan worden verhoogd via

**Succesverhalen** van collega's – met **concrete casuïstiek** kan duidelijk gemaakt worden dat er daadwerkelijk resultaat geboekt kan worden.

**Learning by doing** in kleine stappen – hierdoor krijgt de politiemedewerker de **overtuiging** dat hij/zij **daadwerkelijk wat kan betekenen** in het aanpakken van online criminelen en het helpen van slachtoffers.

denk bijvoorbeeld aan:  
stopgesprekken bij *first offenders*,  
of, het bijwonen/verhoren van rechtszaken tegen lokale/regionale verdachten.

#### 14. Herkent u zich in deze bevindingen?

- Zo ja, kunt u dit verder toelichten?
- Zo niet, wat herkent u niet?
- Mist er nog iets?

**PRINCIPE 3:** Intensiveren is **maatwerk** per basisteam, waarbij gekeken moet worden naar

**Capaciteit** (fte's)

**Affiniteit** (**kerngroep** opzetten met gemotiveerde **early adopters**)

**Type functie** (I&S, recherche, incidentafhandeling, leiding)

**Functie-integratie** (waar mogelijk integreren in huidig takenpakket)

**Complexiteit** (eenvoudige vormen van criminaliteit)

**Tempo** (gebalanceerd in plaats van radicale omslag)

#### 15. Herkent u zich in deze bevindingen?

- Zo ja, kunt u dit verder toelichten?
- Zo niet, wat herkent u niet?
- Mist er nog iets?

**PRINCIPE 4:** Voordat gekeken wordt naar het verhogen van kennis en vaardigheden, moet er eerst een **cultuurver-schuiving** plaatsvinden, waarin de **weerstand tegen verandering** wordt belicht.

#### 16. Herkent u zich in deze bevindingen?

- Zo ja, kunt u dit verder toelichten?
- Zo niet, wat herkent u niet?
- Mist er nog iets?

**PRINCIPE 5:** Wanneer er ingezet wordt op het aanleren van kennis en vaardigheden.

Adequate leervoorwaarden: learning by doing, in fysieke omgeving, leren van politiecollega's.

Minder adequate leervoorwaarden: e-learning, individueel leren, zelf informatie instuderen.

#### 17. Herkent u zich in deze bevindingen?

- Zo ja, kunt u dit verder toelichten?
- Zo niet, wat herkent u niet?
- Mist er nog iets?

**PRINCIPE 6:** Leidinggevend (per afdeling op het basisteam) moeten **sturing** bieden en **prioriteiten** aanbrengen op het gebied van online criminaliteit. Het helpt als de leidinggevende hier van hogeraf (eenheid/landelijk niveau) **afdwingende macht** in krijgt.

**18. Herkent u zich in deze bevindingen?**

- a. Zo ja, kunt u dit verder toelichten?
- b. Zo niet, wat herkent u niet?
- c. Mist er nog iets?

**19. Door wie** moeten deze zes principes worden uitgevoerd binnen het basisteam?

**20. Wie moet hierin de kar trekken?**

**Afsluiting**

**21. Heeft u nog suggesties/opmerkingen** omtrent dit onderwerp die we niet hebben besproken in het interview, maar die u wel graag wilt delen?

**22. Mocht u nog tips hebben qua literatuur of politiedata** die betrekking hebben met wat wij in dit interview besproken hebben, ontvangen wij die graag via de mail.

*Hartelijk dank voor uw tijd voor dit interview!*

*Zodra het onderzoeksrapport gepubliceerd is, zullen wij dit met u delen.*



## Bijlage 6 Experts over de principes voor de landelijke opschaling

In de semigestructureerde interviews (zie hoofdstuk 6) hebben de onderzoekers een zestal principes met experts besproken voor de landelijke opschaling van de taken van basisteams ten aanzien van online criminaliteit. Deze principes – die in deze bijlage in de grijze kaders zijn opgenomen – zijn vooraf door de onderzoekers opgesteld op basis van het literatuuronderzoek, de interviews, vragenlijsten en het ontwerponderzoek naar interventies in de onderzochte basisteams. Hierop is de respondenten gevraagd te reageren met als doel deze aan te scherpen.

*Principe #1 – Het is nodig om urgentie voor online criminaliteit in de basisteams te voelen*  
Om de aanpak van online criminaliteit door de basisteams te intensiveren, moet dit personeel de urgentie voelen voor deze vormen van criminaliteit. Daarbij moeten slachtofferschap en daderschap zichtbaar worden in het lokale werkgebied, zodat de impact van deze criminaliteit op de lokale samenleving voor de medewerkers duidelijk is. Daarbij gaat het zowel om urgentie en omvang – op basis van aantallen online criminaliteitsvormen en slachtoffers in werkgebied, met schade-indicatie (bijvoorbeeld aantal euro's aan oplichting) – als om het rechtvaardigheidsgevoel van de medewerkers, door de verhalen van lokale slachtoffers en daders onder medewerkers van de basisteams bekend te laten zijn.

Vijf respondenten waren het met dit principe eens, vier waren er grotendeels mee eens en één respondent was het oneens met dit principe.

- Daarbij wees de respondent die het *oneens* was met dit principe vooral op de geografische oriëntatie van de politie en basisteams in het bijzonder, waarbij de respondent van mening is dat tijd en plaats als gevolg van de digitalisering veel meer fluïde zijn geworden en het daarmee veel meer nodig is dat er landelijke analyse plaatsvindt, waarop lokaal wordt aangepakt.
- De vijf respondenten die het *eens* waren met dit eerste principe wezen op de kans die er ligt in het leren van concrete lokale casuïstiek en gaven daarbij het belang aan van de beleving van politiemedewerkers: als zij het belang er niet van inzien, gaan zij er niet op acteren. Ook wees men naast de noodzaak voor de zichtbaarheid van lokale daders en slachtoffers op basis van data, op de noodzaak dat leidinggevende prioriteit geven aan online criminaliteit en hierop sturen en dat de medewerkers van de basisteams zich bewust zijn van de impact van slachtofferschap van online

criminaliteit. Daarbij is slachtoffergericht optreden als belangrijkste aangemerkt en werd in het bijzonder de noodzaak tot het tegengaan van *victim blaming* door een respondent genoemd. Ook gaven de respondenten aan dat het opnemen van aangiften van online criminaliteit kunnen bijdragen aan het creëren van meer ervaren urgentie.

- De vier respondenten die het *deels eens* waren met dit principe wezen vooral op de kwalitatieve impact van slachtofferschap: aantallen en schadebedragen zeggen volgens hen niet zoveel, het gaat erom welke betekenis slachtoffer hier zelf aan toekennen. Ook wees men hierbij op de positieve bijdrage van digi-dagen die meer interesse onder collega's zouden kunnen creëren en wees men op de noodzaak voor empathisch handelen richting slachtoffers van online criminaliteit en het aanspreken van het rechtvaardigheidsgevoel van hun collega's.

#### *Principe #2 – Lage motivatie voor de aanpak van online criminaliteit verhogen*

De lage motivatie onder medewerkers van de basisteams om online criminaliteit aan te pakken kan worden verhoogd via succesverhalen van collega's met concrete casuïstiek, hiermee kan hen duidelijk worden gemaakt dat er daadwerkelijk resultaat geboekt kan worden ten aanzien van online criminaliteit. Ook kan *learning by doing* in kleine stappen de politiemedewerker overtuigen dat men daadwerkelijk iets kan betekenen in het aanpakken van online criminelen en het helpen van slachtoffers. Denk hierbij aan stopgesprekken bij *first offenders* of het bijwonen van verhoren of rechtszaken met lokale dan wel regionale verdachten.

Met dit principe waren zes respondenten het eens en drie waren dat deels (een respondent is hier niet over bevraagd).

- De respondenten die het *eens* waren met dit tweede principe wezen vooral op de bevorderende rol van de leerstrategie *learning by doing*, in samenwerking met de eigen collega's, waarbij zij de toegevoegde waarde van lokale casuïstiek en de focus op eenvoudige zaken onderschreven om interesse voor de aanpak van online criminaliteit bij collega's te wekken. Daarbij merkten zij op dat het slachtoffergericht werken bijzondere aandacht behoeft en dat digi-coaches kunnen ondersteunen in de uitvoering van deze transitie op de basisteams. Het hebben van korte lijnen met deze experts, maar ook het raadplegen van beschikbare informatie via het ECDO werden als kansrijk genoemd. Daarbij werd ook gewezen op ervaringen in Oost-Nederland met het project De Digitale Meldkamer. Deze respondenten wezen eveneens op het belang van draagvlak onder de leidinggevenden van het basisteam: zij moeten prioriteit en ruimte geven om zich deze nieuwe materie eigen te maken en daarnaast duidelijk sturen op het realiseren van deze nieuwe politietaak en eventuele weerstand begeleiden. Daarbij worden ook kansen gezien in het verstoren van de lokale daders en dadergroepen. Daarnaast wordt gewezen op het belang van het omarmen van het hybride karakter van criminaliteit.
- De drie respondenten die het *deels* met dit principe *eens* waren, wezen vooral op het belang van het betrekken van de *early adopters* op de basisteams en de voorkeur

---

van basisteammedewerkers om van collega's te leren. Daarbij tekenden zij aan dat collectief leren echt noodzakelijk is en ouderwets, klassikaal leren of leren op basis van e-learningen echt moet worden voorkomen. Daarbij is de beperkte opleidingscapaciteit die er is, naar hun beeld het best in te vullen via *learning by doing* aan de hand van lokale casuïstiek. Daarbij kunnen digi-coaches ondersteunen, maar moet eventuele weerstand onder collega's echt door de teamleiding en andere functionarissen met een inhoudelijke of hiërarchische leidinggevende rol in de basisteams (hierna 'het kader') worden begeleid.

*Principe #3 – Intensiveren is maatwerk in elk basisteam*

De intensivering van de aanpak van online criminaliteit door de basisteams is maatwerk waarbij gekeken moet worden naar capaciteit (fte's). Daarnaast is het goed om medewerkers met affiniteit met deze materie in een kerngroep van gemotiveerde *early adopters* aan de slag te zetten. Het is daarbij nodig om onderscheid te maken in wat elke type functie (I&S, basisteamrecherche, incidentafhandeling, leiding) aan kennis en vaardigheden nodig heeft, maar daarbij ten aanzien van online criminaliteit taken in het huidige takenpakket op te nemen. Daarbij moet het basisteam zich richten op de aanpak van eenvoudige vormen van online criminaliteit en is het raadzaam een gebalanceerd tempo aan te houden in plaats van ineens een radicale omslag te maken.

De respondenten waren ambivalent ten aanzien van dit principe. In eerste instantie waren de tien respondenten het deels eens met dit principe, maar vijf kwamen daar later op terug en waren het toch oneens.

- De respondenten waren het *deels eens* over het aspect dat de aanpak van online criminaliteit onderdeel van de reguliere functies binnen de basisteams zouden moeten worden. Op basis van de aantallen slachtoffers in de samenleving is immers volgens hen niet meer uit te leggen dat hier nog relatief weinig politiecapaciteit naar uitgaat. Daarbij moet wel onderscheid worden gemaakt in de functies binnen de basisteams: niet iedereen moet hetzelfde weten en kunnen. Daarbij merken zij op dat de leidinggevers duidelijk moeten sturen op de aanpak van online criminaliteit, hier ruimte voor moeten geven en het lastige gesprek niet moeten schuwen over welke taken dan niet meer of minder worden gedaan. Een van de respondenten merkte daarbij op dat online criminaliteit, net als georganiseerde misdaad, thematisch in plaats van specialistisch genoemd zou kunnen worden.
- De respondenten waren het eens met de te grote afhankelijkheid van de aanpak van online criminaliteit van de affiniteit onder medewerkers van basisteams. De politie moet met de tijd meegaan en dit betekent dat basisteams moeten investeren in de aanpak van online criminaliteit: zij zijn hierin een belangrijke schakel. In de ogen van deze respondenten is de aanpak van online criminaliteit een algemene politietask waarbij medewerkers niet overspoeld moeten raken met informatie over en taken in de aanpak van online criminaliteit. Men moet de kans krijgen om hier, in samenwerking met de *early adopters* in de basisteams en onder begeleiding van digi-coaches zelf mee aan de slag te gaan omdat de routine ontbreekt. Daarbij wordt

aangetekend dat te veel specifieke aandacht voor ‘online’ en ‘cybercriminaliteit’ alleen maar meer afstand zou creëren: het is van belang dit als criminaliteit te framen.

- De respondenten die het *oneens* waren met dit principe legden de nadruk op de capaciteitsvraag. Zij zijn van mening dat er op basis van de omvang en impact van slachtofferschap meer politiecapaciteit naar de aanpak van online criminaliteit zou moeten gaan. Deze zou altijd al onder druk staan, waardoor het noodzakelijk is om heldere keuzes en afspraken te maken over welke taken niet meer of in mindere mate worden uitgevoerd. Daarbij merken zij op dat de vrijblijvendheid om online criminaliteit aan te pakken voor de basisteams er echt vanaf zou moeten.

#### *Principe #4 – Medewerkers van de basisteams vragen om een heldere leerstrategie*

Wanneer er in de basisteams wordt ingezet op het aanleren van kennis en vaardigheden ten aanzien van de aanpak van online criminaliteit dan zijn *learning by doing*, in een fysieke omgeving op basis van het leren van politiecollega's adequate leervoorwaarden. Minder adequate leervoorwaarden zijn daarbij e-learnings, individueel leren en personeel zelf informatie laten instuderen.

Vijf respondenten waren het eens met dit principe, vier waren dat deels en één was het ermee oneens.

- De respondenten die het met dit principe *eens* waren, leggen de nadruk op de leerstrategie dat medewerkers van basisteams graag van collega's zouden willen leren. Daarbij merken zij op dat groepsgewijs en in offline bijeenkomsten op basis van *learning by doing*, met korte lijnen met experts (bijvoorbeeld via de digi-hulplijn) en vanaf de start gericht op interne samenwerking het meest kansrijk zou zijn. Deze verandering drijft idealiter op interesse en enthousiasme van collega's. Daarin merken zij op dat de steun van leidinggevend en de ruimte om te leren noodzakelijk zijn, waarbij ook duidelijke afspraken gemaakt moeten worden.
- De respondenten die het *deels eens* waren met dit principe merkten op dat het in hun ogen niet te voorkomen is dat deels van het leren individueel plaatsvindt, maar dat e-learnings daarbij echt moeten worden voorkomen. Zij merkten verder op dat leidinggevend ervoor moeten zorgen dat *learning by doing* tijdens werktijd plaatsvindt.
- De respondent die het *oneens* was met dit principe merkte op dat bij veel collega's in de basisteams de nieuwsgierigheid voor nieuwe informatie en werkwijzen ontbreekt en zij te weinig openstaan voor het breder leren dan enkel van collega's uit hun eigen basisteams. Dit werd gekoppeld aan het overall, praktijkgerichte opleidingsniveau van de politieorganisatie en de basisteams waarmee niet te veel zelfstandigheid in het eigen maken van nieuwe kennis en vaardigheden moet worden verwacht. Waarbij de respondent eveneens wees op het ontbreken van routine in de aanpak van online criminaliteit binnen de basisteams. Daarin ligt een risico besloten, als dit niet voldoende wordt begeleid.

---

*Principe #5 – Teamchefs en het kader moeten prioriteren, sturen en afdwingende macht krijgen*

De teamchef en het kader van het basisteam moeten als leidinggevend (per afdeling op het basisteam) sturing bieden en prioriteiten aanbrengen in de aanpak van online criminaliteit. Daarbij helpt het als de leidinggevende hier vanuit de eenheid en het landelijk niveau afdwingende macht voor krijgt.

- De tien respondenten waren *unaniem* over de belangrijke rol van teamchefs en het kader bij deze transitie van basisteams naar de aanpak van online criminaliteit. Zij spelen lokaal een belangrijke rol in de transitie naar de aanpak van online criminaliteit, waarbij naast het sturen van de transitie in het basisteam de nadruk volgens de respondenten ligt op het sturen op de daadwerkelijke aanpak van online criminaliteit en het ruimte geven voor de benodigde verandering en het leren. Daarbij wordt veel belang gehecht aan het maken van duidelijke afspraken binnen het basisteam en wordt eveneens gewezen op de rol die Operationeel Commandanten (OPCO's) spelen binnen de dagelijkse praktijk van basisteams: zij kunnen eveneens mee- en bijsturen en moeten in de transitie niet worden vergeten in stelling te brengen. Dit geldt eveneens voor de OSA's, waarnaast ook experts in de aanpak van online criminaliteit kunnen meesturen.
- De respondenten benadrukken hierbij de noodzaak van een eenduidige verandering van het lokale managementteam waar ook de eenheidsleiding achter moet staan. Deze strategie draait om het lokaal omarmen van de noodzaak online criminaliteit tegen te gaan en het terugdringen van het vrijblijvende karakter van de aanpak van online criminaliteit door de basisteams waarin ook duidelijke KPI's en beleidskeuzes nodig zijn. Zij zetten daarbij in op het motto 'niet afwachten maar aanpakken' en benoemen daarbij het belang van het vieren van successen in de transitie, want dit houdt medewerkers gemotiveerd. Daarbij is het vooral aan de teamchefs om ruimte en duidelijkheid in de verandering te bieden en helderheid te geven over welk werk dan minder of niet meer gebeurt. Daarbij merkte een respondent op dat het van groot belang is om oog te hebben voor de informele processen in het basisteam en hier effectief op in te spelen in het begeleiden van de transitie. Deze verandering doet dan ook een groot beroep op de leidinggevende en veranderkundige vaardigheden van het managementteam van de basisteams. Daarbij wordt opgemerkt dat veel drijft op de veranderbereidheid en het effectief verleiden van medewerkers in plaats van weerstand benoemen en deze medewerkers aanspreken.

*Principe #6 – De lokale cultuur is van grote invloed*

Voordat in basisteams wordt gekeken naar het verhogen van kennis en vaardigheden ten aanzien van de aanpak van online criminaliteit, moet er eerst een cultuurverschuiving plaatsvinden, waarin de weerstand tegen verandering *an sich* wordt aangepakt in basisteams.

Van de zes principes leidde dit principe onder onze respondenten tot de meeste discussie. Van onze respondenten waren zeven het oneens met dit principe en drie waren het eens.

- De respondenten die het *oneens* waren met dit principe gaven aan dat wat hen betreft beter ingezet kan worden op een groep van *early adopters* onder werknemers van de basisteams, die zich willen verdiepen in de aanpak van online criminaliteit in plaats van eerst een cultuurverandering teweeg te willen brengen. Eventuele weerstand tegen de aanpak van online criminaliteit moet wat hen betreft binnen het basisteam als geheel worden aangepakt, in plaats van individueel, waarbij teamchefs en het kader ook oog voor de informele processen in het basisteam moeten hebben. Daarbij wijzen deze respondenten op de noodzaak om mensen te verleiden om mee te bewegen in plaats van deze beweging af te willen dwingen. Daarbij merken zij op dat een cultuurverandering wat hen betreft te lang duurt.
- Ten aanzien van de aanpak van online criminaliteit moet wat hen betreft de vrijblijvendheid er door leidinggevendens vanaf gehaald worden. De weerstand die hierbij eventueel loskomt in het basisteam is aan de teamchef en het kader om in goede banen te leiden. Deze respondenten zien het als onderdeel van de leidinggevende taken van de teamchef en het kader om deze verandering te begeleiden en aan te jagen. Dit moet zeker niet aan digi-coaches worden overgelaten omdat dit hen zou overvragen. Opsporing zien zij ten aanzien van online criminaliteit meer als iets specialistisch waarin het goed zou zijn een toegewijde groep collega's op in te zetten. Verder is de aanpak van online criminaliteit een algemene politietaken waar nu nog te veel afhangt van affiniteit. Een respondent waarschuwt dat de verandering drijft op de bereidheid van mensen om te veranderen. Een teamchef kan daarom niet met een gestrekt been het basisteam naar taken in de aanpak van online criminaliteit bewegen. Ook moeten medewerkers niet ineens overspoeld worden met nieuwe informatie en taken, maar dit moet geleidelijk worden opgebouwd. Daarbij is *learning by doing* met ondersteuning door de digi-coaches de gepaste route in de basisteams.
- De respondenten die het *eens* waren met dit principe zaten duidelijk op een hardere veranderstrategie. Zij benadrukten dat wat hen betreft de vrijblijvendheid van de aanpak van online criminaliteit door het basisteam eraf moet, omdat het politiewerk met de tijd mee moet en criminaliteit intussen een hybride karakter kent. Tijd en plaats zijn hiermee fluïde geworden, waarmee de geografische oriëntatie van basisteams niet altijd houdbaar is omdat moet worden gedaan waar een zaak om vraagt. Daarbij is de afhankelijkheid van affiniteit in deze aanpak wat hen betreft niet meer uit te leggen. Het is aan de teamchef en het kader om hier wat hen betreft prioriteit aan te geven en op te sturen, waarbij wat hen betreft ook afspraken gemaakt kunnen worden over wat voor taken minder of niet meer worden gedaan. Wat deze respondenten betreft wordt iedere medewerker in de basisteams verplicht om bij te dragen aan de aanpak van online criminaliteit. Daarbij wordt ook aangekend dat deze aanpak wellicht ook om ander personeel vraagt en de werving van politiepersoneel wat hen betreft nog te veel inzet op het klassieke 'bloed en spoed'

---

terwijl het basispolitiewerk ook ander, belangrijk werk erbij heeft gekregen in de aanpak van online criminaliteit. Zij verwachten hierbij overigens wel dat jonge politiemedewerkers zich de taken rondom online criminaliteit eenvoudiger eigen zullen maken dan meer seniore medewerkers, omdat jongere medewerkers doorgaans zelf ook meer online actief zijn.



## Bijlage 7 Toestemmingsverklaring

### Inleiding

Allereerst bedankt dat u mee wilt werken met dit onderzoek. NHL Stenden Hogeschool en Hogeschool Saxion voeren een actieonderzoek uit naar de lokale aanpak van online criminaliteit. Dit doen we in samenwerking met de politie waaronder twee basisteams, een Cybercrimeteam en een digitaal platform. In dit formulier wordt u geïnformeerd over het onderzoek. Daarna wordt uw toestemming gevraagd voor deelname aan het onderzoek. In dit toestemmingsformulier wordt u gevraagd digitaal toestemming te geven. Dit dient voorafgaand aan het onderzoek te gebeuren.

### Doel van interview

Het doel van het onderzoek is om inzicht te krijgen in welke zaken nodig zijn om basisteams effectief voor te bereiken op een intensievere aanpak van online criminaliteit op lokaal niveau. In dit interview verkennen wij graag inzichten om deze verandering te realiseren en hierin zouden wij met u graag op verschillende niveaus willen in- en uitzoomen (van landelijk naar eenheid naar lokaal). Hierbij zijn wij niet op zoek naar 'complete kennis' op alle onderdelen, maar vooral of u vanuit uw expertise wat inzichten kunt bijdragen aan het grotere plaatje; dat zou enorm waardevol zijn.

We vragen u hierna aan te geven of u toestemming geeft voor uw deelname aan het onderzoek 'Expeditie Lokaal Digitaal'. Lees onderstaande punten alstublieft goed door. Ik verleen toestemming voor deelname aan het onderzoek 'Expeditie Lokaal Digitaal'. Hiertoe:

1. ben ik over aard, methode en doel van dit onderzoek op een voor mij duidelijke wijze geïnformeerd;
2. heb ik genoeg tijd gekregen om over deelname te beslissen;
3. heb ik de gelegenheid gehad om vragen te stellen over dit onderzoek;
4. weet ik dat deelname vrijwillig is;
5. weet ik dat ik op elk gewenst moment kan stoppen met deelnemen aan het onderzoek. Daarvoor hoef ik geen reden te geven;
6. geef ik toestemming voor het verzamelen, bewaren en gebruiken van mijn gegevens voor de beantwoording van de onderzoeksvraag in dit onderzoek;
7. weet ik dat de uitkomsten van dit interview verwerkt kunnen worden in een verslag of (wetenschappelijke dan wel praktijkgerichte) publicaties;
8. geef ik toestemming voor eventueel vervolgonderzoek op basis van deze data;

9. weet ik dat alleen ter controle van de wetenschappelijke integriteit van het onderzoek andere mensen dan de onderzoekers toegang tot mijn verzamelde gegevens kunnen krijgen;
10. begrijp ik dat alle informatie die ik met betrekking tot deze studie verstrek, zal worden gepseudonimiseerd, waardoor het niet direct naar mij herleidbaar zal zijn;
11. weet ik dat ik inzage kan krijgen in de wijze waarop de gegevens worden verwerkt en bewaard;
12. weet ik dat als ik mij terugtrek, mijn gegevens tot dat moment gebruikt kunnen worden, tenzij ik ook vraag om de reeds verzamelde gegevens te wissen;
13. geef ik toestemming tot het maken van een audio-opname van dit interview. Deze opname wordt in een beveiligde omgeving opslagen en is verder alleen te beluisteren door de onderzoekers en ter controle van de wetenschappelijke integriteit van de onderzoekers en de onderzoeksproducten.

**Audio-opname**

Ik geef toestemming tot het maken van audio-opnames. Deze zijn alleen te beluisteren door de onderzoeker(s) en ter controle van de wetenschappelijke integriteit. De opnamen worden opgeslagen in een beveiligde omgeving.

☐ Ja

☐ Nee

**Uw naam**

[ ]

**Uw functie**

[ ]

**Welke gegevens mogen wij gebruiken in het rapport?**

☐ Naam en functie

☐ Functie

☐ Geen van beide

*Klik a.u.b. op de knop hier beneden om het formulier in te dienen.*

## Bijlage 8 Tijdlĳn interventie-ontwikkeling

In deze bijlage is aanvullende informatie opgenomen aangaande de interventies die zijn opgezet, afgenomen en geëvalueerd bij basisteam Postenveld.

### Tijdlĳn interventieontwikkeling

| Datum              | Reden afspraak                                                                            | Aanwezigen                                                                                                                                    | Uitkomst                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7-5-25<br>1 uur    | Voorbespreking resultaten en huidige stand van zaken basisteam betreft digitale transitie | Huidige OS-C, digitaal wijkagent en één onderzoeker                                                                                           | Herkenning in resultaten en voorzet interventie-ideeën met mogelijkheden en beperkingen                                                                                |
| 14-5-25<br>2 uur   | Terugkoppeling resultaten en voorzet oplossingsidentificatie                              | Toekomstig OS-C, huidig OS-C, OS-A (portefeuillehouder digitaal), digitaal wijkagent, Tactisch Rechercheur Team Cybercrime, drie onderzoekers | Herkenning resultaten deelrapport 1, vaststelling doelstellingen en meerdere interventie-ideeën – keuze voor digi donderdag (later kennislunch)                        |
| 12-6-25<br>1 uur   | Thema's kiezen voor kennislunch en update van andere doelstellingen                       | Digitaal wijkagent, OE-GGP (Leiding en Sturing, verantwoordelijk voor digitalisering), één onderzoeker                                        | Kernteam weinig progressie, keuze gemaakt voor thema's kennislunch, voorstel OSINT opleiding gedaan                                                                    |
| 7-7-25<br>1 uur    | Bespreken inhoud kennislunch en nudges                                                    | Digitaal wijkagent, OS-C, 2 onderzoekers                                                                                                      | Update-ontwikkeling digitale transitie, inhoud kennislunch vastgesteld, nieuwe portefeuillehouder digitalisering nodig, concretere invulling van nudges en presentatie |
| 28-7-25<br>1 uur   | Verdere concretisering interventies                                                       | Digitaal wijkagent, OS-C, STO Team Cybercrime, 1 onderzoeker                                                                                  | Stavaza presentatie september en oktober, HINT-oefening besproken, twee nieuwe portefeuillehouders digitalisering tot en met september                                 |
| 27-8-25<br>1,5 uur | Concrete voorbereiding HINT en stavaza kennislunch                                        | Digitaal wijkagent, STO'er BT, Digi-professional, OS-C, OS-C, 1 onderzoeker                                                                   | Stavaza kennislunch en voorbereiding HINT-oefening. Twee digi-professionals inzetbaar voor opsporing en voorlichting/kennisoverdracht                                  |
| 23-9-25<br>1,5 uur | Verzetten kennislunch en stavaza digitale transitie BT                                    | Digitaal wijkagent, digi-professional, OS-C, 1 onderzoeker                                                                                    | Toelichting afzegging kennislunch, toekomstige interventies (labs/escaperoom), nieuwe kennislunch plannen en concrete stappen bespreken                                |
| 6-10-25            | Bespreken inhoud kennislunch                                                              | Digi-professional, 1 onderzoeker                                                                                                              | Bespreken inhoud kennislunch en organisatie ervan                                                                                                                      |

### Acties van onderzoeker bij deelvraag twee

De onderzoeker heeft een inventarisatie gemaakt van bestaande interventies om digitale kennis en vaardigheden te vergroten binnen basisteams. Na het vaststellen van de doelstellingen en interventies heeft de onderzoeker een bijdrage geleverd aan twee interventies.

- HINT-oefening (ondersteunende rol gespeeld in ontwikkeling en uitvoering)
  1. Locatie verzorgen voor casus-oefening
  2. Ondersteunen in casus-ontwikkeling
  3. Verzorgen figuranten tijdens casus-oefening en ondersteuning in communicatie met figuranten
  4. Uitleg geven figuranten
  5. Zelf figurant spelen (docent die melding maakt)
  6. Enkele keren terugkoppeling gegeven aan groepje over acties die goed gingen of die gemist waren
  7. Nabespreking met digitaal specialisten (1,5 uur)
  8. Verdere ontwikkeling van HINT-oefening (zoals terugkoppeling ter plekke door digitaal specialist)
- Kennislunch (leidende rol gespeeld in ontwikkeling en uitvoering)
  1. Toesturen van thema's met ideeën voor kennislunch
  2. Toesturen van bestaande interventies op thema's
  3. Ontwikkelen en aanscherpen van bestaande presentaties en 'nudges' voor thema dat gekozen is tijdens kennislunch
  4. Voorleggen van presentatie en nudges aan STO'er van Team Cybercrime
  5. Nieuwe datum kennislunch aanjagen met digi-professional
  6. Uitsenden uitnodigingsbrief met cybervrijwilliger voor kennislunch
  7. Verzorgen lunch tijdens kennislunch
  8. Voorbereiding kennislunch
  9. Verzorgen kennislunch (waaronder boodschappen) en evaluatie

## **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 shortlistmethodiek**

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. Römken & 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 tellen. 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 politieke 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. Nongarede & 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 politie-functionarissen**

H. Sollie, Universiteit Twente, Enschede, 2010

**34. Ten strijde tegen overlast. Jongerenoverlast op straat: is de Engelse aanpak geschikt voor Nederland?**

M.L. Koemans, Universiteit 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 basispolitie-zorg**

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 politieke 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 politiebriefting onderzocht. Een onderzoek naar de effectiviteit van de operationele politiebriefting**

A. Scholtens, J. Groenendaal & I. Helsloot, Crisislab, Renswoude 2013

**51a. De operationele politiebriefting onderzocht (2). Een actie(vervolg)onderzoek om tot een effectievere politiebriefting 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. Leiderschapontwikkeling 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. Sijtsma, 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 recherchepraktijk 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. Sijtsma & 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-aftoening**

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. Struiksmā, 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. Lünemann, 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 drugs-smokkel**

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 Merkesteyn, 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

**130. Online blauw. Een onderzoek naar de rol van basisteams in de aanpak van digitale criminaliteit en ervaringen van slachtoffers met de politie**

R. van Steden, S. ter Woerds, A. Merk, K. Schuppers, M. Willekers, D. Valk-van Waarde, R. Jansen, S. Ruiter. Politie en Wetenschap, Amsterdam, juni 2025

**131. Bruggenbouwers. Deel uitmaken en sturen van lokale samenwerkingsverbanden voor veiligheid en leefbaarheid**

A. Walberg, N. van der Klok, R. Spithoven. M.m.v. S. Ebrahim MSc, B. Schuitema, E. Foppen, K. Wittebrood, J. Klopman BA. Politie en Wetenschap, Amsterdam; Saxion, juni 2025

**132. Leren demonstreren. Een onderzoek naar nieuwe manieren van demonstreren en wat die betekenen voor de inzet en aanpak van de politie**

H. Ferwerda, E. Berger, E. Derksen, J. van Esseveldt, J. Wolsink, J. Timmer. Bureau Beke Arnhem, Vrije Universiteit Amsterdam, maart 2026

---

**133. De rol van social media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit**

J. Bergers, S. van Deuren, R. Roks, S. Habets, R. Leukfeldt, V. Eichelsheim. Vrije Universiteit Amsterdam, Erasmus University Rotterdam, Netherlands Institute for the Study of Crime and Law Enforcement, april 2026

**134. Cybercriminele jeugdgroepen. Een onderzoek naar het ontstaan, de groei en de aanpak van criminele jeugdgroepen in een gedigitaliseerde samenleving**

J. Loggen, S. Veenstra, R. Leukfeldt. Vrije Universiteit Amsterdam, Erasmus University Rotterdam, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR), juni 2026

**135. Samenspel bij digitaal en datagedreven politiewerk**

I. van Duijneveldt, L. Segers. Politie & Wetenschap, Apeldoorn; Andersson Elffers Felix (AEF), Utrecht, juli 2026

